INKLUSIVE 48 SEITEN
it security

it management

Der Motor für Innovation
November/Dezember 2024

UNIFIED ENDPOINT MANAGEMENT

Nachhaltigkeit beginnt am Endgerät

Sebastian Weber, Aagon GmbH

LEADERSHIP

Die dunkle Seite der Führung

A leader is one who knows the way, goes the way, and shows the way.

John C. Maxwell

THOUGHT LEADERSHIP

VOR DEM PROJEKT IST NACH DEM PROJEKT

LIEBE LESERINNEN UND LESER,

Nach jeder Ausgabe des it management und des it security, die erfolgreich in den Druck geht, kommt für mich ein Moment des Durchatmens und Neusortierens. Doch so wichtig und erholsam das auch ist, so schnell steht schon wieder die nächste Aufgabe an. Gerade bei der letzten Ausgabe des Jahres kommt ganz schnell der Gedanke, endlich mal alles Liegengebliebene abzuarbeiten und den Schreibtisch zu entmüllen. Die Ausgabe 1-2 erscheint ja erst im kommenden Jahr – also noch viel Zeit bis dahin.

Dieses „viel Zeit" ist aber leider immer relativ und ganz schnell wird es „höchste Eisenbahn" das nächste Projekt zu beginnen.
Genauso geht es wahrscheinlich den meisten Menschen, besonders aber denen, die dieses Jahr mal wieder gesetzliche Richtlinien bis zu einem bestimmten Stichtag umsetzen mussten. Eine davon war die NIS2-Richtlinie, Stichtag 17. Oktober. Es galt eine Reihe von Maßnahmen und Cybersicherheitsanforderungen zu erfüllen, sonst drohen Sanktionen. Nun verzögert sich das Umsetzungsgesetz und mit einem Inkrafttreten wird im März 2025 gerechnet.

Offensichtlich bleibt es manchmal nicht bei einem „nach dem Projekt, Luft holen, nächstes Projekt", sondern es wird zu einem „endlosen Projekt". Um das Risiko dafür zu reduzieren, sollte man von Anfang an ein paar Dinge beachten. Welche genau das sind, lesen Sie ab Seite 62.

Außerdem haben wir in dieser Ausgabe den Fokus auf die Themen ITSM und KI gelegt. Atmen Sie mal tief durch, nehmen sich Zeit und erfahren, welche Neuigkeiten und Entwicklungen es hier gibt.

Herzlichst,

Carina Mitzschke | Redakteurin it management & it security

INHALT

COVERSTORY

IT MANAGEMENT

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

Inklusive 48 Seiten it security

GUT ZU WISSEN

Achten Sie auf dieses Icon und lesen Sie mehr zum Thema im Internet auf **www.it-daily.net**

QUANTENTECHNOLOGIE

UNTERNEHMEN SEHEN DEUTSCHLAND WELTWEIT VORNE

Deutschland hat bei der Forschung zu Quantentechnologien eine weltweite Vorreiterrolle und kann führend in der Entwicklung und Anwendung von Quantum Computing werden. Das ist das Ergebnis einer Befragung von 87 Unternehmen, die bereits als Anbieter oder Anwender von Quantentechnologien aktiv sind oder entsprechende Planungen haben, im Auftrag des Digitalverbands Bitkom.

„Quantentechnologien bieten enorme Einsatzmöglichkeiten in unterschiedlichsten Branchen, von der Optimierung von Lieferketten über die Medikamentenforschung bis hin zur Vorhersage von Extremwetterereignissen. Deutschland hat sich in der Quantentechnologie eine hervorragende Ausgangsposition erarbeitet, nun muss es uns gelingen, diese in marktgängige Produkte und Lösungen zu überführen", sagte Bitkom-Hauptgeschäftsführer Dr. Bernhard Rohleder.

Herausforderungen

Die größte Herausforderung für den Einsatz von Quantentechnologien im eigenen Unternehmen ist für die Befragten dabei die noch unausgereifte Technologie (55 Prozent) sowie der unklare wirtschaftliche Nutzen (43 Prozent). 39 Prozent nennen eigene Investitionen in andere Zukunftstrends als Herausforderung für ein Engagement bei Quantentechnologien, 38 Prozent vermissen praktische Anwendungsbereiche und 38 Prozent beklagen eine noch ungenügende Standardisierung.

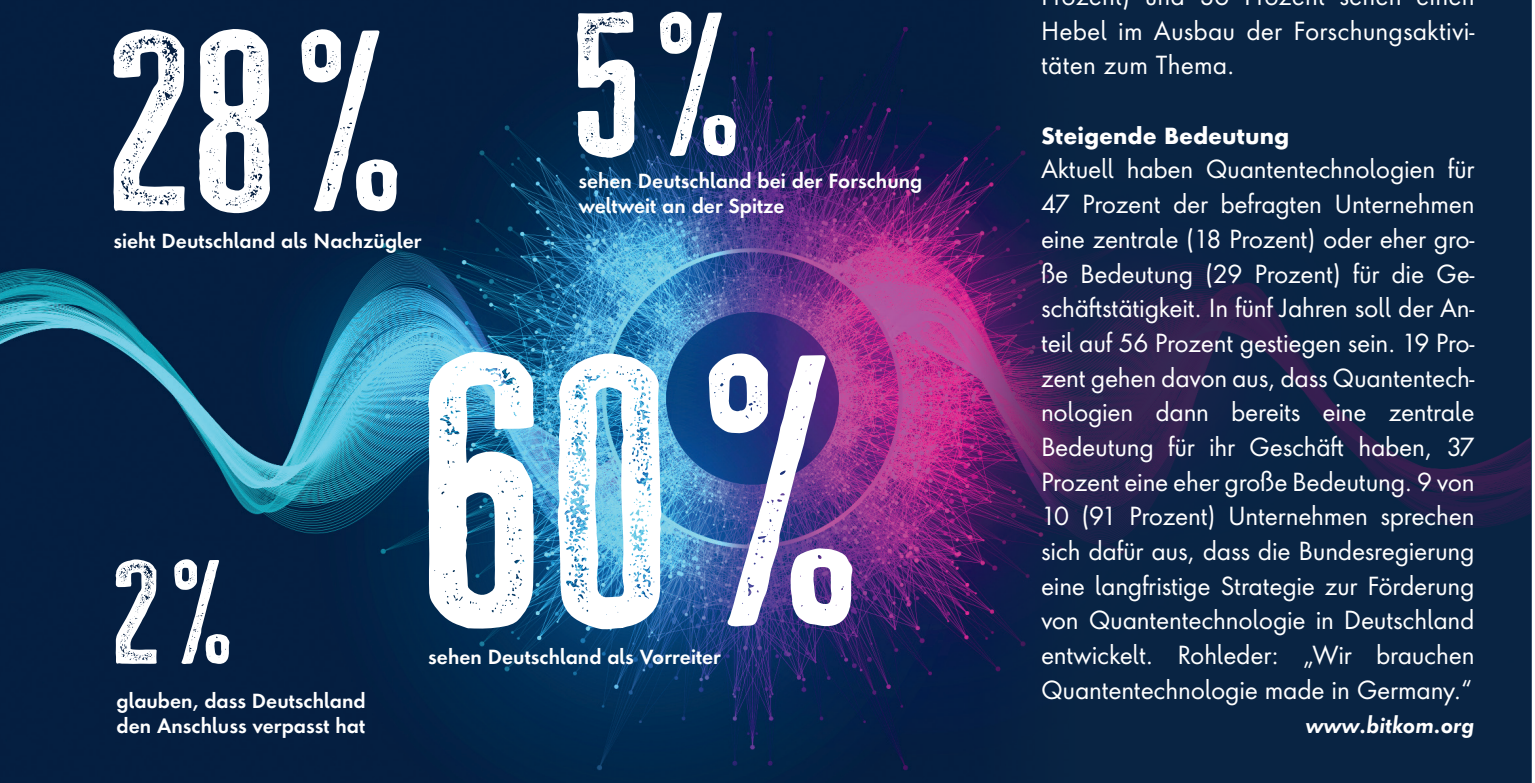
Um die Diskussion über den Einsatz von Quantentechnologien im Unternehmen voranzutreiben, wünschen sich 59 Prozent die finanzielle Förderung von Quantum-Projekten zur Anwendungsentwicklung, 52 Prozent eine bessere Information über marktfähige Anwendungen und 51 Prozent einen Austausch mit Hochschulen und Forschungseinrichtungen. 45 Prozent sprechen sich für einen niedrigschwelligen Zugang zu entsprechender Hardware und Infrastruktur aus. Einem Drittel würde ein Austausch mit Unternehmen helfen, die bei der Quantentechnologie bereits weiter sind (37 Prozent) und 36 Prozent sehen einen Hebel im Ausbau der Forschungsaktivitäten zum Thema.

Steigende Bedeutung

Aktuell haben Quantentechnologien für 47 Prozent der befragten Unternehmen eine zentrale (18 Prozent) oder eher große Bedeutung (29 Prozent) für die Geschäftstätigkeit. In fünf Jahren soll der Anteil auf 56 Prozent gestiegen sein. 19 Prozent gehen davon aus, dass Quantentechnologien dann bereits eine zentrale Bedeutung für ihr Geschäft haben, 37 Prozent eine eher große Bedeutung. 9 von 10 (91 Prozent) Unternehmen sprechen sich dafür aus, dass die Bundesregierung eine langfristige Strategie zur Förderung von Quantentechnologie in Deutschland entwickelt. Rohleder: „Wir brauchen Quantentechnologie made in Germany."

www.bitkom.org

QUANTENTECHNOLOGIE MADE IN GERMANY



KI-Rechenzentren

SCHLÜSSEL ZU EINER „GRÜNEN" ZUKUNFT?

Die zunehmende Nutzung künstlicher Intelligenz (KI) wirkt sich massiv auf den Strom- und Wasserverbrauch von Rechenzentren weltweit aus. Diese Entwicklung konfrontiert die Rechenzentrumsbranche mit Herausforderungen und Chancen in Bezug auf Nachhaltigkeit und Ressourcenmanagement. Dies geht aus der jüngsten unabhängigen Umfrage hervor, die von BCS (Business Critical Solutions) in Auftrag gegeben wurde. Für die Studie wurden die Meinungen von mehr als 3.000 Rechenzentrumsexperten in ganz Europa, darunter Eigentümer, Betreiber, Entwickler, Berater und Endnutzer eingeholt.

Aus dem Report geht hervor, dass mehr als 80 Prozent der Befragten im vergangenen Jahr einen Anstieg der Nachfrage nach Rechenzentrumskapazität verzeichneten, der auf die zunehmende Verbreitung von KI zurückzuführen ist. Allerdings weisen 85 Prozent der Befragten darauf hin, dass der Mangel an angemessener Infrastruktur und Energieressourcen eine erhebliche Einschränkung für die groß angelegte Nutzung dieser Technologie darstellt.

Vorteile nutzen

Trotz erheblicher Bedenken nutzt die Rechenzentrumsbranche KI bereits selbst, um erhebliche betriebliche Vorteile zu erzielen, darunter Effizienzsteigerung, Kostensenkung und Serviceoptimierung. Die Akzeptanz von generativer KI nimmt rapide zu: 65 Prozent der Befragten nutzen sie regelmäßig, fast doppelt so viele wie im Jahr 2023. Bezeichnenderweise schreiben 90 Prozent der Befragten der KI eine positive Wirkung auf die betriebliche Effizienz von Rechenzentren zu.

Der Report zeigt auch auf, wie KI eine Schlüsselrolle bei der Verringerung der Umweltauswirkungen spielen kann. KI-Algorithmen können den Energieverbrauch optimieren, den Kühlungsbedarf vorhersagen, die Arbeitslasten effizienter verwalten und die Ausfallzeiten von Servern minimieren. KI-basierte vorausschauende Wartung hilft außerdem, Ausfälle zu vermeiden und den Kühlungsbedarf zu reduzieren, was zu Energieeinsparungen führt.

www.bcsconsultancy.com

DIGITALE TRANSFORMATION

WO STEHEN DIE DEUTSCHEN BANKEN?

Während Banken mit schrumpfenden Budgets und steigenden Kundenerwartungen konfrontiert sind, setzen sie laut einer aktuellen Studie zunehmend auf künstliche Intelligenz (KI), um wettbewerbsfähig zu bleiben.

Die dritte Ausgabe der Global Banking Benchmark Study 2024 des Beratungsunternehmens Publicis Sapient, für die weltweit mehr als 1.000 Führungskräfte aus dem Bankensektor befragt wurden, belegt, dass die Banken einen entscheidenden Wandel hin zu KI-gesteuerten Lösungen vollziehen.

Fast ein Drittel ihrer Investitionen in die digitale Transformation des Kundenerlebnisses entfallen mittlerweile auf KI, maschinelles Lernen und generative KI (GenAI). Dies unterstreicht einen klaren Trend hin zu stärker personalisierten Dienstleistungen, datengestützter Entscheidungsfindung und agilen Prozessen, die es den Banken ermöglichen, in einem sich rasch wandelnden Markt schneller zu innovieren und effizienter zu arbeiten.

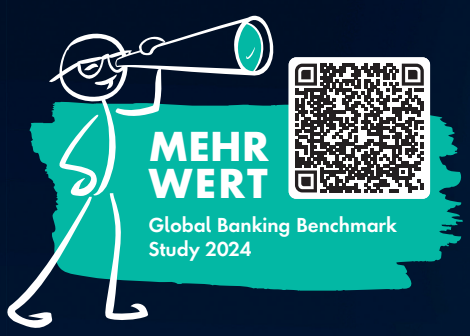
Digitale Transformation für Banken schwieriger geworden

Neben begrenzten Budgets sind regulatorische Herausforderungen, mangelnde operative Flexibilität und veraltete Technologien die größten Hindernisse für die digitale Transformation. Die Studie zeigt jedoch, dass Banken, die strategisch in KI und Agilität investieren, transformatives Wachstum und Effizienz erzielen können.

Der digitale Reifegrad ist sehr unterschiedlich. Die Studie teilt die befragten Banken in vier Gruppen ein, je nachdem, wie weit sie in den Bereichen Customer Leadership und Operational Leadership entwickelt sind. In diesem Jahr wurden nur 11 Prozent als Transformation Leader eingestuft, gegenüber 22 Prozent im Jahr 2022, während der Anteil der Slow Starter von 57 Prozent im Jahr 2022 auf heute 66 Prozent gestiegen ist.

Die Daten lassen große Unterschiede erkennen, wie Transformationsführer verglichen mit Nachzüglern KI einsetzen. Sie investieren nicht nur mehr, sondern konzentrieren sich auch darauf, die Grundlagen zu schaffen, um die Vorteile von KI besser nutzen zu können. So räumen 44 Prozent der Transformation Leader dem internen Einsatz von KI Priorität ein, aber nur 25 Prozent der Slow Starter.

www.publicissapient.com



KI IST AUF DEM VORMARSCH

Banken in Deutschland sehen das Potenzial von KI-Technologien, um die digitale Transformation voranzutreiben.

76 %

glauben, dass das größte Potenzial darin liegt, Prozesse effizienter, profitabler und schneller zu machen

24 %

der Ausgaben der Banken für die digitale Transformation des Kundenerlebnisses fließen vorrangig in maschinelles Lernen, KI und GenAI

Cyberkriminalität

NEUE BEDROHUNGEN FÜR VERBRAUCHERTECHNOLOGIEN

Cyberkriminelle entwickeln immer raffiniertere Methoden, um Verbraucher und Unternehmen anzugreifen. Das passiert oft auf Wegen, die viele von uns nicht einmal erahnen – selbst unsere Smartwatches oder Haushaltsgeräte können ein Einfallstor für Hacker sein.

www.paloaltonetworks.de

SO NEHMEN HACKER KONSUMENTEN INS VISIER

Juice Jacking

Juice Jacking bezeichnet eine Methode, bei der Angreifer öffentliche Ladestationen, etwa in Flughäfen oder Cafés, ausnutzen, um Malware auf Geräten zu installieren oder Daten zu stehlen.

Sobald Nutzer zum Beispiel ihr Smartphone oder Tablet an diese Stationen anschließen, kann Schadsoftware eingeschleust oder persönliche Daten abgegriffen werden.
Im Idealfall sollten Verbraucher eine eigene Powerbank mitführen, um ihre Geräte in öffentlichen Bereichen zu laden.

Evil Twin Angriff

Ein Evil-Twin-Angriff liegt vor, wenn Hacker ein gefälschtes WLAN-Netzwerk in öffentlichen Bereichen wie Restaurants, Flughäfen oder Einkaufszentren einrichten.
Dieses sieht einem legitimen Netzwerk täuschend ähnlich, wodurch der Nutzer dazu verleitet wird, sich damit zu verbinden – ohne die Täuschung zu bemerken.

Dies ermöglicht es Angreifern, sensible Daten wie Passwörter, E-Mails und Kreditkarteninformationen abzufangen. Laut einer Untersuchung von Forbes Advisor haben bereits vier von zehn Nutzern, die ein öffentliches WLAN-Netzwerk verwenden, einen Datenverlust durch solche Angriffe erlitten.

Cryptojacking

Beim Cryptojacking kapern Cyberkriminelle die Rechenleistung einzelner Benutzer oder die Endgeräte von Unternehmen, um ohne deren Wissen Kryptowährungen zu schürfen.
Für Verbraucher kann diese unbefugte Aktivität zu erhöhten Stromkosten, verminderter Geräteleistung und möglichen Hardwareschäden führen. Zum Schutz vor Cryptojacking empfiehlt sich der Einsatz aktueller Antivirensoftware, regelmäßige System- und Anwendungsupdates sowie die Überwachung von Endgeräten auf ungewöhnliche Leistungsprobleme oder übermäßige Ressourcennutzung.

Nachhaltigkeit beginnt am Endgerät

WARUM UNIFIED ENDPOINT MANAGEMENT NACHHALTIGKEITSZIELE VORANTREIBT

Moderne Unternehmen müssen nicht nur effizient und produktiv arbeiten, sondern auch ihren ökologischen Fußabdruck reduzieren. Was Unified Endpoint Management damit zu tun hat und wie eine zukunftsfähige IT-Strategie aussehen kann, darüber sprach it management mit Sebastian Weber, Head of Product Management bei Aagon.

it management: *Herr Weber, haben Sie eine Zahl parat, wieviel Prozent ihrer Energiekosten Unternehmen sparen können, wenn sie elektronische Endgeräte nicht permanent im Standby-Betrieb betreiben oder über Nacht eingeschaltet lassen?*

Sebastian Weber: Jährlich verbrennen Unternehmen viele tausend Euro, wenn sich PCs, Drucker und andere elektronische Geräte im Standby-Betrieb befinden oder unnötigerweise über Nacht eingeschaltet bleiben. Auch die Niedrig-Watt-Bereiche moderner Geräte summieren sich auf. Aktuellen Schätzungen zufolge lassen sich bis zu 45 Prozent der Energiekosten einsparen, wenn Netzwerk-Devices-Geräte über eine zentrale Instanz wie ein Unified-Endpoint-Management (UEM)-System überwacht und verwaltet werden.

it management: *Welche Maßnahmen gibt es, um die Nutzung von IT-Ressourcen im Unternehmen effizienter zu gestalten?*

Sebastian Weber: Da wären zunächst einmal Virtualisierung, um Hardware besser auszulasten, und Cloud Computing für eine bedarfsgerechte IT-Ressourcen-Nutzung. Im Bereich der Softwareoptimierung helfen eine ressourcen-schonende Programmierung und der Einsatz schlanker Software, weil sie die CPU- und Speicherauslastung senken.

Optimierte Kühlung, stromsparende Komponenten wie SSDs und energieeffiziente Prozessoren sowie die Verlängerung der Lebensdauer von Geräten durch Wartung und Upgrades sind hardwareseitig die klassischen Maßnahmen.

Zu diesen technischen Möglichkeiten gesellen sich organisatorische, in dem man durch klare Kommunikation mit den Beschäftigten dafür sorgt, dass bei Feierabend nicht nur die Monitore abgeschaltet, sondern auch die Rechner entsprechend heruntergefahren werden.

it management: *Welche Rolle können UEM-Systeme in diesem Zusammenhang spielen?*

Sebastian Weber: UEM-Systeme, wie die ACMP Suite von Aagon, tragen in diesem Maßnahmenkatalog wesentlich zur Nachhaltigkeit und Umsetzung einer Green-IT-Strategie bei. Mit ihnen reduziert sich der Energieverbrauch, und die Lebensdauer von Geräten wird verlängert. Weniger Turnschuh-Administration heißt außerdem automatisch auch weniger Reisekosten und damit CO^2-Emissionen.

Durch zentrale Steuerung von Software- und Firmware-Updates über das UEM können diese in einem energieeffizienten Zeitfenster durchgeführt werden, anstatt Geräte unnötig lange laufen zu lassen.

Während früher für Updates manchmal alle Rechner eingeschaltet bleiben sollten, lässt sich das mit einem UEM effizienter und besser lösen. So können die PCs außerhalb der Arbeitszeit gestartet werden, erhalten ihre Updates und werden im Anschluss wieder heruntergefahren. Dies ist in doppelter Hinsicht effizient: nicht nur, dass die PCs damit nicht nur für ein einstündiges Update die ganze Nacht über eingeschaltet bleiben, sondern es kommt auch tagsüber zu weniger Arbeitsunterbrechungen. So ist die Nachhaltigkeit auch in finanzieller Hinsicht zu betrachten. Dadurch gesparte Gelder können beispielsweise wieder in energieeffizientere Hardware investiert werden.

Optimiertes Gerätemanagement bedeutet in diesem Zusammenhang, Energie einzusparen, indem Clients durch effiziente Zuweisung und Wiederverwendung länger nutzbar sind. Administratoren können etwa Energiesparpläne einrichten, Geräte bei Inaktivität automatisch in den Ruhemodus versetzen oder außerhalb der Arbeitszeiten herunterfahren. Alte oder weniger energieeffiziente Geräte werden frühzeitig erkannt und gegebenenfalls durch energieeffizientere Alternativen ersetzt. So gelingt der Übergang zu einer zirkulären IT.

Hierbei unterstützen vor allem die Reporting-Tools einer UEM-Lösung, die mit Hilfe der Inventardaten umfassende Auswertungen über etwa verbaute Netzgeräte liefern können. Unter Zuhilfenahme dieser Daten lässt sich effizient Hardware identifizieren, die näher betrachtet werden sollte, weil sich durch einen Austausch der Energieverbrauch senken ließe.

it management: *Im UEM-System „ACMP" von Aagon gibt es kleine Installationsroutinen, sogenannte Client Commands. Sie haben nun ein solches „Green IT Premium Client Command" entwickelt. Was genau tut es?*

Sebastian Weber: Das Green IT Premium Client Command unterstützt Unternehmen dabei, die Energieeffizienz ihrer IT-Infrastruktur zu steigern und damit Energiekosten zu senken. Es beinhaltet gezielte Steuerungs- und Automatisierungsfunktionen, mit denen sich der Energieverbrauch der Computer im Unternehmensnetzwerk reduzieren lässt.

Zentrale Funktionen sind die Automatisierung von Energieprofilen und die Anpassung der Energieeinstellungen. PCs und Notebooks lassen sich darüber nach einer bestimmten Zeit der Inaktivität in den Ruhezustand oder Standby-Modus versetzen. Auch eine Optimierung der Energieeinstellungen je nach Tageszeit ist möglich. Die Administrationsabteilung kann zum Beispiel energieeffiziente Betriebszeiten definieren, etwa, dass nach Feierabend oder in Pausenzeiten Geräte in den Energiesparmodus wechseln.

Denn es kommt immer wieder vor, dass zu Feierabend die IT-Komponenten nicht alle heruntergefahren, sondern nur in den Standby-Modus versetzt werden.

it management: *Ein Client durchläuft während seines Lebenszyklus verschiedene Stufen. Können Sie erklären, auf welcher dieser Stufen sich ein effizienter Ressourcen-Einsatz umsetzen lässt und wie genau das abläuft?*

Sebastian Weber: Ein effizienter Ressourcen-Einsatz im Sinne von Green IT lässt sich vor allem in der Nutzungsphase des Clients realisieren, wobei natürlich auch Maßnahmen in der Beschaffungsphase, der Wartungs- und der Entsorgungsphase eine Rolle spielen. Während der Nutzungsdauer sind die Potenziale zur Energieeinsparung aber am größten. Dort greifen die bereits beschriebenen Funktionen wie automatisierte Anpassung der Energieeinstellungen, automatisches Ein- und Ausschalten, Virtualisierung und frühzeitiges Erkennen weniger energieeffizienter Geräte.

Neben dem aktiven Energiemanagement während der Nutzung gibt es natürlich noch die Möglichkeit, ausgesonderte Hardware über Refurbish-Dienstleister weiter zu verkaufen und so diese nicht nur zu verschrotten, sondern einem zweiten Nutzungszyklus zuzuführen. Hierbei ist selbstverständlich darauf zu achten, dass Firmendaten vorher sicher entfernt oder die Festplatte ausgetauscht wurde. Nur die Festplatte würde bei diesem Vorgehen verschrottet werden; der Verschrottungsnachweis kann im UEM-System revisionssicher hinterlegt werden.

it management: *Herr Weber, wir danken für dieses Gespräch.*

THANK YOU

UEM-SYSTEME, WIE DIE ACMP SUITE VON AAGON, TRAGEN WESENTLICH ZUR NACHHALTIGKEIT UND UMSETZUNG EINER GREEN-IT-STRATEGIE BEI.

Sebastian Weber, Head of Product Management, Aagon GmbH, www.aagon.com

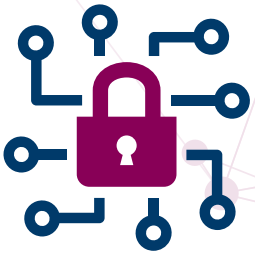
Geplantes Herunter- und Hochfahren sind weitere Maßnahmen für mehr Energieeffizienz, die sich über das Client Command granular einstellen lassen. Diese Flexibilisierung funktioniert nicht nur zeitlich, sondern auch nach Usergruppen. So kann etwa die IT-Abteilung, die eventuell längere Arbeitszeiten hat, andere Energieeinstellungen haben als administrative Abteilungen.

Dadurch ist man nicht auf das Energiebewusstsein des einzelnen angewiesen.

Der Weg zur günstigeren Cyberversicherung

EFFEKTIVE SOAR-ORCHESTRIERUNG DURCH UEM

Durch den Einsatz von UEM erfüllen Unternehmen zentrale Anforderungen von Cyberversicherern und senken gleichzeitig ihre Prämien.



Jeder „normale" Betrieb kann heute gehackt werden. Eine Cyberversicherung bietet zumindest im Nachhinein Schutz vor finanziellen Schäden. Günstiger wird deren Police mit einem SOAR-Konzept, realisiert über eine Unified-Endpoint-Management-Plattform.

Laut Bitkom wurden 2022 neun Zehntel der deutschen Unternehmen Opfer einer Cyberattacke, sei es Datendiebstahl, Spionage oder Sabotage. Die Rolle der organisierten Kriminalität nimmt dabei stetig zu; in Deutschland entsteht dadurch mittlerweile ein Schaden von 203 Milliarden Euro jährlich. Kein Wunder, dass die Versicherungsbranche hier neue Geschäfte wittert. So gibt es mittlerweile spezielle Policen, die Unternehmen vor den finanziellen Folgen eines Cyberangriffes schützen, sogenannte Cyberversicherungen.

Nachfrage nach Versicherungsschutz steigt

Im Visier der Kriminellen sind nicht mehr nur Großorganisationen wie Banken oder Konzerne, sondern jedes Unternehmen ist gefährdet. Auch der Raub von weniger sensiblen Daten kann nämlich Rufschädigung und Schadensersatzansprüche mit sich bringen. Entsprechend groß ist die Nachfrage nach solchen Versicherungen. Sie übernehmen die Kosten für die Untersuchung von Sicherheitsverletzungen ebenso wie das Benachrichtigen von Betroffenen, die Einrichtung von Callcentern für Kundenunterstützung sowie für forensische Analysen und Datenwiederherstellung.

Abgedeckt sind außerdem Haftungsansprüche, die sich aus Verletzungen der Privatsphäre, Verlust oder Diebstahl von Kunden- oder Geschäftsdaten oder anderen Datenschutzverletzungen ergeben. Unterstützung durch IT-Fachleute, Ersatz finanzieller Verluste (durch Betriebsunterbrechung) oder Kostenübernahmen für rechtliche Verteidigung können ebenfalls in den Versicherungsschutz aufgenommen werden.

Voraussetzung für gute Konditionen

Wer diese Leistungen in Anspruch nehmen will, muss allerdings beweisen, dass er sich ihrer als würdig erweist. Sonst lässt die Versicherung im Zweifel nämlich besser die Finger davon oder aber die Police wird unverhältnismäßig teuer. Konkret: Wurde vorgebeugt? Hat das Unternehmen schon Cybersecurity-Maßnahmen wie Firewalls, Verschlüsselung, regelmäßige Sicherheitsüberprüfungen oder Beschäftigten-Schulungen implementiert? Gab es bereits frühere Sicherheitsverletzungen und Datenverluste? Aus welcher Branche kommt der potenzielle Kunde, wie sehen Umsatz und Jahresgewinn aus, wie hoch sollen Deckungssumme und Selbstbeteiligung sein?

All diese Punkte klappert eine Versicherung ab und bemisst danach die Prämie.

Wer also nachweist, bereits im Vorfeld das maximal Mögliche zum Schutz der eigenen IT getan zu haben – das heißt ein robustes Security Orchestration, Automation and Response (SOAR)-Konzept implementiert zu haben – hat definitiv bessere Karten. Ein solches Konzept bietet effektiven Schutz vor Cyberkriminalität, ermöglicht schnellere Reaktionszeiten, reduziert menschliche Fehler und verbesserte Bedrohungserkennung. Dank Automatisierung werden Schwachstellen und Einfallstore frühzeitig entdeckt und geschlossen. Administrative Aufgaben, die bei der Umsetzung von Sicherheitsmaßnahmen anfallen, lassen sich effizient und wirksam bewältigen.

Genau das, was Versicherungen fordern

Über Unified Endpoint Management (UEM)-Lösungen wie die ACMP Suite von Aagon lässt sich genau diese Orchestration erreichen und ein SOAR-Konzept damit wirkungsvoll umsetzen. Sicherheitsmaßnahmen werden zentral verwaltet und automatisiert. Verschiedene Module wie Defender Management, Schwachstellenmanagement, Bitlocker Management, Managed Software, automatisiertes Windows-Update-Management und Desktop Automation greifen dabei ineinander.

Informationen zu potenziellen Gefahren werden kontinuierlich gesammelt und analysiert – durch automatisierte Scans und Updates von Clients, automatische Verschiebung von Clients in vordefinierte Filter, Identifizierung, Bewertung, Priorisierung und Bereitstellung von Patches erhalten Unternehmen jederzeit einen aktuellen Blick auf die digitale Bedrohungslage – genau das, was Versicherungen fordern. Jetzt SOAR umsetzen heißt also später: Sparen bei der Prämie für die neue Cyberversicherung.

www.aagon.com

IT und Nachhaltigkeit

SO GELINGT EFFIZIENTES CO_2-MANAGEMENT

Nicht nur aus Compliance-Gründen, sondern auch aus eigener Verantwortung wollen viele Unternehmen nachhaltiger werden. Der übliche Wert, um die Fortschritte konkret zu messen, ist der sogenannte Corporate Carbon Footprint (CCF), also die CO_2-Bilanz. Sie erfasst alle relevanten Treibhausgasemissionen innerhalb eines bestimmten Zeitraums, meist eines Jahres. Diese werden nach dem Scopes-Modell eingeteilt:

- **Scope 1:** Direkt in eigenen Anlagen erzeugte Emissionen
- **Scope 2:** Indirekte Emissionen aus bezogener Energie, wie Elektrizität und Fernwärme
- **Scope 3:** Weitere vor- und nachgelagerte indirekte Emissionen, etwa aus Geschäftsreisen oder der Lieferkette

In vielen Unternehmen erhöhen vor allem Reisetätigkeiten und der Energieverbrauch von Rechenzentren den CCF. So benötigen die rund 50.000 Data Center in Deutschland heute zehnmal mehr Energie als vor zehn Jahren – und mehr als die ganze Stadt Berlin. Diese Steigerungsrate wird sich in den kommenden Jahren noch deutlich verstärken, insbesondere durch den Einsatz von Künstlicher Intelligenz und ihrer intensiven Datenverarbeitung.

Drei wichtige Schritte

Um die Auswirkungen ihrer Tätigkeiten auf den CCF messen zu können, benötigen Unternehmen geeignete Tools. Sie helfen dabei, einen aktuellen Ist-Zustand der unternehmerischen Emission zu ermitteln sowie geeignete Reduktionsmaßnahmen festzulegen, zu priorisieren und umzusetzen.

UM DIE AUSWIRKUNGEN IHRER TÄTIGKEITEN AUF DEN CCF MESSEN ZU KÖNNEN, BENÖTIGEN UNTERNEHMEN GEEIGNETE TOOLS.

Lennard Everwien, Head of Business Sustainability, Campana & Schott, www.campana-schott.de

Der erste Schritt besteht aus einer tiefgehenden Gap-Analyse. Hier werden alle Datenquellen identifiziert, Daten erhoben und quantifiziert. Es ist wichtig hier alle relevanten Stakeholder im Unternehmen mit einzubeziehen, um das Vorgehen und die Verantwortlichkeiten früh zu verankern. Nach der Gap Analyse hat das Unternehmen ein gutes Bild ihrer Emissionsdaten und kennt optimalerweise interne sowie externe Datenquellen dieser Emissionsdaten.

Der zweite Schritt besteht darin, ein geeignetes Tool zu finden, um die bestehenden Datenquellen automatisiert anzubinden und die CCF-Berechnung dadurch effizient ausführen zu können. Es gibt aktuell eine Vielzahl an ESG-Tools auf dem Markt, die unterschiedliche Herausforderungen angehen. Neben Tools zur Unterstützung der Berichterstattung nach CSRD, gibt es spezialisierte Tools zur Nachverfolgbarkeit der Lieferkette oder zur Umsetzung der EU-Taxonomie. Und es gibt eben auch Plattformen, die sich auf die Messung des CCF fokussieren.

Die Rohdaten die im ersten Schritt manuell gesammelt wurden können jetzt effizient in das ausgewählte Tool hochgeladen werden. Zusätzlich können Schnittstellen mit anderen Systemen in Unternehmen identifizieret und erstellt werden. Daten können somit automatisch aus bestehenden Anwendungen importiert, abgeglichen und bearbeiten werden. Die Daten werden durch eingebaute Kontrollen im Tool verglichen. Nach dem einmaligen Aufsetzen der Datenarchitektur können Mitarbeitende die Ergebnisse kontrollieren und bei Bedarf anpassen. Mit solchen Tools für das CCF-Management lassen sich die Emissionen in Bezug auf Scope 1 bis 3 auch kontinuierlich erfassen, analysieren und verbessern.

Im dritten Schritt sind konkrete Nachhaltigkeitsmaßnahmen festzulegen, deren Umsetzung zu steuern und zu verwalten. Hierfür lassen sich spezialisierte Portfoliomanagement-Anwendungen einsetzen. Sie verbessern die Transparenz und erleichtern das Umsetzen von Synergien zwischen verschiedenen Maßnahmen. Aufgrund des Maßnahmenkatalogs kann das Unternehmen dann ihre Nachhaltigkeitsstrategie und Emissionsreduktionsziele informiert aufsetzen.

Konkrete Herausforderungen erfüllen

Durch diesen Überblick wird schon klar, dass der Einsatz einer Software nie ein Selbstzweck sein, sondern konkrete Probleme lösen sollte. Deshalb muss eine geeignete Anwendung folgende Herausforderungen im Emissionsmanagement meistern können:

#1 Erfassung und Integration von Daten.

Die Erfassung von Emissionsdaten aus den unterschiedlichen Quellen und deren Integration in ein zentrales System ist häufig komplex und zeitaufwändig. Geeignete Softwarelösungen müssen daher Schnittstellen zur automatischen Datenerfassung und -integration aufweisen. Dann können sie Rohdaten aus verschiedenen Quellen – etwa zu Energieverbrauch, Logistik- und Lieferketten oder Reiseaufwand – sammeln und in einem zentralen System konsolidieren. Das minimiert den manuellen Aufwand und erhöht die Datenkonsistenz.

#2 Genaue, zuverlässige Daten.

Falsche, ungenaue oder unvollständige Rohdaten können zu fehlerhaften Emissionsberichten führen. Das beeinträchtigt die Entscheidungsfindung und die Compliance. Das richtige Tool bietet präzise Erfassungs- und Prüfmethoden, um die Genauigkeit und Zuverlässigkeit der Daten sicherzustellen. Bei Bedarf kann eine Echtzeit-Datenanalyse dabei unterstützen, Fehler frühzeitig zu erkennen und zu beheben.

#3 Komplexe Scope-3-Emissionen.

Besonders schwierig ist häufig die Berechnung der Scope-3-Emissionen aus indirekten Quellen entlang der gesamten Wertschöpfungskette. Dies erfordert umfangreiche Daten von Lieferanten und anderen Partnern. Zudem sind sie oft schwer zu quantifizieren. Spezialisierte Lösungen helfen bei der Erfassung und Analyse von Scope-3-Emissionen durch integrative Methoden und Datenbanken. Sie bieten Transparenz entlang der gesamten Lieferkette und unterstützen die Nachverfolgung und Berichterstattung.

#4 Compliance gewährleisten.

Die Einhaltung nationaler und internationaler Vorschriften für Nachhaltigkeit wird immer komplexer. Unternehmen benötigen hier kontinuierliche Updates und regelkonforme Reports. Entsprechende Anwendungen müssen daher stets auf dem neuesten Stand der gesetzlichen Anforderungen bleiben, damit Unternehmen die Compliance-Vorgaben erfüllen und Berichte für Behörden und Stakeholder erstellen können. Dabei sollten sie automatisierte Prüf- und Freigabe-Prozesse unterstützen.

#5 Kosten und Ressourceneinsatz minimieren.

Aufbau und Betrieb eines effektiven Systems für das Emissionsmanagement können kosten- und ressourcenintensiv sein. Der Aufwand lässt sich durch Software mit Hilfe von Automatisierung und Effizienzsteigerung reduzieren. Zusätzlich ermöglicht die genaue Datenanalyse eine bessere Kostenkontrolle und Erkennung von Einsparpotenzialen.

#6 Hohe Transparenz und klare Kommunikation.

Eine nachvollziehbare Kommunikation der Emissionsdaten und CCF-Maßnahmen gegenüber internen und externen Stakeholdern ist oft schwierig, aber erfolgsentscheidend. Benutzerfreundliche Dashboards und Berichtsformate ermöglichen eine klare und transparente Darstellung der Informationen. Dies erleichtert die Kommunikation mit Mitarbeitenden, Kunden, Investoren und Regulierungsbehörden.

#7 Kontinuierliche Verbesserungen.

Unternehmen müssen ständig nach neuen Wegen suchen, um ihre Emissionen zu reduzieren und nachhaltiger zu wirtschaften. Dies erfordert kontinuierliche Innovationen und Anpassungen. Speziallösungen bieten dafür praktische Analysefunktionen und Empfehlungen anhand bewährter Prozesse. Unternehmen können damit einfacher und effizienter neue Strategien zur CCF-Reduktion entwickeln und umsetzen.

Fazit

Softwarelösungen für das Emissionsmanagement müssen zahlreiche Anforderungen erfüllen. Entscheidend sind jedoch vordefinierte Schnittstellen zur Integration mit bestehenden Systemen sowie eine hohe Anpassungsfähigkeit. Denn jedes Unternehmen ist anders und verändert sich ständig. Erfahrene Partner helfen sowohl bei der Daten-Gap Analyse als auch bei der Tool-Auswahl und der individuellen Planung und Umsetzung.

Lennard Everwien

Datenflut im DBMS

OHNE HILFE VON KI UND AUTOMATISIERUNG GEHEN DATENBANKADMINISTRATOREN UNTER

Exponentiell wachsende Datenmengen übersteigen längst die manuellen Verwaltungskapazitäten. Doch moderne KI-gestützte Automatisierungslösungen versprechen Entlastung. Wie genau das funktioniert und welche Aspekte es zu beachten gilt, darüber sprach it management mit Oliver Stein, Redgate Software.

it management: *Redgate hat zwar gerade erst damit begonnen, sich im DACH-Raum einen Namen zu machen, international ist das Unternehmen allerdings bereits sehr erfolgreich und dessen Produkte weit verbreitet. Können Sie uns Redgate vielleicht kurz vorstellen?*

Oliver Stein: Aber sicher, Redgate hat sich mit seinen Tools dem Ziel verschrieben, das Management der immer komplexeren Datenbank-Infrastrukturen zu vereinfachen – und somit das Leben von Datenbankentwicklern und -administratoren zu erleichtern. Oft stoßen Datenbank-Teams an ihre Grenzen und werden für Unternehmen so zum Showstopper. Die Folge: Geschäftsdaten lassen sich nicht mehr gewinnbringend nutzen und die Softwareentwicklung verläuft weniger effizient.

Das liegt häufig daran, dass heute nicht mehr nur eine einzige Datenbankplattform, sondern teilweise über fünf unterschiedliche im Einsatz sind. Zudem erfolgt das Hosting nicht mehr ausschließlich on-premises. Stattdessen sind verschiedene Cloud-Szenarien weit verbreitet und nehmen weiter zu. Auch die Menge an Daten, die Unternehmen erheben, sammeln und speichern müssen, wächst kontinuierlich. Um effizient zu bleiben, Fehler zu vermeiden und geschäftskritische sowie sensible Daten zu schützen, benötigen selbst erfahrene Datenbankexperten bei ihrer täglichen Arbeit Unterstützung. Die liefern wir seit 25 Jahren in Form intuitiver und leicht bedienbarer Tools für erfolgreiches End-to-End Database DevOps.

it management: *End-to-End Database DevOps klingt spannend. Was genau steckt hinter dem Konzept?*

Oliver Stein: Das DevOps-Konzept hat sich in der Softwareentwicklung bereits etabliert. Dieses Modell lässt sich auch erfolgreich auf eine Datenbanklandschaft anwenden. Dafür bieten wir eine Reihe von Lösungen an, die alle einen End-to-End-Ansatz unterstützen. Dieser Ansatz deckt den gesamten Database-DevOps-Lebenszyklus ab – von der agilen Planung über kontinuierliches Testen bis hin zu CI/CD-Automatisierung und KI-gesteuerten Release-Einblicken, um Innovationen zu beschleunigen und gleichzeitig Geschäftsrisiken zu reduzieren. Wichtige Aspekte sind dabei die Automatisierung von Prozessen, etwa das Testen von Datenbankversionen, bevor sie mit dem Live-System zusammengeführt werden, oder Quality-Checks. Zudem können viele Unit- und Integrationstests von unseren Nutzern automatisiert werden. Das Gute: Unsere Lösungen lassen sich hervorragend mit existierenden Tool-Sets kombinieren, die im DevOps-Bereich weit verbreitet sind, darunter Jenkins, GitHub, TeamCity um nur ein paar Beispiele zu nennen. Darüber hinaus unterstützen wir mehr als 30 verschiedene Datenbanktypen.

it management: *Der Schutz von Daten und Datenbanken ist für viele Unternehmen eine zentrale Aufgabe. Wie kann Redgate sie in diesem Bereich unterstützen?*

UNTERNEHMEN SOLLTEN MEHR IN IHRE MITARBEITENDEN INVESTIEREN UND EIN UMFELD SCHAFFEN, DAS DEN AUSTAUSCH VON WISSEN FÖRDERT.

Oliver Stein, Geschäftsführer DACH, Redgate Software, www.red-gate.com/de

Oliver Stein: Durch die Automatisierung von Prozessen können IT-Teams Fehler vermeiden, die sich bei manueller Durchführung einschleichen. Natürlich müssen die entsprechenden Skripte – etwa zur Datenbankmigration – fehlerfrei sein. Automatisiertes Testing reduziert zudem Sicherheitslücken und steigert die Zuverlässigkeit von Datenbanken sowie die Qualität. Unsere Lösungen bieten überdies automatisierte Data Discovery, also das Aufdecken von Mustern und Erkennungsmerkmalen in Datensätzen, sowie Klassifizierung und helfen so bei der Datenanalyse. Auch automatisiertes Masking, also die Anonymisierung der Daten, ist Teil des Funktionsumfangs, sodass sensible Informationen bestens geschützt sind. Darüber hinaus helfen wir Administratoren dabei, den Überblick über die Zugriffsrechte der Mitarbeitenden auf die Datenbanken zu behalten. Sie können mit unseren Tools vergangene und aktuelle Zugriffsrechte nachverfolgen und feingranular die Berechtigungen erteilen.

it management: *Monitoring ist ein weiterer wichtiger Aspekt Ihres Portfolios. Welche Einblicke gewähren die Lö-*

sungen von Redgate in die Datenbankinfrastruktur und wie helfen sie den Database-DevOps-Teams?

Oliver Stein: Viele Hersteller bieten Monitoring-Lösungen, die zwar hervorragende, jedoch oft nur isolierte Ergebnisse liefern. Sie können die CPU-Auslastung überprüfen und zeigen an, wann sie extrem hoch war. Betrachtet man diese Informationen unabhängig von anderen relevanten Daten, sind sie nicht besonders aussagekräftig. Redgate hingegen bietet eine holistische Sicht auf die gesamte SQL-Server- und PostgreSQL-Umgebung. Nutzer können so nicht nur feststellen, ob irgendwo ein Performance-Problem auftritt, sondern es auch in zeitlichen Kontext zu anderen Datenbankoperationen stellen. Ein weiterer Vorteil ist das zentrale, übersichtliche Dashboard, das alle wichtigen Informationen an einem Ort vereint. Die detaillierten und differenzierten Einblicke helfen Unternehmen dabei, potenzielle Risiken und Probleme zu lösen bevor sie akut werden. Zudem können Administratoren individuelle Alerts konfigurieren, die auf ihre spezifische Datenbanklandschaft zugeschnitten sind. Im Gegensatz dazu bieten viele Tools anderer Anbieter häufig nur Standardwarnungen.

? **it management:** *Welche Rolle spielt Automatisierung im Datenbankkontext?*

Oliver Stein: Automatisierung spielt eine entscheidende Rolle, insbesondere angesichts der zunehmenden Komplexität der Datenbanklandschaften und des Fachkräftemangels. Unternehmen haben daher kaum eine andere Wahl, als die Automatisierung ihrer Systeme und Prozesse voranzutreiben. Datenbankadministratoren bleibt heute oft keine Zeit mehr, um die Auslastung der Datenbankserver kontinuierlich zu überwachen oder Tests durchzuführen.

? **it management:** *Künstliche Intelligenz (KI) hat sich zu einem wesentlichen Bestandteil vieler Lösungen für Entwickler und Administratoren entwickelt. Profitieren davon auch Datenbank-Tools?*

Oliver Stein: Mit zunehmender Verbreitung von generativer KI (GenAI) und Machine Learning werden auch im Datenbankkontext immer mehr Aufgaben wie die prädiktive Datenbankanalyse oder die Code-Generierung von generativen KI-Bots übernommen. In den kommenden Jahren wird sich in diesem Bereich viel verändern, doch bis KI als Standard-Tool etabliert ist, wird es sicher noch einige Zeit dauern. Laut unserer Studie „State of the Database Landscape" setzen Nutzer KI heute vor allem zur Analyse sowie zur Optimierung von Querys und Quellcodes ihrer Datenbanken ein. Viele Anwender nutzen die Technologie auch für die Automatisierung von Testszenarien.

? **it management:** *Zum Abschluss werfen wir einen Blick in die Glaskugel: Wie wird sich der Markt für Datenbanken und die Art und Weise, wie wir Daten speichern, sichern und überwachen in den kommenden Jahren entwickeln?*

Oliver Stein: Mit ziemlicher Sicherheit wird der Einsatz von KI-Tools zunehmen. Die steigende Komplexität der Datenbankinfrastrukturen und der dadurch verschärfte Skill Gap wie auch der weiter anhaltende Fachkräftemangel machen diese Entwicklung unvermeidlich.

Die schiere Menge an Daten, die täglich gesammelt wird, explodiert regelrecht und wird dadurch auch immer komplexer. Das erfordert einen kulturellen Wandel innerhalb von Unternehmen. Sie müssen einerseits mehr auf DevOps setzen und andererseits – wo sinnvoll und möglich – Automatisierung durch die Integration neuer Technologien wie KI oder Machine Learning fest in ihren Workflows verankern. Unternehmen sollten mehr in ihre Mitarbeitenden investieren und ein Umfeld schaffen, das den Austausch von Wissen fördert. Nur so können sie die zukünftigen Herausforderungen erfolgreich bewältigen.

! **it management:** *Herr Stein, wir danken für dieses Gespräch.*

Cybersicherheit

STRATEGIEN, PROZESSE UND PRIORITÄTEN

Cybersicherheit ist keine „one fits it all"-Lösung. Sie ist vielmehr eine technische Herausforderung, die heute einen ganzheitlichen Sicherheitsansatz erfordert – angefangen bei der Mitarbeitersensibilisierung über Lieferkettensicherheit bis zur Erfüllung gesetzlicher Anforderungen. Über diese Herausforderungen sprachen wir mit Martin Stephan, Informationssicherheitsbeauftragter bei TOPdesk.

it management: *Wie hat sich das Bedrohungsbild der Cybersicherheit in den letzten Jahren entwickelt? Welche neuen Herausforderungen beobachten Sie?*

Martin Stephan: Es ist zunächst einmal größer geworden. Viele Tools und Kurse zum Thema Hacking sind frei verfügbar. Aufgrund von Corona sind viel mehr Dienste in die Cloud gewandert und mehr Menschen nutzen diese Dienste. Dadurch ist die Zahl der potenziellen Opfer gestiegen, was wiederum attraktiver ist für Menschen, die sich dadurch Profit erhoffen. Dies gilt für legale wie auch illegale Methoden.

it management: *Könnten Sie uns einen Überblick über Ihre Rolle als Informationssicherheitsbeauftragter bei TOPdesk geben? Welche Prioritäten setzen Sie in Bezug auf Cybersicherheit?*

Martin Stephan: Ganz grob kann man sagen, dass ich in Absprache mit Fachabteilungen und anderen Standorten Sicherheitsmaßnahmen plane, deren Umsetzung prüfe und darüber hinaus auf die Erfüllung gesetzlicher Anforderungen achte sowie Fragen von Kunden zu diesem Thema beantworte. Stichwort: Lieferkette.

Wo beginnt Cybersicherheit? Erst wenn jemand sich unerlaubt Zugriff verschafft zu einem System, oder wenn sich diese Person in einem sozialen Netzwerk mit einem Kollegen oder einer Kollegin anfreundet?

Insofern betrachte ich das Thema lieber ganzheitlich im Rahmen der Informationssicherheit.

it management: *NIS2 ist ein zentrales Thema in der aktuellen Cybersicherheitslandschaft. Wie wirkt sich die neue Richtlinie auf TOPdesk und seine Kunden aus?*

Martin Stephan: Erstmal ist die konkrete Umsetzung in Deutschland vermutlich frustrierend. Die unscharfe Definition des MSP wird oft kritisiert. Auch hat der Bundesrechnungshof gerade erst scharfe Kritik geübt. Es besteht also noch Verbesserungspotenzial. Da wir uns intern an der ISO 27001 orientieren und die Rechenzentren SOC2-zertifiziert sind, hatten wir vieles bereits umgesetzt oder auf dem Schirm. Unsere Kunden möchten wir dabei gerne unterstützen. TOPdesk eignet sich hervorragend, um darin den Plan-Do-Check-Act-Zyklus abzubilden.

BESORGEN SIE SICH EXTERNE HILFE, WENN INFORMATIONSSICHERHEIT UND RISIKOMANAGEMENT BISHER „NUR" NEBENBEI LIEFEN.

Martin Stephan, Informationssicherheitsbeauftragter, TOPdesk, www.topdesk.com

it management: *Welche konkreten Maßnahmen müssen Unternehmen im Rahmen von NIS2 ergreifen, um den Sicherheitsanforderungen gerecht zu werden?*

Martin Stephan: Die konkreten Maßnahmen müssen sich nach den Bedürfnissen und Risiken des jeweiligen Unternehmens richten.

it management: *Wie stellt TOPdesk sicher, dass es die Compliance-Anforderungen von NIS2 und ähnlichen Regulierungen erfüllt?*

Martin Stephan: Das ist tatsächlich in das Konzept eingebaut. Der Plan-Do-Check-Act-Zyklus sieht vor, dass man auf geeignete Art und Weise überprüft, ob gewählte Maßnahmen (Plan) umgesetzt wurden (Do) wie geplant und die gewünschte Wirkung entfalten (Check). Ist das nicht der Fall, muss nachgebessert werden (Act).

Wir verwenden als Maßnahme, um die Awareness unserer Mitarbeiter zu erhöhen und das Risiko zu senken, dass einer unserer Kollegen durch eine Phishing-Mail zum Narren gehalten wird, eine Schulungsplattform. Um die Effektivität zu prüfen, werden regelmäßig unsere eigenen (ungefährlichen) Phishing-Mails verschickt. Die Abdeckung stellen wir sicher, indem Kollegen, die ihre Lerneinheiten nicht regelmäßig ausführen, nach einer gewissen Zeit von fast allen Systemen ausgesperrt werden.

it management: *Welche Technologien oder Prozesse erachten Sie als besonders effektiv, um Bedrohungen im Bereich der Cybersicherheit zu begegnen?*

Martin Stephan: Zunächst muss man dafür ein Bewusstsein bei allen Mitarbeitern auf allen Ebenen schaffen und dann müssen die gewählten Maßnahmen hinsichtlich ihrer Wirksamkeit regelmäßig überprüft werden.

it management: *Wie können Unternehmen sicherstellen, dass sie ihre Cybersicherheitsinfrastruktur angesichts des schnellen technologischen Wandels auf dem neuesten Stand halten?*

Martin Stephan: Hier gibt es leider kein „One-Size-Fits-All". Der Aufwand muss wirtschaftlich sinnvoll sein, sofern Wirtschaftlichkeit ein relevantes Kriterium ist.

it management: *Wie gehen Sie bei TOPdesk mit der Herausforderung der Integration von Sicherheitslösungen in die bestehende IT-Landschaft um?*

Martin Stephan: Ich sehe das weniger als technische Herausforderung, eher als menschliche. Die Menschen müssen abgeholt werden und man muss ihnen die Ängste nehmen. Veränderung ist immer auch etwas mühsam.

it management: *Wie fördern Sie bei TOPdesk eine Sicherheitskultur, um sicherzustellen, dass Cybersicherheit nicht nur eine technologische, sondern auch eine unternehmensweite Priorität ist?*

Martin Stephan: Wir fördern unsere Sicherheitskultur zunächst einmal indem die Geschäftsführung sie zu einer unternehmensweiten Priorität gemacht hat. Die Schulungen zu dem Thema sind für alle verpflichtend und wir unterstützen unsere Führungskräfte dabei, als Vorbilder agieren zu können.

it management: *Welche zukünftigen Entwicklungen im Bereich Cybersicherheit sehen Sie auf uns zukommen?*

Martin Stephan: Ich gehe davon aus, dass man in einigen Bereichen zu On-Premises-Lösungen zurückkehren wird, um wieder die Datenhoheit zu haben und – vielleicht viel relevanter – mühsamen Prüfungen der Lieferkette zu entgehen. Der Digital Operational Resilience Act (DORA) fordert dies bereits. Gleichzeitig werden mehr Unternehmen eine ISO 27001-Zertifizierung anstreben.

Ich denke, zumindest in einigen Bereichen wird sich auch die Haftung in Bezug auf Softwarefehler verschärfen. Dadurch wird hoffentlich die gesamte Softwarelandschaft langfristig sicherer.

it management: *Wie schätzen Sie die Bedeutung von Cybersicherheitsstandards in den nächsten Jahren ein, insbesondere in Bezug auf die Vermeidung von Cyberattacken?*

Martin Stephan: Ich gehe stark davon aus, dass die ISO 27001 als Standard für Informationssicherheit stark an Bedeutung gewinnt. Wer diese bereits heute umsetzt, hat lediglich die Spezifizierungen von NIS2 oder DORA umzusetzen.

Man wird dadurch allerdings keine Cyberangriffe vermeiden, nur den potenziellen Schaden verhindern, verringern oder zumindest geplant managen können.

it management: *Welchen Rat würden Sie anderen Unternehmen geben, die mit der Umsetzung von NIS2 und anderen Sicherheitsanforderungen konfrontiert sind?*

Martin Stephan: Gehen Sie davon aus, dass das ein Führungsthema ist, und besorgen Sie sich externe Hilfe, wenn Informationssicherheit und Risikomanagement bisher „nur" nebenbei liefen. Es mag merkwürdig klingen, aber das ist kein originäres IT-Problem.

it management: *Wie unterstützt TOPdesk seine Kunden dabei, ihre eigenen Sicherheitsanforderungen zu erfüllen und Cybersicherheitsrisiken zu minimieren?*

Martin Stephan: Nun, aus meiner Sicht – und ich bin da klar vorbelastet - lässt sich der Plan-Do-Check-Act-Zyklus wunderbar abbilden mit der Knowledge Base (Plan), Incidents und Assets (Do), Operativen Aktivitäten und Serien (Check) und Changes (Act). TOPdesk kann ein sehr gutes ISMS sein.

it management: *Herr Stephan, wir danken für dieses Gespräch.*

IN DIE CLOUD? ABER SOUVERÄN!

BEHALTEN SIE DIE KONTROLLE ÜBER IHRE DATEN

Die Cloud ermöglicht auf vielen Ebenen neue Business-Potenziale und Synergieeffekte. Dennoch steht der Einsatz der Cloud vor einer entscheidenden Herausforderung: der Wahrung der Datensouveränität.

Datensouveränität bedeutet, dass ein Unternehmen jederzeit die vollständige Kontrolle und Hoheit über seine Daten behält – unabhängig davon, wo diese gespeichert oder verarbeitet werden. Doch insbesondere bei sensiblen Daten wird genau diese Kontrolle häufig in Frage gestellt, wenn die Verantwortung für den Betrieb und die Datenhaltung teilweise oder ganz an einen Cloud Provider übertragen wird.

Was können Unternehmen tun, um sicherzustellen, dass sie die volle Kontrolle über ihre Daten in der Cloud behalten?

Dieses Whitepaper gibt Antworten darauf und zeigt, warum Datensouveränität in der Cloud so wichtig ist, wie Sie diese erfolgreich in Ihrem Unternehmen umsetzen können und welche Gesetze und Richtlinien Sie unbedingt kennen sollten.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 9 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/download

Die NIS2-Richtlinie der Europäischen Union

WELCHE BEDEUTUNG HAT SIE FÜR MITTELSTÄNDISCHE UNTERNEHMEN?

In den letzten Jahren hat die Europäische Union (EU) ihre Bemühungen zur Verbesserung der Cybersicherheit in der Union verstärkt und dazu verschiedene Regularien auf den Weg gebracht. Ein entscheidender Schritt in diese Richtung ist die NIS2-Richtlinie. Im Folgenden geht es um einen genaueren Blick auf die NIS2-Richtlinie und ihre Auswirkungen auf mittelständische Unternehmen in der EU.

Überblick über die NIS2-Richtlinie

Die NIS2-Richtlinie baut auf den Grundlagen der ersten Version auf, zielt jedoch darauf ab, die Sicherheitsanforderungen für mittelständische Unternehmen zu verschärfen und den Schutz kritischer Infrastrukturen zu verbessern. Die Mitgliedsstaaten der EU müssen die NIS2-Richtlinie in Form von Umsetzungsgesetzen in nationales Recht überführen.

Geltungsbereich und betroffene Sektoren

Im Vergleich zur vorherigen Version umfasst die NIS2-Richtlinie nun ein breiteres Spektrum an Sektoren, darunter Energie, Gesundheit, Finanzwesen, Cloud-Dienste, soziale Netzwerke und weitere. Grundsätzlich gilt: Unternehmen, die in einem der Sektoren tätig sind und die mindestens 50 Mitarbeitende haben oder einen Jahresumsatz von mehr als 10 Millionen Euro aufweisen, können in den Anwendungsbereich der NIS2-Richtlinie fallen. Unterschieden wird zwischen besonders wichtigen bzw. wesentlichen (auch KRITIS-Betreiber) und wichtigen Einrichtungen mit differenzierten Anforderungen.

Anforderungen

Unter der NIS2-Richtlinie müssen Unternehmen des Mittelstands eine Reihe von Anforderungen erfüllen, um ihre Netz- und Informationssicherheit zu verbessern. Sie lassen sich im Wesentlichen in das Risikomanagement und organisatorische Aufgaben aufteilen.

Zum Risikomanagement wird die Implementierung von wirksamen technischen und organisatorischen Maßnahmen aus zehn Bereichen gefordert. Der Großteil dieser Themen wird durch die Einführung eines Informationssicherheitsmanagementsystems (ISMS) abgedeckt. Die organisatorischen Aufgaben umfassen Meldepflichten, Unterrichtungspflichten, Pflichten für die Geschäftsführung, Nachweispflichten sowie Registrierungspflichten.

Praktische Auswirkungen auf mittelständische Unternehmen

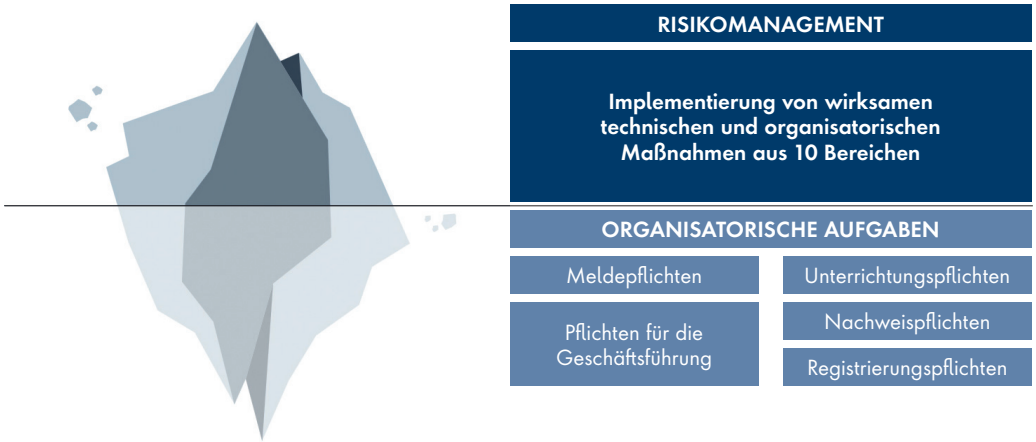
Die Einhaltung der NIS2-Richtlinie erfordert von mittelständischen Unternehmen eine sorgfältige Vorbereitung und Planung sowie möglicherweise Investitionen in neue Technologien. Bei Nichteinhaltung der Umsetzungsgesetze drohen Bußgelder. Trotz dieser Herausforderungen bietet die Compliance erhebliche Vorteile, darunter einen verbesserten Schutz vor Cyberangriffen und ein gestärktes Vertrauen der Kunden und Geschäftspartner. Mittelständische Unternehmen, die proaktiv auf die neuen Anforderungen reagieren, können ihre Wettbewerbsfähigkeit und Resilienz erheblich steigern.

Fazit und Ausblick

Die NIS2-Richtlinie hat weitreichende Auswirkungen auf mittelständische Unternehmen in der Europäischen Union, insbesondere auf diejenigen, die kritische Dienste bereitstellen. Die verschärften Sicherheitsanforderungen stellen eine Herausforderung dar, eröffnen jedoch auch die Möglichkeit, die Resilienz gegenüber Cyberbedrohungen zu stärken.

Die NIS2-Richtlinie ist ein bedeutender Schritt in Richtung einer sichereren digitalen Infrastruktur. Verzögerungen in der Umsetzung der Mitgliedsstaaten verschaffen mittelständischen Unternehmen zusätzliche Vorbereitungszeit. Eine koordinierte Herangehensweise an Cybersicherheit ist entscheidend.

Dr. Kai A. Simon, Nikolas Strommenger
www.kobaltblau.com/de



kobaltblau
Management Consultants

Das Fundament für die digital-vernetzte Zukunft

OFFENE ERP-SOFTWARE FÜR MEHR EFFIZIENZ

Gerade in konjunkturell schwächeren Phasen fällt den mittelständischen Produktions- und Engineering-Unternehmen aus dem Umfeld der Losgröße 1+ eine besondere volkswirtschaftliche Rolle zu. Sie sind zusammengerechnet nicht nur einer der größten Arbeitgeber in Deutschland, sondern wegen ihrer technologischen Innovationskraft zugleich einer der Antriebe der wirtschaftlichen Entwicklung. Auch wenn sie sich in ihrer branchenindividuellen Ausrichtung voneinander unterscheiden, sind sich Maschinen-, Anlagen-, und Apparatebauer, Werkzeug- und Formenbauer, Stahl-, Holz- und Industriebauer sowie Schiffs- und Sonderfahrzeugbauer bei der Abwicklung ihres zumeist komplexen Projektgeschäfts häufig sehr ähnlich. Bei der Bewältigung ihrer anspruchsvollen Aufgaben besitzen diese Unternehmen besondere Fähigkeiten und stellen infolgedessen hohe Anforderungen an die von ihnen eingesetzte Geschäftssoftware für das Enterprise Ressource Planning (ERP). Vor allem deshalb, weil sie im Zentrum der Digitalisierung steht.

Prozesse durchgängig gestalten

Bezüglich ERP-Software geht es um mehr als um deren reinen Funktionsumfang und die Abbildung branchenspezifischer Funktionalitäten, die den hochspezialisierten Mittelständlern nur die wenigsten Systeme bieten. Vielmehr benötigen sie Datendrehscheiben mit offenen Architekturen, die in der Lage sind, verschiedenste Datenquellen, Drittsysteme, Maschinen- und Gerätetypen unkompliziert zu integrieren. Denn nur so wird es möglich, Prozesse durchgängig zu gestalten, effizientere Abläufe zu etablieren und Partner, Kunden und Lieferanten einzubeziehen. Nur so sind innovative Service-Modelle überhaupt erst denkbar. Flexible, integrationsfähige ERP-Plattformen bilden das Fundament für Vernetzung, Automatisierung und Digitalisierung.

Ein Bereich, in dem die intelligente Vernetzung verschiedener Komponenten gut sichtbar für mehr Automatisierung sorgt, ist die vorausschauende Wartung (Predictive Maintenance). Sensorisch erfasste Maschinendaten werden in einem wohl abgestimmten Szenario über eine performante API an das ERP-System übergeben und dort verarbeitet. Die kontinuierliche Analyse der eingehenden Massendaten versetzt Maschinenbetreiber in die Lage, im Bedarfsfall automatisiert und in Echtzeit vordefinierte Prozesse und Workflows auszulösen – zum Beispiel Instandhaltungsmitteilungen und -maßnahmen. Ebenso können die Maschinenbauer ihren Kunden neuartige und individuell angepasste Service- und Wartungsmodelle anbieten, etwa im Rahmen von turnusmäßigen Abonnements oder orientiert an der tatsächlichen Maschinenleistung (Verschleiß).

Predictive Maintenance als Einstieg in die Welt der KI

Damit ist Predictive Maintenance in gewisser Weise der Einstieg in die Welt der Künstlichen Intelligenz (KI), wo Echtzeitdaten für gezielte Prognosen dienen. Abseits der Maschinendatenerfassung lassen sich weitere Einsatzfelder für KI definieren, um deren vielfältige Möglichkeiten zum Beispiel mit Blick auf die Usability von ERP-Systemen oder für die detaillierte Prognose vertrieblicher Wahrscheinlichkeiten zu nutzen. Etwa dann, wenn den Usern auf Basis der bisher gesammelten Anwendungsmuster über eine dynamische Benutzeroberfläche automatisch die nächsten Prozessschritte vorgeschlagen werden. Oder wenn sich bei einer Angebotsanfrage aufgrund der Kontakthistorie das Verhalten von Interessenten oder Kunden besser vorhersagen lässt.

Darüber hinaus spielt der Faktor Mobilität eine immer entscheidendere Rolle für die effektive betriebliche Organisation. Um Mittelständlern über alle Firmenbereiche und Abteilungen hinweg den flexiblen und standortunabhängigen Zugriff auf die volle ERP-Funktionalität zu ermöglichen, empfiehlt sich die nahtlose Anbindung einer modernen, webbasierten Konfigurationsplattform, über die sich im Low-Code-Verfahren – also ohne Programmierkenntnisse – betriebssystemunabhängige, standardisierte Business-Apps zur Abbildung individueller Geschäftsprozesse erstellen lassen.

Sind ERP-System und Konfigurationsplattform optimal aufeinander abgestimmt, ist der sichere und kontrollierte Zugriff auf die Geschäfts-Software gewährleistet. Die Außendienst-, Service- und Montageeinsätze, die sich aus den flexiblen Service- und Wartungsmodellen ergeben, lassen sich dann nicht nur optimal disponieren und koordinieren, es entfällt auch die bislang papierbasierte, langwierige Eingabe von Personal- und Einsatzzeiten – mit dem Vorteil, dass alle Daten sofort in Echtzeit verfügbar sind.

MIT EINER OFFENEN ERP-SOFTWARE IM ZENTRUM IHRER DIGITALISIERUNGSMASSNAHMEN KÖNNEN MITTELSTÄNDISCHE EINZEL-, AUFTRAGS- UND VARIANTENFERTIGER IHRE EFFIZIENZ INSGESAMT DEUTLICH STEIGERN.

Simone Schiffgens, Vorstandsvorsitzende, ams.Solution AG, www.ams-erp.com

Mit einer offenen ERP-Software im Zentrum ihrer Digitalisierungsmaßnahmen können mittelständische Einzel-, Auftrags- und Variantenfertiger ihre Effizienz insgesamt deutlich steigern. Sie können kostengünstiger produzieren, bleiben wettbewerbsfähig und leisten somit einen wichtigen Beitrag zur Verbesserung der konjunkturellen Gesamtlage. Vernetzung, Digitalisierung und Automatisierung sind zudem wirksame Mittel zur Bekämpfung des Fachkräftemangels und tragen somit zur langfristigen Sicherung des Standorts bei.

Simone Schiffgens

ZUKUNFTSSICHERES SERVICE MANAGEMENT

ERFOLGSFAKTOREN FÜR TOOLBESCHAFFUNG UND DIE ROLLE DER KÜNSTLICHEN INTELLIGENZ

Die digitale Transformation hat in den letzten Jahren deutlich an Fahrt aufgenommen. Besonders für größere Unternehmen mit mehr als 200 PC-Arbeitsplätzen wird ein effizientes IT und Enterprise Service Management (ITSM / ESM) immer wichtiger. Viele Betriebe unterschiedlichster Branchen sehen sich mit der Herausforderung konfrontiert, ihre Prozesse mithilfe von IT-Tools zu modernisieren und den Betrieb zukunftssicher aufzustellen.

Viele Unternehmen arbeiten bereits mit einem Service Management Tool, stoßen jedoch an Grenzen hinsichtlich Effizienz, Betriebsmodell, Skalierbarkeit oder technischer Integration. Sie überlegen daher, zu einem moderneren System zu wechseln. Andere Unternehmen hingegen haben noch keine dedizierte Lösung im Einsatz und arbeiten beispielsweise mit Excel-Tabellen oder manuellen Prozessen, die sehr ineffizient und aufwendig sind.

Machen Sie Ihr Unternehmen fit für die Zukunft!

Im Whitepaper erfahren Sie, warum für Unternehmen der Wechsel zu einer modernen IT- und Enterprise Service Management Software entscheidend ist. Entdecken Sie die häufigsten Gründe für eine Neueinführung, die wichtigsten Schritte für eine erfolgreiche Tool-Evaluation und wie Künstliche Intelligenz Ihre Prozesse revolutioniert.

Dieses Whitepaper unterstützt IT-Entscheider und IT-Leiter gezielt bei der Evaluierung und Auswahl einer neuen Service Management Software oder beim Wechsel von bestehenden Lösungen. Besonderer Fokus liegt dabei auf der Rolle der Künstlichen Intelligenz bei der Evaluation einer modernen Software.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 17 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/Download

Compliance-Vorgaben

HINDERNIS IN DER PROFESSIONELLEN KOMMUNIKATION?

MIT DEM SP800 BIETET SNOM EINEN ECHTEN GAMECHANGER.

Felix Glowatzka, Produktmanager, Snom Technology GmbH, www.snom.com

UCaaS-Lösungen für die Unternehmenskommunikation wie MS Teams und Zoom oder auch Telefonie-Plattformen mit Soft-Clients verdrängen allmählich das traditionelle Tischtelefon. Über den Computer mittels Softphone zu telefonieren, funktioniert gut, daran besteht kein Zweifel. Doch Firmen, die sensible Daten bearbeiten, haben häufig strikte Richtlinien für den Zugang und die Nutzung von Unternehmensressourcen sowie eine Vorliebe für Thin Clients: Ein Notariat mit 10 Mitarbeitern oder das Callcenter eines Finanzdienstleisters mit 300 Arbeitsplätzen haben die gleichen strengen Compliance-Vorgaben, wenn es um Datensicherheit und Kommunikationsqualität geht. Letztere zieht jedoch bei Remote-Desktop-Infrastrukturen häufig den Kürzeren, denn Terminal-Server können nicht zwischen Daten- und Audioübertragung unterscheiden. Das positive UCaaS-Erlebnis gerät also rasch in Vergessenheit, wenn der Kampf mit der Qualität beginnt – denn eine schlechte Tonqualität und Verzögerungen in der Übertragung gehören leider auch zum Alltag bei dieser Art der Kommunikation.

Diese Benutzererfahrungen und die steigenden Anforderungen an Sicherheit und Komfort auch in sensiblen Arbeitsumgebungen waren daher treibende Argumente für die Entwicklung des SP800 durch Snom Technology, den Berliner Spezialisten für IP-basierte Kommunikation.

Mit „Trick 17“ zur perfekten Lösung

Remote-Desktop- oder Terminal-Server-Umgebungen bieten einerseits einen effektiven Schutz vor Ressourcenmissbrauch und Sicherheitsrisiken, andererseits wurden sie für den Zugriff auf Daten und deren Verarbeitung konzipiert. Eine integrierte Telefonanlage mit entsprechenden Softphones verhindert zwar eigenmächtiges Telefonieren und bietet hohe Sicherheit, gewährleistet jedoch nicht die notwendige Audioqualität der Kommunikation. Genau hier setzt das Snom SP800 an.

Es wurde genau für die Umgebungen entwickelt, in denen Kopfhörer anstelle des Hörers zum Einsatz kommen. So ist das SP800 zwar innen ein vollwertiges Snom-Telefon mit allen Sicherheits- und Komfortmerkmalen, für die der Hersteller bekannt ist, von außen aber ein kleines flaches Gerät mit einigen Anschlüssen. Vollgepackt mit innovativer Technologie, benötigt das Gerät weder Tastatur noch Display und ist dadurch deutlich kleiner als ein klassischer Android-Mediaplayer. Durch den kompakten Formfaktor kann es unsichtbar hinter dem Monitor oder unter dem Schreibtisch montiert werden, ist also ideal für Remote-Arbeitsplätze und Arbeitsumgebungen mit „Clean-Desk“-Vorgaben.

Der Anwender schließt nun sein eigenes Headset an und kann die über das IP-Telefon zu führenden Gespräche direkt über den Monitor des Thin Clients ansteuern und parallel entsprechende Gesprächsprotokolle verwalten. Wie die UC-Software wird auch das SP800 zentral von der IT konfiguriert und verwaltet, was ebenfalls den Sicherheitsstandards vieler Unternehmen entspricht und für eine schnelle Implementierung sorgt.

Mit dem SP800 bietet Snom einen echten Gamechanger in diesem Bereich. Die Nachfrage nach einer solchen Lösung ist entsprechend groß: Das SP800 könnte sich als unverzichtbares Tool für die sichere und effiziente Kommunikation im Büroalltag jener Organisationen etablieren, die aufgrund ihrer Compliance-Vorgaben bislang Kompromisse bei der Qualität der Gespräche eingehen mussten.

Felix Glowatzka

SELFCARE NEXT LEVEL

7 STRATEGIEN FÜR KRISENFESTE FÜHRUNGSKRÄFTE

Wer sich als Führungskraft strategisch auf die Zukunft vorbereiten will, ist gut beraten: Denn die zu erwartenden Turbulenzen in der Arbeitswelt sind enorm und zeigen sich auch in einem starken Anstieg der Krankheitsquoten bei Führungskräften.

Nur: Was lässt sich dagegen tun? Und zwar bevor es zum Burnout oder einer schweren Herz-Kreislauferkrankung kommt?

Business-Health-Coach Kara Pientka zeigt in diesem Buch sieben praxistaugliche Selfcare-Strategien, wie es Ihnen als Führungskraft gelingt, klug, selbstbewusst und mit vollen Akkus durch anstrengende Krisenzeiten zu kommen. Das Buch macht Lust auf Führungsverantwortung in Transformationszeiten, weil es eine praxiserprobte Perspektive bietet, um sich selbst und die Mitarbeitenden motiviert, produktiv und gesund zu halten.

Wie auch immer es Ihnen als Führungskraft aktuell geht: Am Ende dieses Buches werden Sie gestärkt sein.

Selfcare Next Level:
7 Strategien für krisenfeste Führungskräfte;
Kara Pientka,
campus Verlag, 10-2024

KMU-Praxisleitfaden Datenschutz und Datensicherheit:
Nur wer die Risiken und Gefahren kennt, kann sich davor schützen;
Dieter Grohmann,
Werner Grohmann;
08-2024

KMU-PRAXISLEITFADEN DATENSCHUTZ UND DATENSICHERHEIT

NUR WER DIE RISIKEN UND GEFAHREN KENNT, KANN SICH DAVOR SCHÜTZEN

Datenschutz und Datensicherheit gehören derzeit sicher zu den größten Herausforderungen für Unternehmen und dabei ganz besonders für kleine und mittlere Unternehmen (KMU) in Deutschland.

Im Gegensatz zu den „Großen" verfügen die KMU – wir halten uns dabei an die Definition des Statistischen Bundesamtes – also Unternehmen mit bis zu 250 Beschäftigten und bis zu 50 Millionen Euro Umsatz, in der Regel nicht über die entsprechenden Prozesse, Strukturen und Kapazitäten, müssen aber dieselben Konsequenzen fürchten, wenn etwas schief geht.

Ziel des Praxisleitfadens ist es, Führungskräften in kleinen und mittleren Unternehmen einen kompakten und präzisen Überblick über die wichtigsten Themen zu Datenschutz und Datensicherheit zu vermitteln. Dabei sollen das Bewusstsein für die Risiken und Gefahren in diesen Bereichen gestärkt und Möglichkeiten für erfolgreiche Gegenmaßnahmen aufgezeigt werden.

Denn: Nur wer die Gefahren kennt, kann sich davor schützen!

Reibungslos digitalisieren

MIT RETARUS CLOUD FAX ZU EFFIZIENTERER PROZESSKOMMUNIKATION

Wenn es darum geht, Dokumente nicht nur schnell und sicher, sondern auch nachvollziehbar und rechtsverbindlich auszutauschen, ist das digitale Fax für viele Unternehmen das Mittel der Wahl. Um ihre Kommunikationsprozesse zu modernisieren und zu digitalisieren, bietet der Umstieg auf Fax-Services aus der Cloud zahlreiche Mehrwerte. Mit Retarus Cloud Fax können Unternehmen schnell und unkompliziert in die Cloud migrieren, den Kommunikationskanal Fax modernisieren sowie die Komplexität der IT-Infrastruktur reduzieren. Die technischen Experten von Retarus realisieren nicht nur einen kompletten, risikofreien Wechsel zu Cloud Fax, sondern auch eine schrittweise Migration einzelner Anwendungen.

Moderne Funktionen des Cloud Fax

Mit den hochverfügbaren und skalierbaren Retarus Cloud Fax Solutions gelingt den Unternehmen der Umstieg auf eine effiziente, flexible und reibungslose Kommunikationslösung. So macht eine Cloud-Fax-Lösung Ressourcen frei und bietet intelligentes Routing, einen weltweiten Faxnummern-Service, Echtzeit-Monitoring, Data-at-Rest- und Data-in-Transit-Verschlüsselung sowie Langzeitarchivierung. Zudem lässt sich die Lösung einfach, transparent und zentral administrieren. Mit einem übersichtlichen Reporting, weitreichender Automatisierung, nahtloser Integration in nahezu jeder IT-Landschaft plus einem erstklassigen 24/7-Support und maßgeschneiderten SLAs.

Sensible Daten sicher übertragen

Fax als weltweit standardisiertes Übertragungsprotokoll kommt insbesondere in stark regulierten Branchen wie dem Gesundheitswesen oder im Finanzsektor zum Einsatz. Dort müssen besonders strenge gesetzliche Vorgaben und Compliance-Richtlinien für die Verarbeitung kommerzieller, personenbezogener und finanzieller Daten eingehalten werden. So erfolgt die Anbindung an die Retarus Enterprise Cloud über verschlüsselte Verbindungen (TLS, VPN). Auf Wunsch signiert und verschlüsselt Retarus auch eingehende Fax-Dokumente – je nach Dateityp per AES 256-bit, PGP oder X.509. Darüber hinaus erfüllt Retarus mit seinen auditierbaren Rechenzentren alle branchen- und länderspezifischen Datenschutz- und Sicherheitsanforderungen wie DSGVO, ISO 27001, SOC1 und SOC2 (jeweils Type II).

Problemlose Integration mit SAP S/4HANA

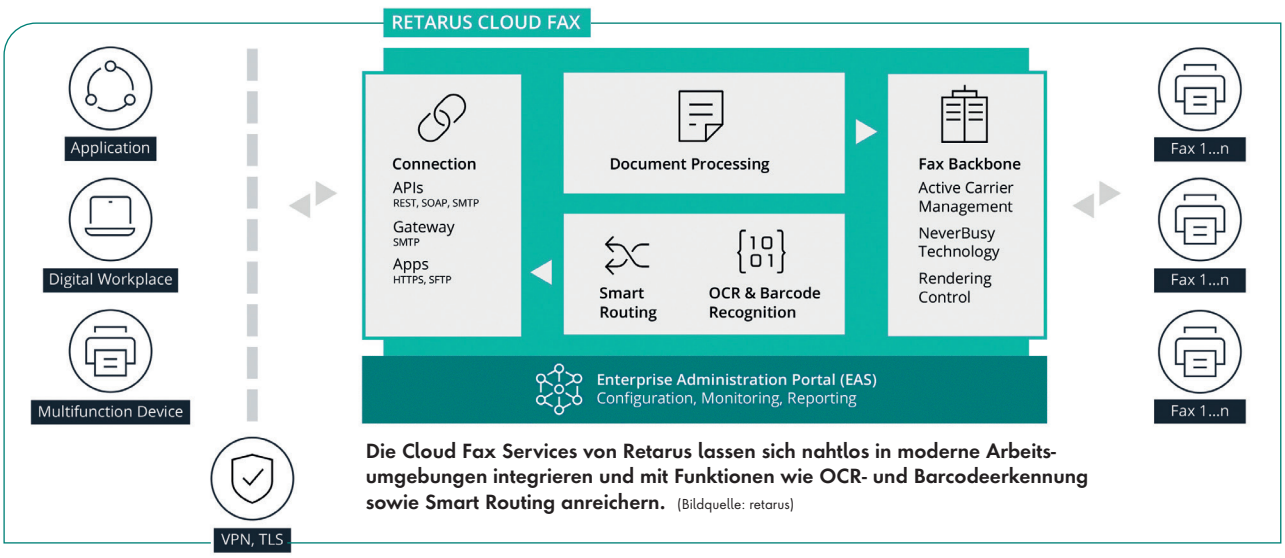
Ein weiterer Vorteil der Cloud-Fax-Lösungen von Retarus besteht darin, dass sich diese dank offener Standards nahtlos in nahezu jede Prozesslandschaft, Business-Applikation und jedes ERP-System, wie zum Beispiel SAP S/4HANA, integrieren lassen. Dies erfolgt entweder per Webservice via REST-API oder über Standard-Schnittstellen und Protokolle wie SMTP, SFTP und HTTPS. Anwender kommunizieren zudem per Fax direkt aus ihrer gewohnten E-Mail-Umgebung heraus – zum Beispiel via Outlook Plugin.

Best-in-class Business-Kommunikation

Insgesamt ermöglicht Retarus Cloud Fax effizientere Workflows mit einer wesentlich geringeren Fehlerquote und daraus resultierend niedrigeren Kosten. Dabei werden Unternehmen durch die Integration von Cloud Fax in moderne Arbeitsumgebungen und die Automatisierung von Arbeitsabläufen den Anforderungen an moderne Kommunikation und Dokumentenverarbeitung heute sowie in Zukunft gerecht.

www.retarus.de

retarus



Die Cloud Fax Services von Retarus lassen sich nahtlos in moderne Arbeitsumgebungen integrieren und mit Funktionen wie OCR- und Barcodeerkennung sowie Smart Routing anreichern. (Bildquelle: retarus)

SAP S/4HANA

WEGBEREITER FÜR DAS INTELLIGENTE UNTERNEHMEN

Analysten von Marktforschern wie Gartner, Deloitte, EY und PwC prophezeien, dass Störungen in der globalen Supply Chain durch Trendwenden oder Marktturbulenzen geopolitischer, ökologischer, sozialer oder wettbewerblicher Natur künftig zur Tagesordnung gehören. Um diesen Herausforderungen effektiv zu begegnen, ist die S/4HANA-Migration ein entscheidender Schritt, denn sie repräsentiert den Übergang auf ein zukunftsweisendes ERP-System und ebnet somit den Weg zur technologischen Innovation. Diese neue Evolutionsstufe in der betriebswirtschaftlichen Systemlandschaft ermöglicht nicht nur eine End-to-End-Transparenz über die gesamte Lieferkette hinweg, sondern hilft mit innovativen, digitalen Lösungen dabei, Risiken entlang der gesamten Wertschöpfungskette zu identifizieren, zu bewerten sowie transparent und steuerbar zu machen. Unternehmen erreichen dadurch die optimale Balance zwischen Reaktions- und Lieferfähigkeit, Beständen, Durchlaufzeiten, Nachhaltigkeit (Circular Economy) und Kundenzufriedenheit.

Welche Möglichkeiten der Migration gibt es?

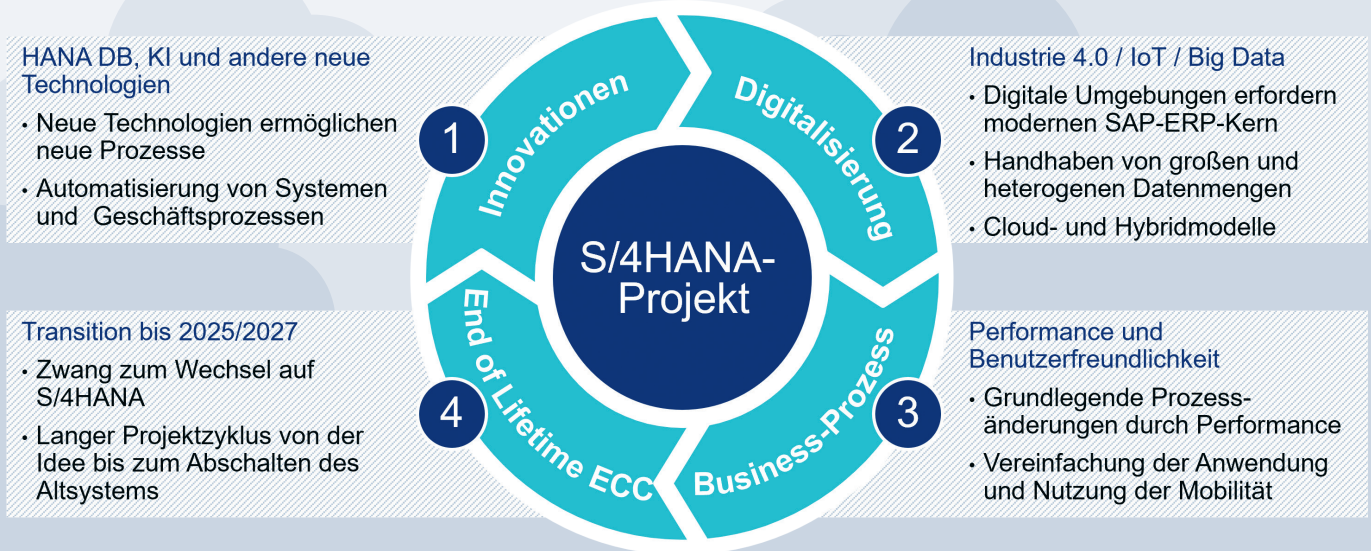
Ein Umstieg auf S/4HANA ist prinzipiell kein standardisierter Prozess, sondern vielmehr durch die individuellen Voraussetzungen und Anforderungen des Unternehmens vorgezeichnet. So bietet die SAP für den Umstieg auf S/4HANA einen On-Premises- und einen Cloud-Pfad an.

#1 On-Premises: der Klassiker

Langjährige SAP-Bestandskunden betreiben ihr Unternehmenssystem auf diese Weise – daher ziehen diese Deployment-Methode viele Anwender-Unternehmen in Betracht.

Brownfield: Die Systemumwandlung klingt zunächst wenig innovativ und wird gerade im Management als vertane Chance betrachtet, um Prozesse zu standardisieren. Sie muss jedoch nicht als rein technischer Releasewechsel durchgeführt werden. Wer mehr will, sollte sich die Beyond-Brownfield-Methode von CONSILIO ansehen. Sie entfernt nicht nur überflüssige Altlasten – etwa nicht mehr notwendige Erweiterungen und Modifikationen oder archiviert Stamm- und Bewegungsdaten, sondern erhält Investitionen, die in die SAP-Software getätigt wurden und Wettbewerbsvorteile für das Unternehmen bringen. Dabei konzentriert dieses Vorgehen auf Prozesse, bei denen

S/4HANA: ALLE FAKTEN IM ÜBERBLICK



Die neueste Version des SAP-Systems adressiert aktuelle Themen wie Industrie 4.0, Big Data, Mobilität und höhere Prozess-Performance.

(Quelle: CONSILIO)

tatsächlich Handlungsbedarf besteht. So wird das verfügbare Budget zielgerichtet für Innovationen und die wirklichen wichtigen Prozesse eingesetzt.

Greenfield: Dieser Pfad beschreibt eine vollumfängliche Neu-Implementierung von S/4HANA. Dabei werden sämtliche Prozesse, Organisation, Stammdaten etc. in der Regel auf Basis von SAP-Best-Practices neu konfiguriert. Der Greenfield-Ansatz bietet Unternehmen somit die Chance, überholte Prozesse und ineffiziente Anpassungen des Systems von Beginn an zu vermeiden. Der Greenfield-Ansatz erfordert eine umfangreiche Planung und kann mehr Zeit und Ressourcen als die anderen Transformationspfade in Anspruch nehmen.

Crossfield: Diese Methode ist vor allem für große Unternehmen und globale Systemlandschaften mit Buchungskreisen und Werken im 2-3-stelligen Bereich interessant, da sie einen Mix aus Brown- und Greenfield darstellt. Er ermöglicht einen schrittweisen Umstieg nach S/4HANA wie z.B. einzelne Werke, Buchungskreise etc. Hierbei ist es auch möglich Stamm- und Bewegungsdaten selektiv zu übernehmen und umfassender zu ändern als beim Brownfield-Ansatz. Zusammengefasst: Das Ziel der der Crossfield-Methode ist, bewährte Bestandteile des Altsystems nach SAP S/4HANA zu übernehmen und veraltete Komponenten sowie unflexible, nicht weiter optimierbare Prozesse durch neue zu ersetzen. Der Anwender sichert so seine Investitionen und schafft Platz für neue Innovationen – ganz nach seinen individuellen Anforderungen.

#2 Cloud: Die moderne Variante

Wie die SAP mitteilte, fokussiert sich das Unternehmen auf die Cloud. Das bedeutet, dass die On-Premises-Varianten zwar noch funktional weiterentwickelt werden, Innovationen – etwa KI-basierte Lösungen wie die Umweltberichterstattung Green Ledger oder größere Funktionsbereiche und Erweiterungen auf der Business Technology Platform (BTP) – sollen aber nur noch SAP-Cloud-Kunden zur Verfügung stehen. Wer davon profitieren will, muss also in die Cloud wechseln.

Die S/4HANA-Cloud bietet die SAP in zwei Vertragsmodellen an: GROW with SAP und RISE with SAP. Für Anwender, die noch kein ERP im Einsatz haben, oder zu SAP wechseln wollen, bietet sich ein GROW with SAP an. Diese Cloud-Variante bietet ein hohes Maß an Standardisierung und hat einen festgelegten Funktionsumfang.

Durch diesen hohen Standardisierungsgrad ist diese Version weniger für Unternehmen geeignet, die bspw. in Nischenbereichen agieren, sehr spezielle Abläufe haben oder außergewöhnlichen gesetzlichen Regularien unterliegen. Interessierte SAP-Anwender-Unternehmen sollten in Betracht ziehen, dass es bei dieser Lösung nicht möglich ist Prozesse aus einem Altsystem mitzunehmen. Zudem steht hier die Bedienoberfläche FIORI im Mittelpunkt, die eine intuitive Bedienung des Systems ermöglicht. GROW

with SAP bietet den idealen Start in die SAP ERP Welt und ist speziell für wachsende Unternehmen ausgelegt, um in der S/4HANA Cloud die maximale Flexibilität zu gewährleisten

Wer die Flexibilität und den Funktionsumfang seines On-Premises-Systems nicht missen möchte, aber sein ERP-System mithilfe der Cloud auf ein neues Level heben will, sollte einen Blick auf RISE with SAP in der Private Cloud werfen. Das bedeutet: Diese Variante von S/4HANA umfasst nicht nur den gesamten Funktionsumfang der S/4HANA-On-Premises-Lösung, sondern der Anwender kann im Gegensatz zur Public Cloud auch bestimmen, in welcher Region sein System gehostet wird oder welchen Transformationspfad (Brown-, Cross- und Greenfield) er für sich festgelegt. Da RISE with SAP Private Cloud weitestgehend der On-Premises-Variante entspricht, bietet diese Edition neben der Fiori-Oberfläche auch die Nutzung der modernisierten SAP GUI an, auch Customizing und Eigenentwicklungen sind nach wie vor möglich. Insbesondere für SAP Bestandskunden ist dieser Ansatz eine Alternative um die Cloudvorteile nutzbar zu machen.

Fazit

Kompetente SAP-Partner wie CONSILIO schaffen mit ihren Assessment-Werkzeugen Klarheit welcher Weg am besten passt, denn Optionen gibt es mehr als genug. Bei diesen Analysen gehen daher nicht nur Informationen über Systemarchitektur ein, sondern es werden auch ganzheitlich Faktoren wie personelle Ressourcen berücksichtigt.

Für Organisationen, die eine schnelle, einfache und damit kostengünstige Implementierung und Verwaltung wünschen, trumpft SAP mit Lösungen wie GROW with SAP auf. Unternehmen mit komplexen und individuellen Ansprüchen und jene, die von einer bereits gut eingespielten älteren SAP-Umgebung aufrüsten wollen und nicht willens sind, die Kontrolle über ihre Daten aus der Hand zu geben, sind hingegen mit RISE with SAP Private Cloud am besten bedient. S/4HANA-On-Premises ist durch die strategische Ausrichtung der SAP langfristig keine Option, denn künftige Innovationen will die SAP nur noch für die Cloud-Varianten bereitstellen.

Yannik Jodehl

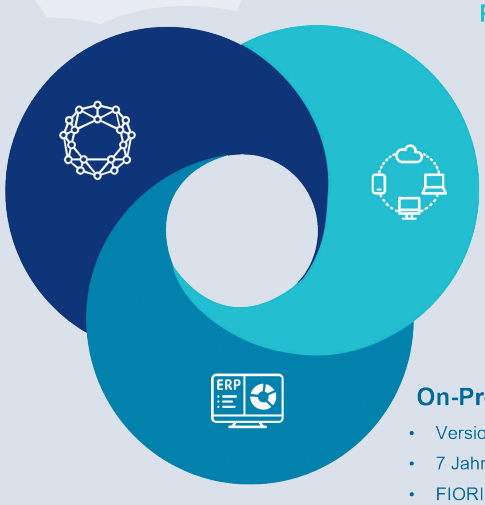
BEIM WECHSEL AUF S/4HANA MÜSSEN SICH DIE VERANTWORTLICHEN AUF DEN RICHTIGEN WEG FESTLEGEN – KEINE EINFACHE ENTSCHEIDUNG. CONSILIO SCHAFFT KLARHEIT UND ZEIGT DEN BESTEN WEG AUF.

Yannik Jodehl, Partner und Head of S/4HANA, CONSILIO GmbH, www.consilio-gmbh.de

CLOUD VS. ON-PREMISES

Private Cloud

- Version 2023 als Zielrelease
- 7 Jahre Wartungszyklus
- 2 FPS/Jahr in den ersten beiden Jahren
- Alle 5 Jahre ein Update notwendig
- FIORI oder GUI
- Alle Migrationswege
- Lizenzabonnement
- Hyperscaler-Entscheidung durch Kunden
- Compatibility Scope bis Ende 2025 entsprechend SAP Note 2269324
- KI-Themen
- Green Ledger
- AI/KI-Lösungen



Public Cloud

- Definierter Funktionsumfang
- Hyperscaler-Wahl durch SAP
- Halbjährlich verpflichtende & automatische Updates
- Greenfield mit FIORI only
- Custom Code via Steampunk
- Zertifizierte Public-Cloud Add-ons von Drittanbietern
- Keine Compatibility Pack Möglichkeit
- Lizenzabonnement
- Vordefinierte SAP Lizenz Add-ons

On-Premise

- Version 2023 als Zielrelease
- 7 Jahre Wartungszyklus, 2 FPS/Jahr in den ersten beiden Jahren
- FIORI oder GUI
- Alle Migrationswege, Compatibility Scope entsprechend SAP Note 2269324
- Kauf der Lizenz inkl. jährlicher Wartung
- Hostingentscheidung durch Kunden
- Keine Sustainability bzw. KI-Erweiterungen

Innovationen – etwa KI-basierte Lösungen wie die Umweltberichterstattung Green Ledger oder größere Funktionsbereiche und Erweiterungen auf der Business Technology Platform (BTP) – sollen künftig nur noch SAP-Cloud-Kunden zur Verfügung stehen. (Quelle: CONSILIO)

ERP und Softwarelösungen

SCHLÜSSEL ZUR ZUKUNFT INTELLIGENTER MASCHINEN

Software wird zunehmend das „Nervensystem" moderner Maschinen und ermöglicht intelligente, vernetzte und automatisierte Systeme. Enterprise-Resource-Planning-Systeme spielen dabei eine entscheidende Rolle, indem sie Maschinen mit dem gesamten Produktionsprozess verbinden und so die Basis für datengestützte Entscheidungen schaffen.

Die Steuerung von Maschinen, die lediglich mit einer einfachen Software ausgestattet sind, während der Rest der Steuerung durch manuelle Programmierung und Tests an der physischen Anlage erfolgt, gehört der Vergangenheit an. Intelligente Maschinen, die mit ERP-Systemen vernetzt sind, nutzen moderne Technologien, um Daten in Echtzeit auszutauschen. Dies führt zu neuen Möglichkeiten wie der vorausschauenden Wartung (Predictive Maintenance) und reduziert Ausfallzeiten durch automatisierte Wartungsmaßnahmen. Die wachsende Bedeutung von Software in der Fertigung verlangt von kleinen und mittelständischen Unternehmen (KMU) eine Abkehr von rein hardwarezentrierten Lösungen. Moderne ERP-gestützte Maschinen sind effizienter und bieten eine längere Lebensdauer. Damit können KMU auf Nachhaltigkeit und Kosteneffizienz setzen.

Viele Unternehmen haben tiefgehendes Know-how im mechanischen Bereich, jedoch oft nicht ausreichend Softwareentwicklungsfähigkeiten. Ein ERP-System, das Daten nahtlos verarbeitet und in Produktionsabläufe integriert, schafft hier Abhilfe. Durch Echtzeit-Daten können Maschinenzustände überwacht und Wartungsintervalle optimiert werden, was nicht nur die Produktivität steigert, sondern auch neue Geschäftsmodelle ermöglicht. ERP-Systeme bieten zudem die Grundlage für „Smart Factories", indem sie sämtliche Abläufe unternehmensweit vernetzen und optimieren. Daten aus der Produktion werden gesammelt und analysiert, um Prozesse kontinuierlich zu verbessern. Durch die Anbindung an das Internet der Dinge (Internet of Things – IoT) können Maschinen und ERP-Systeme autonom Entscheidungen treffen, die Effizienz steigern und die Flexibilität in der Produktion erhöhen.

Neue Wege in der Softwareentwicklung

Moderne Softwareplattformen ermöglichen eine flexible und modulare Entwicklung. Die Software wird hardwareunabhängig simuliert, getestet und erst dann in die Maschinen integriert. Dies beschleunigt Entwicklungszyklen, da Codes für verschiedene Hardware schnell generiert werden können. Dadurch lassen sich Kosten und Zeit sparen. Besonders im Bereich der Simulation zeigt sich das Potenzial von „Digital Twins" – virtuellen Abbildern realer Maschinen. Diese digitalen Zwillinge ermöglichen es, Prozesse vorab zu testen und spätere Wartungsarbeiten präzise zu planen. In Kombination mit ERP-Systemen können KMU so Fehler minimieren und die Produktivität steigern.

ERP-SYSTEME SAMMELN UND VERWALTEN DATEN IN ECHTZEIT, WAS UNTERNEHMEN ERMÖGLICHT, PRÄZISE EINBLICKE IN DEN ZUSTAND IHRER MASCHINEN UND ANLAGEN ZU ERHALTEN.

Peter van Harten, Geschäftsführer und Gesellschafter, Isah GmbH, https://isah.com/de/

Lösungen für fehlende Softwarekompetenzen

Viele KMU stehen vor der Herausforderung, die notwendigen Softwareentwicklungsfähigkeiten aufzubauen. Eine Option ist die Zusammenarbeit mit Fieldlabs, die Zugang zu Expertenwissen und Lösungen bieten. Solche Innovationszentren ermöglichen den Austausch mit anderen Unternehmen und Forschungseinrichtungen, um neue Technologien zu testen und zu entwickeln. Auch externe Dienstleister oder Technologiepartner können helfen, die notwendigen Kompetenzen zu integrieren. Gemeinsam mit dem Unternehmen entwickeln sie passende Softwarearchitekturen, die langfristig intern übernommen werden können. Eine enge Kooperation mit Technologiepartnern ermöglicht es zudem, Entwicklungsaufwände zu teilen und die Risiken zu minimieren.

Peter van Harten

Minimale Downtime

KOMPLEXE MIGRATION IM ENERGIESEKTOR

Nachdem NRG Energy mehrere Energieversorger im Privat- und Geschäftskundenbereich der USA übernommen hatte, wollte das Unternehmen dieses Wachstum systemseitig angemessen unterstützen. Deshalb entschied sich NRG, seine im SAP ECC-System bestehende National Retail Platform (NRP) von einer Oracle-Datenbank auf eine Suite on HANA (SoH)-Datenbank umzuziehen. Es war das Ziel, den Kundenbetrieb in einer einzigen Instanz zu konsolidieren, Synergien zu nutzen und mehr Effizienz und Effektivität zu erreichen. Außerdem musste NRG seine SAP IS-U-Datenbank verschlanken. Diese war nach den Übernahmen auf fast 28 TB angewachsen und beeinträchtigte die Systemleistung im Unternehmen. Die größte Herausforderung war die möglichst geringe Ausfallzeit. NRG wollte die Ausfallzeit auf weniger als einen Tag beschränken, um Auswirkungen auf die Geschäftskontinuität für 7,5 Millionen Kunden zu vermeiden.

Um all das sicherzustellen, unterstützte das Natuvion Transformationsteam mit dem Natuvion Data Conversion Server (DCS).

Der Near-Zero-Downtime-Projektansatz

Der Natuvion DCS ist speziell für die Verarbeitung großer Datenmengen entwickelt und kann viele Transformationsaufgaben automatisieren - ideal also für Migrations- und Transformationsprojekte mit engen Zeitvorgaben.

Natuvion strukturierte die Umsetzung folgendermaßen: Während der Betriebszeit wurde parallel zum Einsatz des Natuvion DCS die SAP Database Migration Option (DMO) verwendet. Um eine Ausfallzeit von maximal 18 Stunden einzuhalten, kam zudem der Near Zero Downtime (NZDT) Ansatz zum Einsatz. Hierbei werden mithilfe des Natuvion DCS Verfahren wie die Datensynchronisation (Trigger), die Identifizierung von warmen oder kalten Daten und Waving-Mechanismen angewendet.

Schritt für Schritt zu einer reibungslosen Migration

Zunächst erstellte Natuvion eine Kopie der Oracle-Datenbank (Quellsystem). Diese enthielt alle Stamm- und Bewegungsdaten, die in eine leere HANA-Shell (Zielsystem) migriert wurden. Die zweite Phase umfasste alle Aktivitäten aus dem ersten Schritt sowie einen Test des NZDT-Ansatzes.

In der folgenden Generalprobe führte Natuvion die Uptime-Migration von der Oracle-Quelle zum HANA-Ziel durch. Diese erforderte eine Betriebsunterbrechung von nur zwei Stunden, lief aber zwei Wochen, während der Betrieb des Altsystems aufrechterhalten wurde. Erst als die Uptime-Migration

MEHRWERT

Natuvion Data Conversion Server (DCS)

Near Zero Downtime

abgeschlossen und validiert war, wurden die Trigger deaktiviert und die Änderungen der letzten zwei Wochen in das HANA-System migriert. Danach erfolgte der Go-live.

Erfolgreiche Migration mit nur 13 Stunden Ausfallzeit

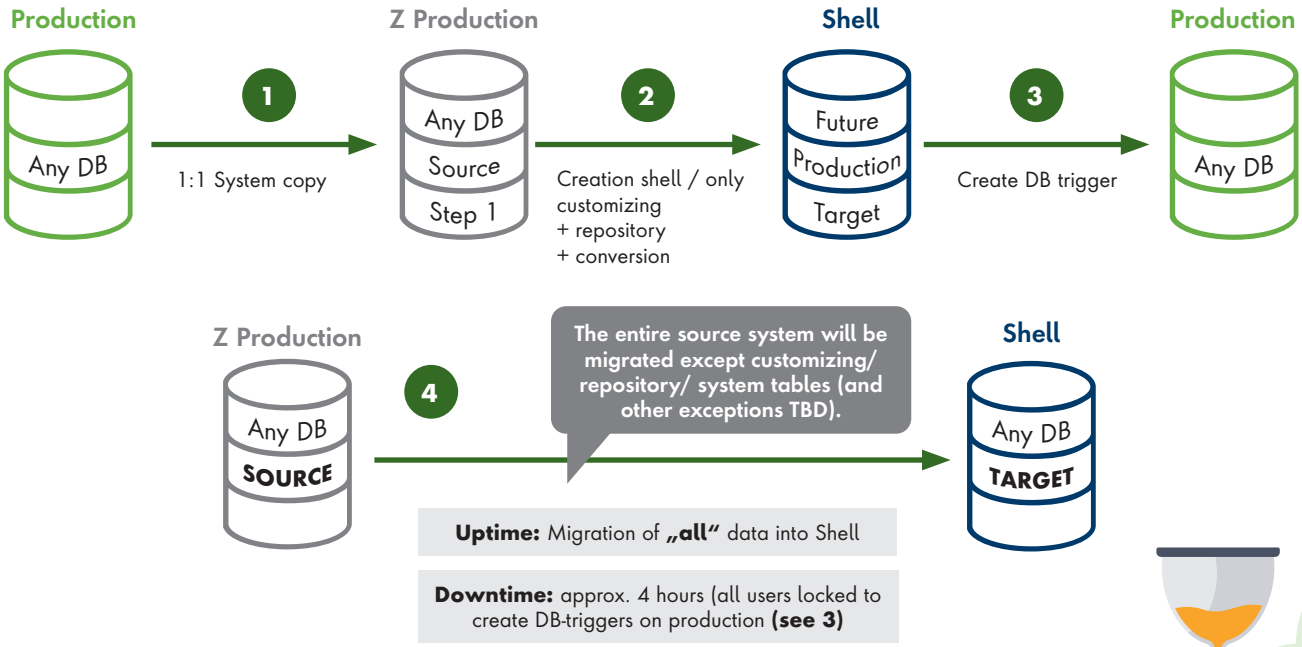
Ziel des Projekts war eine Datenmigration mit einer sehr geringen Ausfallzeit. Der Umzug aller Daten wurde statt der vereinbarten Zeit von 18 Stunden in nur 13 Stunden abgeschlossen.

Kalim Tippitt, IT Senior Director bei NRG Energy, zeigt sich zufrieden: „Die wichtigsten Vorteile für uns waren die außergewöhnlich schnelle Migrationszeit und die Reduzierung der Datenbankgröße. Die geplante Downtime von 18 Stunden war schon sehr ehrgeizig. Wir waren wirklich beeindruckt, dass Natuvion die Migration sogar schneller als geplant durchführen konnte. Die Migration und die Verkleinerung der Datenbank – wir starteten bei 28 TB und landeten bei schlanken 4,21 TB in SAP HANA – werden sich definitiv positiv auf unsere Unternehmensleistung auswirken und unsere Wachstums- wie auch M&A-Pläne unterstützen."

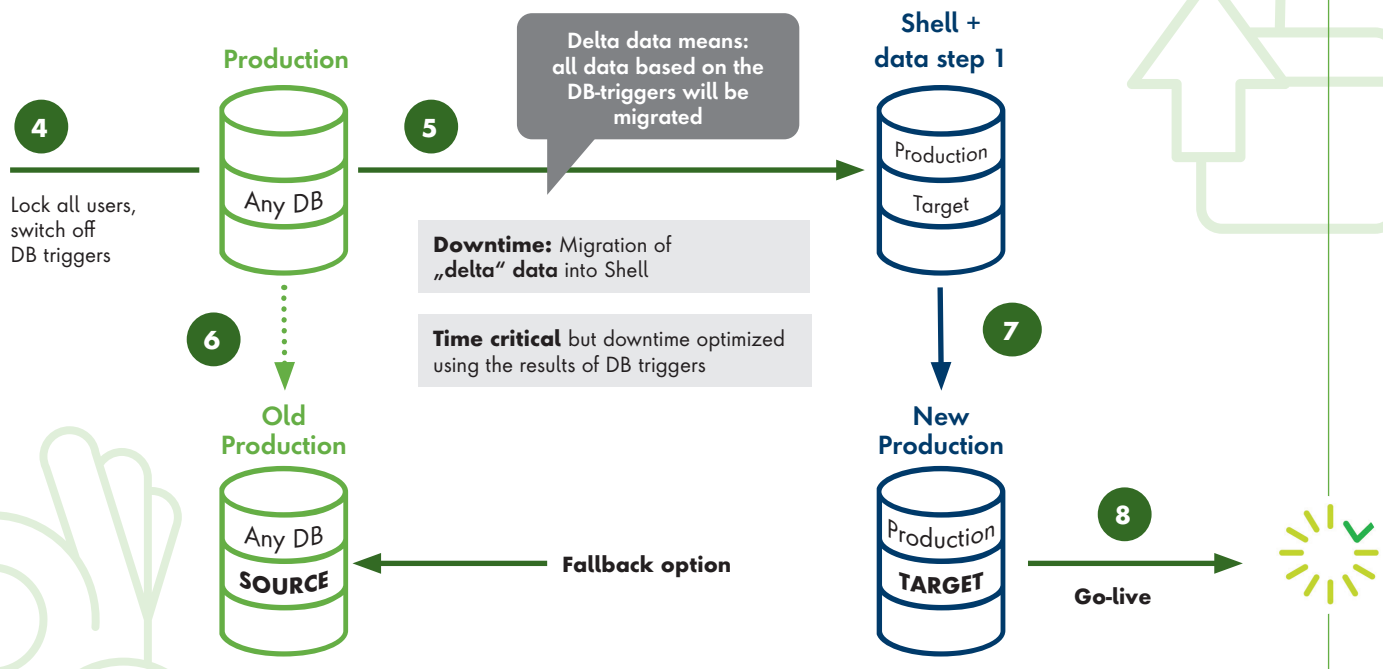
Philipp von der Brüggen
www.natuvion.com

NZDT: DATA MIGRATION – ANY DB TO ANY DB

STEP 1 High level (using DB-trigger)



STEP 2 Cutover: Prod system is down – this step is carried out 1 or 2 weeks after step 1



Bedrohungserkennung und Compliance in SAP

SIEM-INTEGRATION: LOG-CRAWLING, EVENT-HANDLING ODER SPEZIALSOFTWARE?

Die Verwaltung und Verarbeitung sensibler und geschäftskritischer Daten wie Finanz- und Personalinformationen macht SAP-Systeme zum häufigen Ziel von Cyberangriffen. Durch die Vielzahl unterschiedlicher Benutzer sowie die tief- und systemübergreifende Kommunikation mit Betriebssystemen und Datenbanken sind sie zudem besonders anfällig und Sicherheitsverletzungen können gravierende Folgen haben. Eine effektive Überwachung erfordert nicht zuletzt die Integration von SAP-Logs in SIEM-Systeme. Hier gilt es für Unternehmen, sich für einen von zwei Log-Agenten zu entscheiden – oder für eine Drittanbieter-Software. Eine Gegenüberstellung.

Die Überwachung von Aktivitäten, die frühzeitige Erkennung von Anomalien sowie die Einhaltung von Compliance-Vorgaben wie der Datenschutz-Grundverordnung und dem Sarbanes-Oxley Act (SOX) sind für die IT-Security unverzichtbar. Ein wesentlicher Bestandteil ist hier die Integration von SAP-Logs in ein Security Information and Event Management System (SIEM), um Security Operation Centers (SOC) mit geeigneten Informationen auszustatten.

Durch die Wahl ihres SIEMs treffen Unternehmen gleichzeitig eine Entscheidung, welcher native SIEM-Agent der passende Ansatz ist, Log-Crawling oder Event-Handling. Beide Methoden der Erfassung und Verarbeitung von Log-Daten in einem SIEM haben Vor- und Nachteile, die Unternehmen bei der Wahl des passenden Ansatzes berücksichtigen sollten.

Das Log-Crawling

Beim Log-Crawling werden Logs in regelmäßigen Abständen aus den verschiedenen Systemen und Anwendungen gesammelt. Dieser Ansatz ermöglicht die Erfassung von großen Mengen an Daten, die nicht nur sicherheitsrelevante Ereignisse, sondern auch detaillierte Informationen über alltägliche Aktivitäten im System beinhalten. Log-Crawling bietet somit ein vollständiges Bild über Systemvorgänge und ist ideal für forensische Analysen, da es auch weniger offensichtliche sicherheitsrelevante Informationen erfasst.

So ermöglicht die vollständige Erfassung aller Log-Daten eine umfassende und rückwirkende Analyse: Auch ältere Log-Daten können auf Bedrohungen oder Anomalien geprüft werden. Dass nicht nur Echtzeit-Ereignisse erfasst werden, macht das Log-Crawling ideal für zyklische Berichte und Sicherheitsprüfungen, die in festgelegten Intervallen durchgeführt werden.

Diese Methode birgt aber auch Nachteile: Die Erfassung großer Datenmengen erhöht den Speicherplatzbedarf und verzögert die Erkennung und damit die Reaktion auf Bedrohungen. Zudem führt die Menge der erfassten Logs in SIEM-Systemen, die volumenbasiert abrechnen, zu höheren Kosten.

Das Event-Handling

Event-Handling konzentriert sich hingegen auf das Echtzeit-Monitoring sicherheitsrelevanter Ereignisse. Anstatt alle Logs zu erfassen, werden nur jene Ereignisse an das SIEM übermittelt, die vordefinierte Bedingungen erfüllen, wie etwa ein fehlgeschlagener Login-Versuch, eine Änderung an Benutzerrechten oder der Zugriff auf sensible Daten. Dieses selektive Vorgehen der Echtzeit-Erkennung ermöglicht eine schnellere Reaktion auf Bedrohungen und Gegenmaßnahmen können unverzüglich eingeleitet werden.

Event Handling bedeutet auch eine effizientere Nutzung der Ressourcen, da ausschließlich sicherheitsrelevante Daten gespeichert werden, was die Kosten reduziert. Durch die Fokussierung auf relevante Events wird zudem die Analyse beschleunigt und die Gesamtbelastung des Systems minimiert.

Aber auch diese Methode weist Nachteile auf: Durch die begrenzte Erfassung von Patterns können unter den nicht sicherheitskritischen Daten auch weniger offensichtliche Anomalien unerkannt bleiben, was die Qualität forensischer Analyse einschränkt. Für rückwirkende Analysen oder Audits fehlen möglicherweise wichtige historische Daten-Informationen, denn es gibt keine Deckungsgleichheit mit den SAP-Logs. Ein ernstzunehmendes Risiko ist auch die Abhängigkeit von der Qualität der definierten Regeln: Wenn diese für sicherheitskritische Ereignisse nicht korrekt festgelegt sind, können relevante Bedrohungen übersehen werden.

Die Vor- und Nachteile SIEM-nativer Log-Agenten

Die Nutzung von SIEM-eigenen Log-Agenten zur Erfassung von SAP-Logs

bringt sowohl Vor- als auch Nachteile mit sich. Von Vorteil ist sicherlich die nahtlose Integration in das SIEM-System, da sie speziell für die Erfassung und Verarbeitung von Log-Daten optimiert sind. Unternehmen müssen dadurch weniger Zeit und Ressourcen in die Konfiguration und Wartung der Agenten investieren. Außerdem sind Agenten in der Lage, die Logs direkt zu normalisieren und so für eine effizientere Analyse im SIEM zu sorgen.

Ein wesentlicher Nachteil besteht jedoch in der eingeschränkten Flexibilität. SIEM-eigene Log-Agenten sind auf die spezifischen Funktionen des SIEM-Anbieters zugeschnitten, was die Anpassung an kundenspezifische Anforderungen erschwert. Hinzu kommen die Kosten für die Nutzung dieser Agenten, insbesondere wenn das Unternehmen große Mengen Log-Daten generiert. Hier gilt es, die Vorteile einer einfacheren Integration gegen die potenziellen Kostensteigerungen abzuwägen.

Ein weiterer Kritikpunkt ist die mangelnde Einbindung von Ergebnissen aus Vulnerability-Management-Systemen. Diese liefern wertvolle Informationen wie Schwachstellenanalysen und Konfigurationsprüfungen, die meist zyklisch und nicht in Echtzeit generiert werden. Da SIEM-eigene Log-Agenten in der Regel auf Echtzeit-Events und Logs ausgerichtet sind, fehlt ihnen die Fähigkeit, diese nicht-eventbasierten Informationen effizient zu integrieren. So können wichtige Daten aus periodischen Prüfungen nicht in die Sicherheitsüberwachung einfließen und Sicherheitslücken übersehen werden.

SPEZIELLE SOFTWARE-LÖSUNGEN DER CYBER APPLICATION SECURITY SCHLIESSEN DIE LÜCKE DER INTEROPERABILITÄT, DIE BEI SIEM-EIGENEN LOG-AGENTEN BESTEHT.

Raphael Kelbert, Product Manager, Pathlock Deutschland GmbH, www.pathlock.de

Während Log-Crawling eine umfassendere Datenerfassung erlaubt, überzeugt Event-Handling durch seine Effizienz und die schnelle Reaktionsmöglichkeit bei sicherheitsrelevanten Vorfällen. Unternehmen sollten daher eine Mischung beider Ansätze in Betracht ziehen, um sowohl Echtzeit-Reaktionen als auch rückwirkende forensische Untersuchungen zu ermöglichen. Hier empfiehlt sich der Einsatz spezialisierter Drittanbieter-Lösungen.

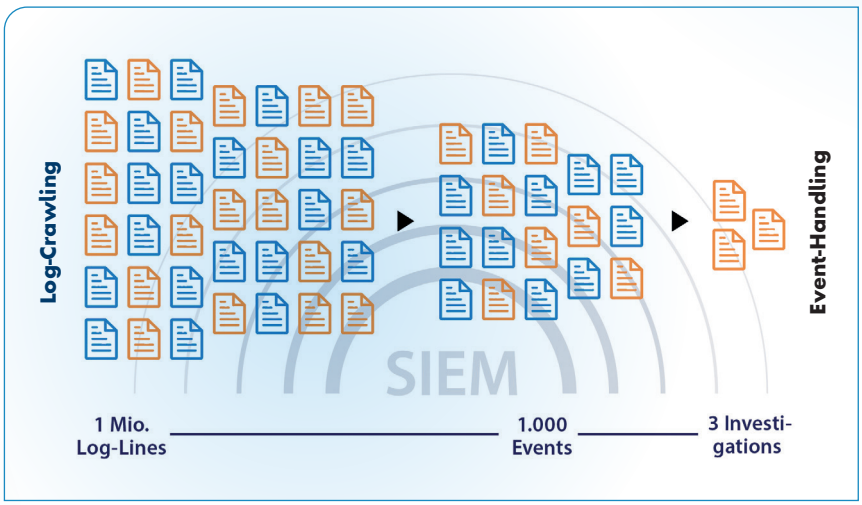
Cyber-Security-Lösungen

Spezielle Software-Lösungen der Cyber Application Security wie von Pathlock schließen die Lücke der Interoperabilität, die bei SIEM-eigenen Log-Agenten besteht. Sie bieten Security Operation Centers eine fundierte Entscheidungsgrundlage, indem sie sicherheitsrelevante Ereignisse und Schwachstelleninformationen zusammenführen. Sie lesen SAP-Logs vollständig aus, filtern die Inhalte vor und übertragen nur relevante Daten in das SIEM-System. Unternehmen profitieren also von einem anpassbaren Vorfilterungsprozess, der spezifisch auf ihre Anforderungen abgestimmt ist, während alle Details für forensische Analysen im SIEM- oder SAP-System verfügbar bleiben.

Dank ihrer hohen Kompatibilität lassen sich diese Lösungen nahtlos in bestehende SIEM-Systeme integrieren, unabhängig von der verwendeten Plattform. Unternehmen können somit von allen Vorteilen profitieren, und das ohne umfassende Systemwechsel. Ein bedeutender Aspekt, denn hat man sich für einen SIEM-Anbieter und den entsprechenden Agenten-Ansatz entschieden, lässt sich dies nicht mehr ohne Weiteres rückgängig machen.

Die Integration einer Drittanbieter-Lösung wie der Pathlock-Software in ein SIEM-System kombiniert eine verbesserte Systemsicherheit durch die Vorfilterung relevanter Logs und die Einbindung von Informationen über Schwachstellen mit geringeren Kosten durch die Reduzierung der Datenmengen. Ihr Ansatz ist daher besonders geeignet, um eine flexible und zukunftssichere Sicherheitsstrategie zu entwickeln, die sowohl Echtzeit-Reaktionen als auch langfristige forensische Analysen unterstützt.

Raphael Kelbert



Während Log-Crawling eine umfassendere Datenerfassung ermöglicht, überzeugt Event-Handling durch Effizienz und Reaktionsschnelligkeit. (Bildquelle: Pathlock Deutschland GmbH)

SMART zu nachhaltigen und resilienten Supply Chains

FÜNF KRITERIEN FÜR RESILIENTE LIEFERKETTEN UND KONKRETE SCHRITTE ZUR UMSETZUNG

Die Anforderungen des Wettbewerbs an globale Supply Chains werden zunehmend komplexer. Ohne moderne Technologien sind die Herausforderungen in den Lieferketten aber nicht zu bewältigen. Diese sind dabei lediglich eine notwendige Bedingung. Ihre volle Wirkung entfalten sie erst dann, wenn Unternehmen sie sinnvoll mit den entsprechenden strategischen und operativen Ansätzen sowie dazu passenden Prozessen, Organisationstrukturen und IT-Applikationen kombinieren. Bei diesem Zusammenspiel kann das von uns entwickelte SMART-Konzept unterstützen.

Technologien mehrwertsteigernd einsetzen

Das Akronym „SMART" definiert die fünf zentralen Kriterien, die Technologien erfüllen sollten, um Unternehmen sinnvoll bei der Gestaltung ihrer Supply Chains unterstützen zu können. SMART steht dabei für:

#1 **Sustainable** (nachhaltig): Sämtliche Technologien, die Unternehmen einsetzen, sollten sie dazu befähigen, die Lieferkette möglichst nachhaltig und ressourcenschonend zu gestalten. Dazu gehört auch, dass sie mit ihnen alle gesetzlichen Anforderungen wie etwa das Lieferkettensorgfaltspflichtengesetz oder die europäische CSR-Richtlinie rechtzeitig und vollständig erfüllen können.

#2 **Measurable** (mess- und steuerbar): Lieferketten lassen sich nur datengestützt sinnvoll steuern. In der Vergangenheit fehlte es dafür oft an der nötigen Transparenz – so blieb häufig unklar, wie zuverlässig Lieferanten bezüglich wichtiger Parameter wie CO_2-Fussabdruck, Liefertreue oder Warenverfügbarkeit waren. Neue Technologien sollten ein durchgehendes Monitoring und eine datengestützte Analyse dieser Kriterien ermöglichen.

#3&4 **Advanced & Resilient** (fortgeschritten & widerstandsfähig): Heutige Lieferketten benötigen vor allem eines: Resilienz. Resilienz bedeutet, dass eine funktionierende Supply Chain auch unter widrigen Umständen aufrecht erhalten bleibt. Das erfordert moderne Technologien und Prozesse, die den Unternehmen zu mehr Flexibilität verhelfen, wenn Lieferbeziehungen unter Druck geraten und sie kurzfristig reagieren müssen.

FLEXIBILITÄT, SCHNELLIGKEIT UND PRÄVENTION SIND WICHTIGE VORAUSSETZUNGEN, UM UNVORHERSEHBARE UNTERBRECHUNGEN IN LIEFERKETTEN ZU BEWÄLTIGEN.

Dr. Sylvia Trage, Partner, MHP Management- und IT-Beratung, www.mhp.com

#5 **Together** (Zusammenarbeit): Lieferkettenbezogene Zahlen können nur dann messbar werden, wenn Lieferanten und Abnehmer eng zusammenarbeiten und bereit sind, Daten auszutauschen und ihre IT eng zu vernetzen. Daher wird die organisatorische Zusammenarbeit zwischen Unternehmen und der Zugang zu IT-Systemen, die diese Vernetzung ermöglichen, noch wichtiger.

SAP BTP und SAP Business Network

Um die im SMART-Konzept definierten Kriterien erfüllen zu können, benötigen Unternehmen ein solides technisches Fundament. Dazu gehören aus unserer Sicht neben einem modernen ERP-System, beispielsweise SAP S/4HANA, vor allem die SAP Business Technology Platform (SAP BTP) und das SAP Business Network.

Gerade hinsichtlich unklarer, zukünftiger Anforderungen verschafft die SAP BTP Unternehmen sehr große Spielräume. Noch bedeutender für ein flexibles Supply-Chain-Management ist derzeit vor allem das SAP Business Network. Der Hintergrund: Im Kern erfordern alle Maßnahmen für eine resiliente und nachhaltige Lieferkette eine enge Kooperation und prozessuale Vernetzung mit den Vorlieferanten, damit sich die Beschaffungsabteilungen schrittweise weiterentwickeln können. Daher benötigen sie einen einfachen Zugriff auf deren Daten- und Lagerbestände, Möglichkeiten zur Echtzeitkommunikation, automatisierte Bestellprozesse sowie Tools, die sie bei der Lieferantenbewertung und -suche unterstützen. Genau hierfür stellt das SAP Business Network die nötigen Funktionen bereit.

Strategische Lieferantenplanung
Bei der strategischen Planung geht es darum, als Unternehmen die passenden Partner zu finden beziehungsweise bestehende Partnerschaften zu bewerten (Lieferantenbewertung). Wichtig wird hierbei, Partnerschaften bezüglich möglicher Risikofaktoren zu evaluieren und für erfolgskritische Partnerschaften bereits im Vorfeld Back-up-Konzepte zu entwickeln. Mögliche Risikofaktoren sind dabei unter anderem der Standort des Unternehmens oder auch die Variationsmöglichkeiten bei den Transportrouten, auf die es im Notfall zurückgreifen kann. Ausgangspunkt dafür können zum Beispiel Länderanalysen sein (Deeskalationsmanagement). Wichtige Lieferanten sollten Unternehmen zudem schrittweise weiterentwickeln und stärker in ihre Prozesse integrieren (Lieferantenentwicklung).

Die Herausforderung dabei: Prinzipiell sind die Ressourcen jedes Unternehmens beschränkt. Die Evaluation sollte daher systematisch erfolgen. Sinnvollerweise beginnt sie bei den wichtigsten Lieferanten – also den Partnern, die die bedeutendsten und preisintensivsten Vorprodukte liefern. Sobald die Beschaffung diese Priorisierung vorgenommen hat, kann sie damit starten, die benannten Kriterien – etwa die Liefertreue – systematisch zu monitoren und in KPIs zu überführen. Das SAP Business Network Track und Trace sowie Material Traceability ermöglicht es sogar, Lieferungen in Echtzeit zu überwachen.

Für das Deeskalationsmanagement offeriert das SAP Business Network zudem Funktionen, mit denen der Abnehmer aufbauend auf spezifische Kriterien nach alternativen Lieferanten suchen kann – insbesondere dann, wenn sich bei diesen mehrere Risikofaktoren aufsummieren. Unternehmen könnten dann bereits im Vorfeld Rahmenverträge mit Ersatzlieferanten abschließen, um die Versorgung sicherzustellen, wenn die Risiken sich realisieren.

Supply-Chain-Management
Neben der strategischen Beschaffungsplanung spielen auch viele operative Aspekte im Supply-Chain-Management eine wichtige Rolle – beispielsweise bei:

- Ermittlung optimaler Bestellmengen,
- Frachtauslastung von Transportmitteln,
- Routen- und Verkehrsmittelplanung sowie
- Reduktion des CO_2-Footprints beim Transport.

Ausgangspunkt hierfür ist ebenfalls häufig eine datenbasierte Betrachtung der bisher verwendeten Transportmittel, -routen und -systeme. Dabei können Unternehmen auf ähnliche Methoden zur Priorisierung zurückgreifen wie in der strategischen Planung – etwa auf ABC- oder Szenarioanalysen. Ansonsten handelt es sich primär um klassische Optimierungsprobleme, mit denen sich die angewandte Mathematik (Operation Research) bereits seit Jahrzehnten beschäftigt und hierfür ein breites Spektrum heuristischer Verfahren entworfen hat – die Stepping-Stone-Methode oder das Potenzialverfahren zur Tourenplanung sind nur zwei Beispiele. Jedenfalls gibt es eine ganze Reihe von Software-Tools, die auf diese oder ähnliche Vorgehensweisen zurückgreifen und die Unternehmen zur Lösung solcher Aufgaben einsetzen können. Durch die SAP BTP lassen sie sich nahtlos in die IT-Infrastruktur einfügen und eine End2End-Prozesskette aufbauen.

EFFIZIENZ IN DER LOGISTIK BEDEUTET, JEDEN SCHRITT ZU OPTIMIEREN UND KONTINUIERLICH NACH VERBESSERUNGEN ZU STREBEN.

Bastian Kempe, Associated Partner, MHP Management- und IT-Beratung, www.mhp.com

Smarte Lieferketten setzen auf den daten- und technologiegetriebenen Netzwerkgedanken, bei dem strategische Supply-Chain-Themen im Vordergrund stehen und der sinnvolle Einsatz von Künstlicher Intelligenz (KI) sowie Internet of Things (IoT) wesentliche Erfolgstreiber sind. Künftige Supply Chains sollten Unternehmen dahingehend ausrichten.

Dr. Sylvia Trage, Bastian Kempe
www.mhp.com

Hardware-Lieferkette

WARUM DIE LIEFERKETTE ZUR ACHILLESFERSE IHRER IT-SICHERHEIT WERDEN KANN

Die betriebliche Ausfallsicherheit wird immer öfter zum Schlagwort von IT- und Unternehmensführung – und das aus gutem Grund. Die globale IT-Infrastruktur ist heute in hohem Maße vernetzt und damit voneinander abhängig. Auch deswegen muss sie gegen eine Vielzahl verschiedener Bedrohungen gewappnet sein. Eines der Risiken, die am häufigsten im Bereich der Cybersicherheit übersehen werden, ist die Herausforderung, Hardware- und Firmware-Bedrohungen zu entschärfen. Dies ist ein blinder Fleck, der in einer kürzlich durchgeführten HP Wolf Security-Umfrage erkannt wurde. Denn die Sicherheit von Hardware-Lieferketten endet nicht mit der Auslieferung der Geräte. Im Gegenteil: Sie erstreckt sich über den gesamten Lebenszyklus der Geräte, die in der Infrastruktur verwendet werden – und darüber hinaus, wenn sie von einem Besitzer zum nächsten weitergegeben werden.

Unterbrechungen der Hardware-Lieferkette können viele Formen annehmen. Diese reichen von einer physischen Unterbrechung durch Ransomware-Gruppen bis hin zur Manipulation von Hardware oder Firmware, um heimlich Malware einzuschleusen. Dies kann in jeder Phase des Lebenszyklus das Gerät als Einfallstor in das Netzwerk nutzen. Diese Angriffe untergraben die Hardware- und Firmware-Grundlagen der Geräte, auf denen die gesamte Software läuft. Daher ist es enorm wichtig, dass Unternehmen Endgeräte einsetzen, die so konzipiert sind, dass sie gegen solche Bedrohungen resistent sind.

Schutz von Anfang bis Ende

Einige Regierungen haben damit begonnen, Maßnahmen zu ergreifen, um die Sicherheit der Lieferkette zu verbessern.

DIE SICHERHEIT VON HARDWARE-LIEFERKETTEN ENDET NICHT MIT DER AUSLIEFERUNG DER GERÄTE.

Dominic Scholl,
Head of Software Sales CEE, HP,
www.hp.com

Eine vollständige Security-Strategie für die Lieferkette erfordert die Einhaltung von Risikomanagement-Prinzipien und den Defense-in-Depth-Ansatz. Natürlich müssen auch Regularien wie Zollbestimmungen, DSGVO oder das IT-Sicherheitsgesetz berücksichtigt werden. Darüber hinaus führt die EU neue Anforderungen an die Cyber-Security in jeder Phase der Lieferkette ein, angefangen bei Software und Diensten mit der Richtlinie über Netz- und Informationssysteme (NIS2) bis hin zu den Geräten selbst mit dem Cyber Resilience Act, um sichere Hardware und Software zu gewährleisten.

In der Zwischenzeit kämpfen Unternehmen mit Hardware- und Firmware-Bedrohungen. 29 Prozent der für die Studie befragten Organisationen gaben an, dass sie oder andere ihnen bekannte Personen von staatlich unterstützten Akteuren betroffen waren. Diese versuchten, bösartige Hardware oder Firmware in PCs oder Drucker einzuschleusen. Vor diesem Hintergrund und der wachsenden Besorgnis über Angriffe auf die Lieferkette müssen Firmen einen neuen Ansatz für die Sicherheit physischer Geräte in Betracht ziehen.

Auswirkungen von Cyber-Angriffen

Die Folgen eines mangelnden Schutzes der Hardware- und Firmware-Integrität von Endgeräten sind schwerwiegend. Angreifer, die erfolgreich Geräte auf der Firmware- oder Hardware-Ebene kompromittieren, erhalten beispiellose Transparenz und Kontrolle. Die Angriffsfläche, die die unteren Schichten des Technologie-Stacks bieten, ist schon seit längerer Zeit Ziel erfahrener und gut ausgestatteter Bedrohungsakteure. Sie können heimlich Malware unterhalb des Betriebssystems (OS) verankern. Ein weiteres Risiko: Diese offensiven Fähigkeiten gelangen leicht in die Hände anderer bösartiger Akteure. Kompromittierte Hardware- oder Firmware-Ebenen sind hartnäckig und geben Angreifern ein hohes Maß an Kontrolle über das gesamte System. Sie sind mit aktuellen Sicherheitstools, die sich in der Regel auf Betriebssystem- und Softwareschichten konzentrieren, nur schwer zu erkennen und zu beheben.

In jüngerer Zeit wurde das BlackLotus UEFI-Bootkit entwickelt, um Boot-Sicherheitsmechanismen zu umgehen und Angreifern die Kontrolle über den Boot-Prozess des Betriebssystems zu geben.

Kein Wunder, dass Unternehmen über Versuche besorgt sind, Geräte während der Übertragung zu manipulieren. Viele berichten, dass sie nicht in der Lage sind, solche Bedrohungen zu erkennen und zu stoppen. 75 Prozent der teilnehmenden

Unternehmen gaben an, dass sie eine Möglichkeit benötigen, um die Hardware-Integrität zu überprüfen. Nur dann sind sie in der Lage, Bedrohungen durch Gerätemanipulationen einzudämmen.

Um die Sicherheit von Hardware und Firmware zu gewährleisten, ist es wichtig, Technologieanbieter und -lieferanten mit vertrauenswürdigen Design-, Entwicklungs- und Herstellungsprozessen auszuwählen. Außerdem sollten Unternehmen modernste Technologien einsetzen. Diese unterstützen dabei, die Geräteintegrität über den gesamten Lebenszyklus des Geräts hinweg zu überprüfen, zu verwalten und zu überwachen – von der Herstellung bis zum Ende des Lebenszyklus oder der Wiederverwendung.

Ausgereifte Sicherheit

Mittlerweile gibt es eine Reihe von ausgereiften Prozessen, um die Softwaresicherheitskonfiguration über die gesamte Lebensdauer eines Geräts zu verwalten und zu kontrollieren. Darüber hinaus verbessert sich auch die Fähigkeit, die Herkunft der Software und die Sicherheit der Lieferkette zu verfolgen. Nun ist es an der Zeit, die Verwaltung und Überwachung der Hardware- und Firmware-Sicherheit über den gesamten Lebenszyklus von Endgeräten auf den gleichen Stand zu bringen. Denn Geräte sind die Hardware-Lieferkette einer Firma, solange sie verwendet werden.

Die technischen Möglichkeiten, um dies geräteübergreifend zu ermöglichen, waren bisher nicht umfangreich verfügbar. Der Grund: Alle Maßnahmen müssen auf Security by Design basieren und direkt in die Hardware-Entwicklung einfließen. Inzwischen sind die Grundlagen dafür geschaffen. Unternehmen sollten damit beginnen, die von Herstellern und Geräten zur Verfügung gestellten Funktionen für Sicherheit und Widerstandsfähigkeit aktiv zu nutzen. So können sie aktiv die Kontrolle über das Sicherheitsmanagement von Hardware und Firmware über den gesamten Lebenszyklus ihrer Geräte hinweg übernehmen.

Es gibt vier wichtige Schritte, mit denen Unternehmen die Sicherheit von Geräte-Hardware und -firmware proaktiv verwalten können:

- Sichere Verwaltung der Firmware-Konfiguration während des gesamten Lebenszyklus eines Geräts. Hier kommen digitale Zertifikate und Public-Key-Kryptografie ins Spiel. Administratoren sind dadurch in der Lage, die Firmware remote zu verwalten und eine schwache kennwortbasierte Authentifizierung zu vermeiden.

- Werksdienste der Hersteller nutzen, um stabile Hardware- und Firmware-Sicherheitskonfigurationen direkt ab Werk zu ermöglichen.

- Mit der Plattformzertifikatstechnologie die Integrität von Hardware und Firmware nach der Auslieferung der Geräte überprüfen.

- Konformität der Hardware- und Firmware-Konfiguration der Geräteflotte kontrollieren.

Die System-Security beruht auf einer starken Sicherheit der Lieferkette. Im ersten Schritt muss gewährleistet sein, dass die Geräte mit den vorgesehenen Komponenten gebaut und geliefert werden. Aus diesem Grund sollten sich Unternehmen zunehmend auf die Entwicklung sicherer Hardware- und Firmware-Grundlagen konzentrieren. Dies ermöglicht ihnen, die Hardware- und Firmware-Sicherheit während des gesamten Lebenszyklus jedes Geräts in ihrer Flotte zu verwalten, zu überwachen und zu beheben.

Dominic Scholl

CEO FRAUD

HAPPY END DURCH INTERPOL

Im Juli 2024 ereignete sich einer der bedeutendsten Fälle von Business E-Mail Compromise (BEC) Betrug. Ein Unternehmen mit Sitz in Singapur wurde dabei Opfer eines ausgeklügelten Betrugsschemas. Die Täter gingen dabei höchst raffiniert vor: Sie gaben sich als legitimer Zulieferer des betroffenen Unternehmens aus und forderten in einer täuschend echt wirkenden E-Mail die Überweisung einer vermeintlich ausstehenden Zahlung. Als Zahlungsziel wurde ein neues Bankkonto in Osttimor angegeben.

Ahnungslos überwies die Firma am 19. Juli 42,3 Millionen US-Dollar an das Betrügerkonto. Erst vier Tage später, als der echte Zulieferer sich meldete und die nicht erhaltene Zahlung einforderte, flog der Schwindel auf.

Schnelle internationale Reaktion dank Interpol

Das Unternehmen reagierte prompt und schaltete die Polizei ein. Diese wendete sich wiederum an Interpol. Innerhalb weniger Tage konnten 39 Millionen US-Dollar vom Betrügerkonto eingefroren werden. Darüber hinaus führten weitere Ermittlungen in Osttimor zur Festnahme von sieben Tatverdächtigen und zur Rückführung von weiteren über 2 Millionen US-Dollar an die Opferfirma in Singapur.

„Schnelles Handeln ist entscheidend, um die Erlöse aus Onlinebetrügereien abzuschöpfen", betonte Isaac Oginni, Direktor des Interpol-Zentrums für Finanzdelikte und Korruptionsbekämpfung. „Die enge Zusammenarbeit zwischen den Behörden in Singapur und Osttimor in diesem Fall ist ein hervorragendes Beispiel dafür, wie Interpol dabei helfen kann, die Opfer zu entschädigen und die Täter zu überführen."

Wie funktioniert CEO Fraud?

CEO Fraud, auch bekannt als Business E-Mail Compromise (BEC), ist eine immer raffinierter werdende Form des Finanzbetrugs. Dabei erlangen Kriminelle Zugriff auf E-Mail-Konten von Führungskräften oder imitieren deren Identität, um Mitarbeiter gezielt zu täuschen und sie dazu zu bringen, Überweisungen an Scheinkonten vorzunehmen.

Der typische Ablauf sieht wie folgt aus: Die Täter verschaffen sich zunächst Zugang zu einem E-Mail-Konto einer Führungskraft, zum Beispiel des Geschäftsführers oder Finanzvorstands. Dann senden sie von diesem Konto eine Nachricht an Mitarbeiter im Rechnungswesen oder der Finanzverwaltung, in der sie um eine dringende Überweisung auf ein neues Konto bitten. Dabei imitieren sie den Schreibstil und die Gepflogenheiten der betroffenen Führungskraft, um die Authentizität der Anfrage vorzutäuschen. Manchmal, wie in dem Beispiel des Unternehmens aus Singapur, weichen die verwendeten E-Mail-Adressen nur geringfügig von den offiziellen Adressen ab.

Oftmals gelingt es den Kriminellen so, hohe sechs- oder gar siebenstellige Summen auf ihre Konten umleiten zu lassen, bevor der Betrug auffliegt.

Der Vorfall in Singapur unterstreicht eindrücklich die anhaltende Bedrohung durch BEC-Betrügereien und verdeutlicht die Notwendigkeit strenger Überprüfungsprozesse bei jeglichen Änderungen von Zahlungsinformationen.

Lars Becker | www.it-daily.net

Digitale Transformation in der Logistik

CHECKLISTE: WAS EINE ZENTRALE DATENDREHSCHEIBE KÖNNEN MUSS

Ein wichtiger Erfolgsfaktor der digitalen Transformation ist der Datenaustausch. Problematisch ist dieser vor allem dann, wenn es um Daten aus unterschiedlichen Systemen und mit verschiedenen Formaten geht. Für die Konsolidierung dieser heterogenen Ausgangslage bietet sich die Nutzung einer modernen Datendrehscheibe an. Diese Daten- und Prozessintegrationsplattform fungiert wie ein zentraler Hub, der die Daten der aller am Logistikprozess beteiligten Sensor- und IT-Systeme zusammenbringt und nutzbar macht.

Die nachstehende Checkliste bietet den Verantwortlichen des Logistikmanagements sowie der IT eine gute Orientierung bei der Suche nach dem passenden Datenkatalysator. Sie fasst die sieben wichtigsten Aspekte zusammen, auf die es bei der Einführung einer Datendrehscheibe ankommt.

#1 Standardisierte Schnittstellen

Die Implementierung standardisierter Schnittstellen und Datenformate ist entscheidend. Sie sorgen für die Interoperabilität zwischen den verschiedenen Systemen. Das kann die Verwendung von branchenüblichen Standards wie EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) oder modernen APIs umfassen.

#2 Sicherheits- und Datenschutzmaßnahmen

Die Implementierung umfassender Sicherheits- und Datenschutzmaßnahmen ist unerlässlich und sollte vor der Einführung einer zentralen Datendrehscheibe erfolgen. Empfohlen werden Lösungen für die Datenverschlüsselung, Zugangskontrolle, Überwachung sowie Audits.

#3 Integration von IoT-Technologien

Die Integration von Internet of Things (IoT)-Technologien ermöglicht die Echtzeitüberwachung von physischen Assets, wie beispielsweise von Containern, Fahrzeugen, Ausrüstungen. Außerdem unterstützen sie den Datenaustausch und deren Nutzung – unabhängig davon, dass IoT-Technologien die Effizienz des Prozessmanagements grundsätzlich verbessern.

#4 Berücksichtigung von Big Data und Analytics

Die Nutzung von Big-Data-Technologien und Analytics hilft, wertvolle Erkenntnisse aus den umfangreichen Datenmengen zu gewinnen, die während des Logistikprozesses generiert werden. Im Zusammenspiel mit einer zentralen Datendrehscheibe kann das zu einer weiteren Optimierung von Abläufen und besseren Nutzung von Ressourcen beitragen.

#5 Mobile Anwendungen

Die Entwicklung von mobilen Anwendungen für verschiedene Benutzergruppen ermöglicht eine flexible und standortunabhängige Nutzung der Systeme, im Hafen beispielsweise des PCS (Port Community System). Auch die hier genutzten Daten sollten unbedingt in der zentralen Datendrehscheibe konsolidiert werden.

#6 Robuste Ausfallsicherheit und Redundanz

Die Architektur sollte Mechanismen für Ausfallsicherheit und Redundanz beinhalten. Damit wird sichergestellt, dass die Steuerungssysteme auch bei technischen Problemen oder Ausfällen zuverlässig arbeiten – eine Anforderung, die auch ein zentraler Datenhub erfüllen muss.

#7 Berücksichtigung von Legacy-Systemen

Sollten Legacy-Systeme zum Einsatz kommen, ist es wichtig, dass auch deren Daten in das Gesamtsystem integriert werden. Schnittstellen und Konverter können erforderlich sein, um die nahtlose Interaktion der Datendrehscheibe mit älteren Technologien zu gewährleisten.

Fazit

Logistikunternehmen, die diese Aspekte frühzeitig berücksichtigen, verschaffen sich damit optimale Voraussetzungen für eine erfolgreiche Transformation ihres Managementprozesses. Das bringt ihnen nicht nur strukturelle Vorteile und erhöht die Zukunftssicherheit, sondern verbessert auch die Wettbewerbsfähigkeit im stark umkämpften internationalen Logistikmarkt.

Volker Hettich | www.compacer.com

KI-basierte Assistenten im IT-Self-Service

SO ENTLASTEN SIE IHREN SERVICEDESK

In einer zunehmend digitalisierten Welt, in der IT-Systeme das Rückgrat vieler Unternehmen bilden, steigt auch der Bedarf an effizientem IT-Support. Der Einsatz von KI-basierten Assistenten im IT-Self-Service bietet eine vielversprechende Möglichkeit, den Servicedesk zu entlasten und gleichzeitig die Benutzerzufriedenheit zu steigern. Dieser Artikel beleuchtet, wofür virtuelle Assistenten im IT-Umfeld eingesetzt werden können, welche Besonderheiten es in diesem Bereich gibt und welche Merkmale ein leistungsfähiger virtueller Assistent mitbringen sollte.

Wofür man die virtuellen Assistenten einsetzen kann

Virtuelle Assistenten, auch als Chatbots oder digitale Helfer bekannt, können in einer Vielzahl von IT-Szenarien eingesetzt werden. Ihre Stärke liegt in der Automatisierung von Routineaufgaben und der schnellen Bereitstellung von Informationen. Zu den wichtigsten Einsatzmöglichkeiten zählen:

➤ **Fragen beantworten:**
Ein KI-basierter Assistent kann häufig gestellte Fragen (FAQs) beantworten, wie etwa „Wie setze ich mein Passwort zurück?“ oder „Wo finde ich die VPN-Einstellungen?“. Durch den Zugriff auf eine Wissensdatenbank kann der Assistent sofort Antworten liefern, ohne dass ein menschlicher Servicedesk-Mitarbeiter eingreifen muss.

➤ **Störungen beheben:**
Der Assistent kann Störungen diagnostizieren und beheben, indem er Benutzer durch standardisierte Lösungsschritte führt. Beispielsweise kann er bei einem Druckerproblem helfen, indem er den Benutzer anleitet, die Verbindung zum Netzwerk zu überprüfen oder den Treiber neu zu installieren.

➤ **Services starten:**
Ein weiterer Nutzen virtueller Assistenten ist die Fähigkeit, IT-Services zu starten oder anzupassen. Der Assistent kann beispielsweise einen Software-Installationsprozess initiieren, Berechtigungen verwalten oder einen neuen Benutzeraccount anlegen.

Die Besonderheiten im IT- und Enterprise-Service

Der Einsatz von KI-Assistenten im IT- und Enterprise-Service unterscheidet sich von anderen Servicebereichen durch spezifische Herausforderungen und Anforderungen:

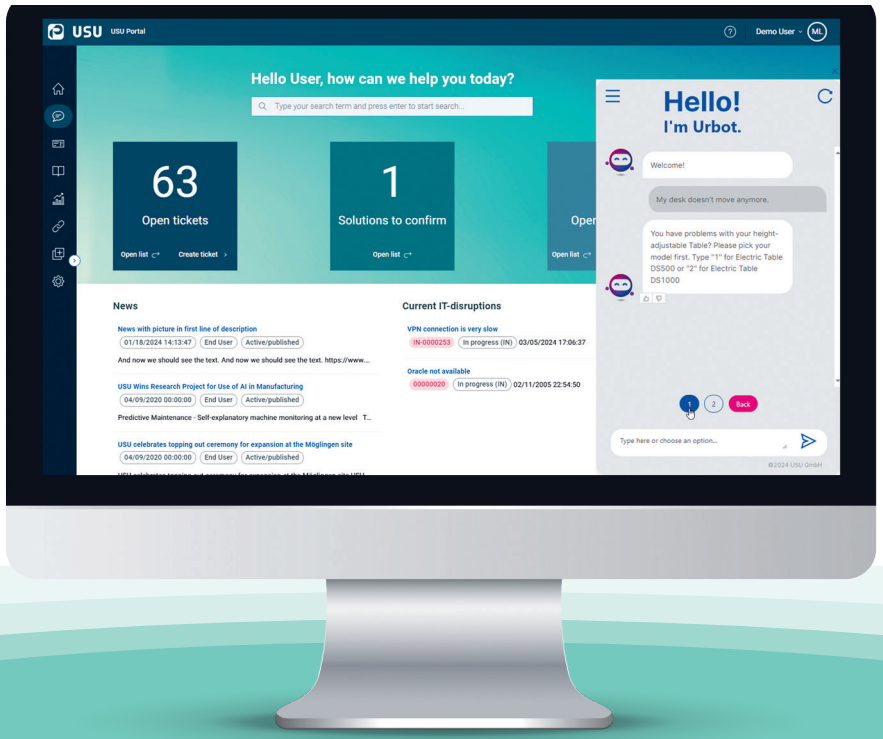
➤ **Begrenzte und bekannte Use Cases:**
Im Gegensatz zu allgemeinen Kundenservices sind die Anwendungsfälle im IT-Support oft klar definiert und wiederholen sich. Ein virtueller Assistent muss daher nicht für unerwartete oder vollkommen neue Anfragen gewappnet sein. Dies ermöglicht eine gezielte Optimierung des Assistenten auf spezifische, häufig auftretende Probleme.

➤ **Schrittweise Erweiterbarkeit:**
Da sich IT-Umgebungen kontinuierlich weiterentwickeln, sollte ein virtueller Assistent so konzipiert sein, dass er leicht um neue Use Cases erweitert werden kann. Diese Erweiterungen sollten ohne großen Aufwand möglich sein, um sicherzustellen, dass der Assistent immer auf dem neuesten Stand bleibt und den aktuellen Bedürfnissen des Unternehmens gerecht wird.

Die Merkmale eines effizienten, virtuellen Assistenten

Um in der Praxis effektiv zu sein, sollte ein virtueller Assistent im IT-Self-Service über bestimmte Eigenschaften verfügen:

➤ **Einfache Erweiterbarkeit ohne exponentiellen Pflegeaufwand:**
Ein virtueller Assistent sollte so gestaltet sein, dass neue Use Cases einfach hinzugefügt werden können, ohne dass der Wartungsaufwand überproportional ansteigt. Dies erfordert eine modulare Architektur und eine intuitive Benutzeroberfläche zur Konfiguration. Kern einer solchen Multi-Bot-Architektur ist, dass ein Bot nur für einen speziellen Use Case zuständig ist. Ein sogenannter „Lead-Bot“ erkennt den Use Case und leitet die Anfrage and den zuständigen „Expert-Bot“ weiter. So können Schritt für Schritt neue Expert-Bots hinzugefügt werden, ohne dass dies Auswirkungen auf die bisherigen Bots hat. Ein Nachteil herkömmlicher Single-Bot-Architekturen kann so vermieden werden: hier müssen alle Use Cases von einem einzigen Bot abgedeckt werden. Dieser wird so immer „mächtiger“ und somit aber auch schwerer zu warten. Nebeneffekte auf bisher funktionierende Use Cases sind häufig die Folge.



Self-Service-Portal mit Virtuellem Agenten

(Quelle: USU Software AG)

➤ Sofortiger Einsatz von KI ohne vorhergehendes Training:

Da die Use Cases in der Anzahl begrenzt sind sollte die eingesetzte KI auch ohne vorhergehendes Training mit Massendaten in der Lage sein, die Benutzer zu unterstützen. Somit entfällt auch das ständige Weitertrainieren beim Hinzufügen weiterer Use Cases.

➤ Nutzung von Generativer KI (GenAI):

Durch die Integration von GenAI-Technologien kann der Assistent nicht nur vorgegebene Antworten liefern, sondern auch kontextbezogen neue Antworten auf Basis der Wissensdatenbank generieren. Dies erweitert den Anwendungsbereich und entlastet die Serviceorganisation.

➤ Weiterleitung an Sachbearbeiter oder Ticket-Erstellung:

Wenn der Assistent ein Problem nicht selbst lösen kann, muss er in der Lage sein, den Fall an einen menschlichen Mitarbeiter weiterzuleiten oder ein Support-Ticket zu erstellen. Diese Fähigkeit ist entscheidend, um sicherzustellen, dass komplexe Probleme nicht unbeantwortet bleiben und der Benutzer nicht im Stich gelassen wird.

➤ Integration in ein Self-Service-Portal:

Der virtuelle Assistent sollte nahtlos in das bestehende Self-Service-Portal integriert werden. Dies erleichtert den Zugriff für die Benutzer und stellt sicher, dass der Assistent in das bestehende IT-Ökosystem eingebettet ist, was seine Effektivität und Benutzerakzeptanz erhöht.

➤ Fähigkeit zur Durchführung von Transaktionen:

Ein fortschrittlicher virtueller Assistent sollte nicht nur Fragen beantworten, sondern auch aktiv Transaktionen starten können. Beispiele für die transaktionsgesteuerte Lösung technischer Probleme sind das Neustarten eines Servers oder das Zurücksetzen eines Passworts. Auch aber auf dem Client des Endbenutzers sollten Self-Healing-Prozesse gestartet werden können, wie das Leeren des Browser-Caches oder die Korrektur von Browser-Einstellungen. Weitere sinnvolle transaktionsgesteuerte Use Cases sind die Ausführung von Software-Installationen oder das Buchen von Urlauben und Seminaren.

Fazit

KI-basierte Assistenten bieten enormes Potenzial, um den IT-Support effizienter zu gestalten und den Servicedesk zu entlasten. Sie können Routineaufgaben übernehmen, einfache Probleme lösen und Benutzer durch komplexe IT-Landschaften navigieren. Um jedoch das volle Potenzial dieser Technologie auszuschöpfen, müssen virtuelle Assistenten speziell auf die Anforderungen des IT-Supports zugeschnitten sein. Dazu gehören die einfache Erweiterbarkeit, die Integration in bestehende Systeme, die Fähigkeit zur Durchführung von Transaktionen und die Nutzung fortschrittlicher KI-Technologien. Richtig implementiert, können diese Assistenten nicht nur die Produktivität steigern, sondern auch die Zufriedenheit der Benutzer erheblich verbessern.

Martin Landis | www.usu.com

Zukunftssicheres Service Management

ERFOLGSFAKTOREN FÜR TOOLBESCHAFFUNG UND DIE ROLLE DER KÜNSTLICHEN INTELLIGENZ

Die digitale Transformation gewinnt zunehmend an Bedeutung, besonders für Unternehmen mit mehr als 200 PC-Arbeitsplätzen. Ein effizientes IT- und Enterprise Service Management (ITSM/ESM) wird unverzichtbar, da viele Betriebe ihre Prozesse mit IT-Tools modernisieren und zukunftssicher aufstellen müssen.

Unternehmen mit bestehender Service Management Software stoßen häufig an Grenzen in Bezug auf Effizienz, Skalierbarkeit oder technische Integration, während andere noch mit ineffizienten, manuellen Prozessen arbeiten. In beiden Szenarien ist es entscheidend, den Tool-Evaluierungsprozess zu verstehen, die Erfolgsfaktoren für die Implementierung oder einen Wechsel zu kennen und die Rolle der Künstlichen Intelligenz (KI) im modernen Service Management zu berücksichtigen.

10 Gründe für die Neueinführung oder den Wechsel einer Service Management Software

Die Einführung oder der Wechsel einer Service Management Software wird durch zahlreiche Faktoren getrieben. Unternehmen ohne technische Hilfsmittel kämpfen oft mit ineffizienten, manuellen Prozessen, die zu Intransparenz, Fehlern und Überforderung führen. Unternehmen mit einem bestehenden Tool ziehen einen Wechsel in Betracht, wenn es etwa Integrationsprobleme oder unzureichenden Support gibt. Die verbreitetsten Gründe sind:

#1 Unübersichtliche, manuelle Prozesse:
Ohne Tool entstehen durch manuelle Abläufe Fehler und Doppelspurigkeiten.

#2 Skalierbarkeit:
Wachsende Unternehmen benötigen Tools, die mit ihnen mitwachsen.

#3 Fehlende Automatisierung:
Hoher manueller Aufwand wird durch Automatisierung in modernen ITSM/ESM-Tools reduziert.

#4 Veraltete Technologie:
Alte Systeme behindern oft die Integration neuer Technologien.

#5 Fehlende mobile Unterstützung:
Gerade im mobilen Arbeiten sind Lösungen mit mobilen und Remote-Funktionen entscheidend.

#6 Schlechte Benutzerfreundlichkeit:
Komplizierte Tools mindern die Effizienz und Zufriedenheit der Nutzer.

#7 Hohe Betriebskosten:
Veraltete Systeme führen zu erhöhten Kosten.

#8 Betriebsmodell:
Unternehmen wechseln zu Anbietern, die On-Premise-Optionen oder flexible Cloud-Lösungen bieten.

#9 Schlechter Service & Support:
Langsame Reaktionszeiten und umständliche Support-Strukturen führen oft zum Wechsel.

#10 Sprachbarrieren:
Fehlende Unterstützung in der Sprache des Unternehmens erschwert die Zusammenarbeit.

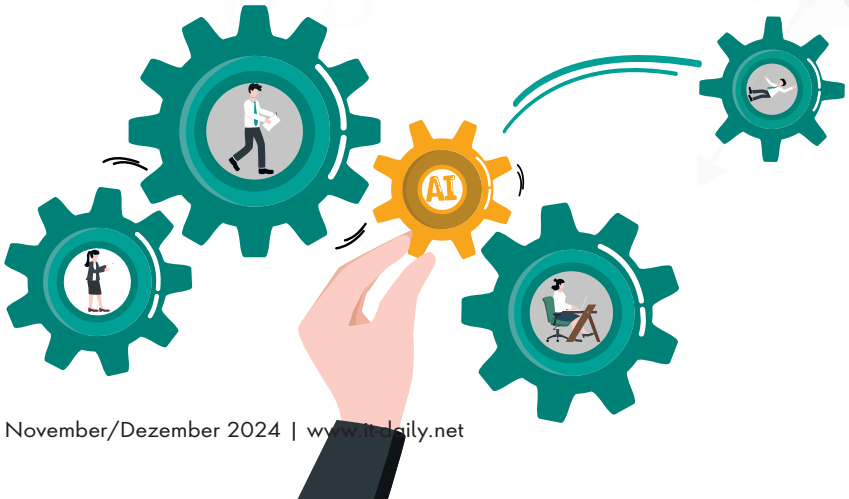
Die „8 Steps" für eine erfolgreiche Tool-Neuevaluation

Unabhängig davon, ob ein Unternehmen eine neue IT- und Enterprise Service Management Lösung sucht oder ein bestehendes Tool ersetzen möchte – der Prozess der Neuevaluation sollte strukturiert und systematisch ablaufen. Nachfolgend sind die acht wichtigsten Schritte für eine erfolgreiche Tool-Evaluation aufgelistet:

#1 Anforderungsdefinition:
Anforderungen, die sich an den Zielen des Unternehmens orientieren, bilden die Grundlage für die Implementierung.

#2 Business Case:
Ein Business Case quantifiziert den Nutzen und hilft, die Entscheidung gegenüber Stakeholdern zu rechtfertigen.

#3 Einbindung relevanter Stakeholder:
Alle betroffenen Abteilungen und Endnutzer sollten frühzeitig einbezogen werden.



#4 Mitarbeiterzufriedenheit: Die Einführung des Tools sollte auch die Zufriedenheit und das Engagement der Mitarbeiter fördern.

#5 Marktanalyse: Flexibilität, Skalierbarkeit, Sicherheitsfunktionen und Integrationsfähigkeit sind wichtige Kriterien bei der Auswahl eines Tools.

#6 Proof of Concept (PoC): Eine Testphase stellt sicher, dass das Tool in der Praxis funktioniert.

#7 Anbieterauswahl und Vertragsverhandlungen: Faktoren wie Support, Sprache und Preis-Leistungs-Verhältnis sollten berücksichtigt werden.

#8 Implementierungsplan: Ein detaillierter Plan mit klaren Verantwortlichkeiten und Meilensteinen ist entscheidend für eine erfolgreiche Einführung.

UNTERNEHMEN MÜSSEN IHRE SERVICE MANAGEMENT-PROZESSE IM ZUGE DER DIGITALEN TRANSFORMATION MODERNISIEREN.

David Cohen, Marketing & Communication Manager, KYBERNA, www.kyberna.com

Die Rolle von KI in einem zukunftssicheren Service Management

Künstliche Intelligenz spielt eine zunehmend wichtige Rolle im Service Management. Durch den Einsatz von KI können Routineaufgaben automatisiert, Prozesse optimiert und effizienter gestaltet werden. Die Vorteile von KI-Integrationen sind vielfältig und müssen heute bereits in der Evaluationsphase berücksichtig werden.

> **Effizienzsteigerung:** Automatische Lösungsvorschläge und Ticketklassifizierung reduzieren die Bearbeitungszeit signifikant.

> **Verbesserung der Nutzererfahrung:** Chatbots und ähnliche Technologien bieten rund um die Uhr Unterstützung.

> **Wissensgenerierung:** KI kann dabei helfen, Knowledge Base Artikel zu schreiben und so Lösungen und Abläufe zu dokumentieren. Dadurch wird Wissen für das Unternehmen generiert und gleichzeitig auch die KI stetig verbessert.

So werden Funktionen wie KI-basierte Supportassistent mit automatischen Lösungsvorschlägen, Unterstützung bei der Generierung von Wissen/Knowledge Base Artikeln, Chatbots für automatisierten Support und das Vorschlagen ähnlicher Tickets oder Knowledge Base Artikeln verbreitet in ITSM Tools zu finden sein. Diese Funktionen haben das Potenzial, die Effizienz erheblich zu steigern, die Antwortzeiten zu verkürzen und die allgemeine Zufriedenheit der Endnutzer zu verbessern.

Nicht ausser Acht lassen darf man in diesem ganzen Hype um Künstliche Intelligenz die Datensicherheit. ITSM Hersteller sind sich der Bedenken bewusst und arbeiten kontinuierlich daran, die höchsten Sicherheitsstandards zu erfüllen und Vertrauen in die Nutzung von KI-Technologien zu fördern. Der KI-Sicherheitsaspekt sollte also in der Tool-Evaluation zwingend berücksichtigt werden.

Takeaways und Schlüsselerkenntnisse

Unternehmen müssen ihre Service Management-Prozesse im Zuge der digitalen Transformation modernisieren. Die Einführung oder der Wechsel zu einer modernen ITSM- oder ESM-Software bietet klare Vorteile, darunter Automatisierung, Skalierbarkeit und die Unterstützung mobiler Arbeitsumgebungen. Drei Schlüsselerkenntnisse sind:

#1 Effizienzsteigerung und Automatisierung: Moderne ITSM- und ESM-Lösungen reduzieren den manuellen Arbeitsaufwand und steigern die Effizienz.

#2 Bedeutung einer sorgfältigen Evaluierung: Eine strukturierte Evaluierung, die sich an den Zielen des Unternehmens orientiert, stellt den langfristigen Nutzen sicher.

#3 Wachsende Rolle der Künstlichen Intelligenz: KI verbessert die Nutzererfahrung, beschleunigt Prozesse und fördert die Wissensgenerierung, wobei Sicherheitsaspekte besonders berücksichtigt werden müssen.

Lösung der Zukunft

Die IT- und Enterprise Service Management Software ky2help® von KYBERNA bietet umfassende Funktionen für Unternehmen, die eine flexible und zukunftssichere Lösung suchen. Sie unterstützt sowohl On-Premises- als auch SaaS-Modelle (Private Cloud, Datenstandort EU) und passt sich den individuellen Anforderungen des Unternehmens an. Durch die Integration von Automatisierung und benutzerfreundlichen Schnittstellen optimiert ky2help® die Prozesse und maximiert die IT-Betriebszeit. KYBERNA agiert als direkter Ansprechpartner und begleitet Unternehmen von der Implementierung bis zum Support – und das zu 100 Prozent in deutscher Sprache.

David Cohen

MEHR WERT
ky2help®: Booster für Workflows

AI & IT Service Management

KÜNSTLICHE INTELLIGENZ IN DER PROZESSOPTIMIERUNG

Künstliche Intelligenz (KI) spielt zunehmend eine zentrale Rolle für die Optimierung von Geschäftsprozessen. Besonders im IT-Service-Management (ITSM) eröffnet KI neue Möglichkeiten, Abläufe effizienter und flexibler zu gestalten. Atlassian Intelligence – die neue KI der Atlassian-Tools – automatisiert Routineaufgaben und ermöglicht datenbasierte Entscheidungen in Echtzeit. Jodocus – Now Part of Eficode, hat das Potenzial von KI frühzeitig erkannt und seine Expertise in den Bereichen ITSM, Cloud und Collaboration weiter ausgebaut – durch eine übergeordnete Focus-Line für KI.

Künstliche Intelligenz prägt zunehmend die Geschäftswelt und wird zum entscheidenden Faktor für Effizienzsteigerungen und Prozessoptimierungen. Die Einsatzmöglichkeiten von KI sind dabei vielfältig – von der Automatisierung alltäglicher Aufgaben bis zur Unterstützung komplexer Herausforderungen. Für Unternehmen ist KI nicht nur eine technologische Weiterentwicklung, sondern ein strategisches Instrument, das langfristige Wettbewerbsvorteile ermöglicht.

UNTERNEHMEN, DIE FRÜHZEITIG AUF KI-TECHNOLOGIEN SETZEN, STEIGERN DIE EFFIZIENZ IHRER GESCHÄFTSPROZESSE UND SICHERN SICH GLEICHZEITIG LANGFRISTIGE WETTBEWERBSVORTEILE

Christopher Mohr, Managing Consultant, Jodocus – Now Part of Eficode, www.jodocus.io/de

Die Möglichkeit, wiederkehrende Aufgaben durch KI zu automatisieren, bedeutet neben der zum Teil enormen Zeitersparnis eine erhebliche Steigerung der Effizienz. Besonders in Bereichen wie dem IT-Service-Management (ITSM) beziehungsweise dem Enterprise-Service-Management (ESM) hat die Prozessautomatisierung durch KI das Potenzial, Prozesse zu verschlanken und flexibler zu gestalten.

KI als Schlüsseltechnologie

ITSM-Lösungen waren lange auf starre, manuell gesteuerte Abläufe angewiesen. Künstliche Intelligenz hat diese Landschaft verändert. Heute bieten KI-gestützte Tools die Möglichkeit, Prozesse flexibler und schneller zu gestalten. Ein konkretes Beispiel für den Einsatz von KünstlicherIntelligenzimIT-Service-Management ist Jira Service Management (JSM): Mit der Integration von KI-Funktionen durch Atlassian Intelligence wird herkömmliches Service-, Incident- und Problem-Management in JSM noch effizienter. Die Lösung beinhaltet eine Reihe an KI-gestützten Funktionen, die in der gesamten firmeneigenen Cloud verfügbar sind – etwa in Jira, JSM und Co. Dazu werden interne sowie von OpenAI entwickelte künstliche Intelligenz genutzt.

Die KI-gesteuerten Automatisierungen ermöglichen beispielsweise eine schnelle Priorisierung von Anfragen, das automatische Routing von Tickets und das proaktive Erkennen von Störungen, bevor sie kritische Auswirkungen haben. Genauso helfen KI-unterstützte Kollaborationsplattformen wie Confluence Unternehmen dabei, die Kommunikation effizienter zu gestalten und projektübergreifende Abläufe zu vereinfachen.

Ob beim Brainstorming, Zusammenfassen von Inhalten, Automatisieren von Aufgabenverteilungen: KI-Assistenten können die Arbeit von Teams in nahezu allen Bereichen optimieren. Dabei darf der Einsatz von KI jedoch nicht isoliert betrachtet werden. Denn auch wenn Atlassian Intelligence in der gesamten Cloud verfügbar ist, muss die jeweilige Instanz auf die Geschäftsprozesse angepasst sein.

Treiber der KI-Entwicklung

Die Implementierung von KI erfordert neben der technischen Basis vor allem Expertise in der Konfiguration und Anpassung von Lösungen. Spezialisierte Partner, die in der Implementierung von KI-gestützten Tools erfahren sind, spielen hierbei eine Schlüsselrolle. Christopher Mohr, Managing Consultant Jodocus GmbH, setzt sich täglich mit diesen Herausforderungen auseinander und sieht den dringenden Handlungsbedarf bei vielen Unternehmen als Chance: „Unternehmen, die frühzeitig auf KI-Technologien setzen, steigern die Effizienz Ihrer Geschäftsprozesse und sichern sich gleichzeitig langfristige Wettbewerbsvorteile."

Das Unternehmen ist als Atlassian Solution Partner ausgewiesener Produktex-

perte und unterstützt Unternehmen unter anderem bei der Produktkonfiguration, Anpassung von Lösungen und der Implementierung der Tools sowie beim Lizenzmanagement. Seit der Einführung Ende 2023 hat sich das Hamburger IT-Unternehmen nochmal verstärkt auf KI-Lösungen spezialisiert und das auch in seiner strategischen Ausrichtung forciert.

Fokus auf KI

IT-Unternehmen sind meist Taktgeber beim technischen Fortschritt, müssen sich dafür aber auch ständig an moderne Lösungen und Trends anpassen – oder diese selbst setzen. Als Platinum Partner hat die Jodocus GmbH verschiedene Spezialisierungen im Atlassian-Umfeld erreicht und seine Expertise in drei klar definierten Business-Lines aufgebaut:

- **ITSM/ESM:** Optimierung und Automatisierung von IT- und Enterprise-Service-Management-Prozessen (zum Beispiel mit Jira Service Management).
- **Cloud/Cloud Migration:** Unterstützung bei der Migration und Optimierung von Cloud-Infrastrukturen.
- **Collaboration:** Verbesserung der Zusammenarbeit und Workflows.

Die drei Bereiche decken die wesentlichen Anforderungen für die Optimierung von IT-Infrastrukturen und Geschäftsprozessen ab. Um jedoch den Anforderungen der Zukunft gerecht zu werden, wurde über die bestehenden Business-Lines hinaus eine übergeordnete Focus-Line für KI eingeführt. Damit reagieren die IT-Spezialisten auf die rasante KI-Entwicklung und gehen neben der Arbeit im Atlassian-Umfeld noch weiter: „Wir nutzen die Möglichkeiten der Künstlichen Intelligenz innerhalb des Atlassian-Ökosystems, setzen aber gleichermaßen auf zusätzliche KI-Tools, um neue Effizienzniveau für unsere Kunden zu erreichen“, erläutert Jan Szczepanski, Head of Marketing bei der Jodocus GmbH.

Damit zeigen sich die IT-Spezialisten als flexible Partner für technologische Entwicklungen, um Herausforderungen von Unternehmen individuell zu bewältigen. „KI-basierte Prozessoptimierung ist nicht nur eine technologische Neuerung – sie verändert grundlegend, wie Unternehmen ihre Abläufe steuern können und müssen“, fasst Szczepanski zusammen.

KI-BASIERTE PROZESSOPTIMIERUNG IST NICHT NUR EINE TECHNOLOGISCHE NEUERUNG – SIE VERÄNDERT GRUNDLEGEND, WIE UNTERNEHMEN IHRE ABLÄUFE STEUERN KÖNNEN UND MÜSSEN.

Jan Szczepanski,
Head of Marketing,
Jodocus – Now Part of Eficode
www.jodocus.io/de

Ausblick: KI als entscheidender Faktor

Ob im IT-Service-Management oder bei der Optimierung von Geschäftsprozessen: Unternehmen benötigen heute Tools, um ihre Abläufe effizient und flexibel zu steuern.

Tools wie Jira Service Management bieten Optionen, ITSM-Prozesse out-of-the-box zu unterstützen und gleichzeitig an die spezifischen Anforderungen von Unternehmen anzupassen. Atlassian Intelligence und weitere KI-Technologien heben diese Möglichkeiten jetzt nochmal auf ein neues Level. Und das ist erst der Anfang der KI-Revolution in der Arbeitswelt: „Wir sehen großes Potenzial darin, KI-Lösungen weiterzuentwickeln und sie zu verbinden. So können wir Prozesse noch individueller und damit effizienter gestalten“, schließt Szczepanski ab.

Vincent Effertz

IT-Plattform-Economy

IT-BRANCHE DURCHLÄUFT BIS 2030 MASSIVE KONSOLIDIERUNG MIT FOKUS AUF AUTOMATISIERUNG UND INTEGRATION

Für die Orchestrierung der zahlreichen IT-Silos aus den vergangenen Jahren brauchen die IT-Verantwortlichen nicht nur Enterprise-Architekten, sondern auch eine passende und robuste Infrastruktur. Somit entstand in den vergangenen Jahren eine lebendige IT-Plattform-Economy, die nun konsolidierte werden muss, denn eine Meta-Ebene für eine Plattform in Form einer weiteren Plattform erscheint kontraproduktiv.

Bereits SAP-Ex-Technikvorstand Shai Agassi erkannte die Kraft einer IT-Plattform für unterschiedliche Algorithmen und Applikationen. Mit NetWeaver schuf er bei SAP eine Funktionssammlung hochwertiger Programme.

Auf dem vergangenen Steampunk und BTP Summit in Heidelberg Anfang 2024 kritisierte Scheer-CTO Wolfram Jost den SAP-Ansatz erneut: Wie beim SAP NetWeaver erscheint auch die Business Technology Platform (SAP BTP) als bunte Zusammenstellung vieler nützlicher Funktionen. Laut Jost fehlt das verbindliche User-Interface und die konsistente Behandlung von Datenmodellen. Aber BTP wird nach Meinung der SAP-Community die bestimmende ERP-Strategie.

Composable ERP

Mit der Clean-Core-Strategie will SAP zu einem konsolidierten, Release-fähigen ERP-System gelangen, dessen Kern nur noch über APIs angesprochen werden kann. Modifikationen jeder Art sollen zukünftig auf der SAP Business Technology Platform stattfinden.

Die Möglichkeiten mit dem runderneuerten Abap und Cloud-Funktionen auf der Business Technology Platform sind gewaltig. Die ERP-Zukunft, auch jenseits von S/4HANA, wird durch BTP, CAP und RAP geprägt. Für SAP-Bestandskunden und Partner eröffnen sich Optionen für innovative End-to-End-Prozesse: Die Zukunft ist ein Composable ERP.

Die nächste ERP-Generation

Clean Core bedeutet „Frozen" Core und auch End-of-Life für ein ERP, wie es die SAP-Community bisher kannte. Mit Business Technology Platform entsteht ein neues ERP-Universum mit einer Best-of-Breed-Philosophie. Die Metamorphose begann 2020 und wurde mit dem Steampunk und BTP Summit 2024 in Heidelberg fortgesetzt. SAP BTP wird der Kern einer neuen ERP-Generation!

Einige Beobachter der SAP-Community bezeichnen BTP als ein weiteres ERP-System neben S/4. Dieses duale System, BTP und S/4, macht Sinn unter der Prämisse des S/4-Clean-Core. Ein wesentlicher Vorteil der SAP BTP gegenüber anderen IT-Plattformen ist die breite Verfügbarkeit: BTP gibt es als Service auch bei Microsoft Azure, Google Cloud Platform und Amazon Web Services.

SAP-Partner LeverX präsentierte auf der Konferenz LeverEdge 2024 Anfang Oktober in Miami, Florida, eine Zusammenarbeit mit AWS und ein Framework, das BTP ergänzt und Clean-Core-Konzepte ermöglicht. Damit scheint LeverX einer der ersten SAP-Partner zu sein, die strategisch die Themen Clean Core und BTP umsetzen werden. Aber BTP bedient in erster Linie die SAP-Silos on-prem und in der Cloud. Für den berühmten Blick über den Tellerrand brauchen die SAP-Bestandskunden andere und weitere IT-Plattformen, die offene sind und integrieren können. Boomi ist aktuell einer der führenden agnostischen IT-Anbietern im Markt und verfügt über die meisten Schnittstellen und Datenmodelle. Diesen Diskurs wird es in Heidelberg auf dem Steampunk und BTP Summit 2025 geben, ob nun BTP eine Meta-Plattform von Boomi braucht oder ob es eine Orchestrierung im Sinn einer Plattform-Economy geben kann.

https://e3mag.com/de/

STEAMPUNK UND BTP SUMMIT 2025

5. und 6. März 2025 in Heidelberg

Bild: AdobeStock

IT Service Management

DIE DIGITALE TRANSFORMATION BESCHLEUNIGEN

Veraltete ITSM-Lösungen mindern die Produktivität in Organisationen. Sie sind zu starr für die sich entwickelnden IT-Landschaften und Arbeitsweisen von heute, sie beruhen auf manuellen Prozessen und liefern einen geringen Geschäftswert. Service Management bietet hier die Chance, ITSM-Prozesse effektiver und die Nutzererfahrung intuitiv zu gestalten. Dadurch steigt nicht nur die Produktivität, sondern auch die Wettbewerbsfähigkeit.

Die europäische Wirtschaft setzt auf innovative Technologien, um die digitale Transformation voranzutreiben. Nie zuvor war der technologische Wandel so rasant wie derzeit – insbesondere durch Künstliche Intelligenz. Vor dem Hintergrund dieser Entwicklungen gewinnt die Wahl des richtigen Partners für IT Service Management zunehmend an Gewicht. Viele europäische Unternehmen ziehen es zunehmend vor, mit Anbietern zusammenzuarbeiten, die sowohl die hiesigen Regularien berücksichtigen als auch ihre Anforderungen kennen.

Sicherheit und Compliance im Blick

Matrix42 versteht, was Organisationen in Europa bewegt und welche Anforderungen sie erfüllen müssen. Dabei machen die modernen, skalierbaren und anpassungsfähigen Lösungen ITSM zum Business Booster. Vom sofort einsatzbereiten Ticketing bis hin zu einer vollständig integrierten IT-Management-Suite begleitet das Unternehmen Kunden dabei, verschiedene Phasen des Service Managements zu digitalisieren und zu automatisieren, um IT-Abteilungen zu entlasten.

Als europäisches Unternehmen kennen die Experten für Service Management die Sorgen von IT-Leitern in Europa genau. Sie wissen: Es geht nicht nur um „Bits und Bytes". Auch Gesetze, Datenschutz und kulturelle Feinheiten spielen eine Rolle. Ein Schlüsselelement der Firmenstrategie ist das Partnernetzwerk – 300 Partner in ganz Europa. So können sie auf lokale Anforderungen eingehen, und zwar von sprachlichen Besonderheiten über länderspezifische Vorschriften bis hin zur Datensicherheit. Das hilft in der komplexen Digitalwelt Europas.

Von Europäern für Europäer

Der Zusammenschluss von Matrix42 mit dem finnischen Unternehmen Efecte im April 2024 war ein entscheidender Schritt, um seine Marktposition und sein Know-how in Europa weiter auszubauen. Kunden profitieren durch die gebündelte Expertise beider Unternehmen. Der neue CEO Niilo Fredrikson hat große Pläne. Seine Vision ist klar: „Wir wollen Europas Top-Adresse für Service Management sein." Das heißt: Europäische Firmen sollen eine echte Wahl haben – jenseits der internationalen Anbieter. Die jahrelange Erfahrung zahlt sich aus, denn das Unternehmen kennt den europäischen Markt in- und auswendig.

Europäische Spitzenleistung für die Digitalisierung

Zusammenfassend lässt sich feststellen, dass das europäische Unternehmen hervorragend positioniert ist, um Firmen bei der Erneuerung ihrer ITSM-Prozesse zu unterstützen. Dazu gehören ein europaweites Partnernetz und ein geschulter Blick für Sicherheit und Regeln. So individualisiert Matrix42 die Lösungen für die Herausforderungen von morgen und gestaltet die Arbeit der Zukunft mit.

Wobei ein wichtiges Element im ITSM zunehmend Künstliche Intelligenz sein wird. Schon jetzt bereichert KI den Service Desk, entlastet IT-Teams und steigert die Effizienz. Mit dieser ganzheitlichen Herangehensweise ist das Unternehmen bereit, zum „European SaaS Champion" im Service Management aufzusteigen und Unternehmen in Europa dabei zu unterstützen, ihre Digitalisierungsziele mit Effizienz in Einklang zu bringen.

www.matrix42.com

KI im IT Service Management

HILFREICH. NOTWENDIG. FRAGWÜRDIG.

Künstliche Intelligenz (KI) hat sich zu einer wegweisenden Kraft im IT Service Management (ITSM) entwickelt. Denn sie verändert grundlegend, wie IT-Abteilungen funktionieren, zusammenarbeiten und Services bereitstellen.

Am deutlichsten erlebt man dies derzeit wohl anhand der Transformation des Support-Erlebnisses. So gehören KI-gestützte Chatbots und virtuelle Assistenten schon heute zu etablierten Funktionen im First Level Support: Sie geben unmittelbar Antworten auf häufig gestellte Fragen, führen Benutzer durch die Schritte zur selbständigen Fehlerbehebung und bieten proaktiv Lösungsvorschläge an. Hierfür nutzen sie nicht nur öffentlich verfügbare Informationen, sondern beziehen ebenso die unternehmenseigene Tickethistorie oder Knowledge Base mit ein.

Eine neue Art der Interaktion

Was dabei den Unterschied macht, ist die dialogbasierte Interaktion. Denn während der traditionelle Knowledge-Base-Eintrag oft unbeachtet in den Tiefen der Datenbank verstaubt, vermag es KI, eben dieses Wissen zielsicher an den Nutzer zu kommunizieren. Der Endanwender wird damit befähigt, unkompliziert auf benötigte Informationen zuzugreifen und Probleme im besten Fall selbstständig zu lösen.

Muss doch einmal ein klassisches Ticket erstellt werden, geschieht auch dies dialogbasiert, ohne Service-Portal oder unliebsames Ticket-Formular – bei REALTECH erreichen wir dies zum Beispiel durch eine direkte Integration in Microsoft Teams. Der intelligente Assistent reichert die Anfrage eigenständig mit relevanten Informationen an und erfragt bei Bedarf fehlende Details. Auf dieser Basis erfolgen wiederum die automatisierte Klassifizierung, Priorisierung sowie Weiterleitung der Anfrage an den bestmöglichen Ansprechpartner.

Es sind einfache Automatismen wie diese, die das Support-Erlebnis neu definieren. Sie befreien IT-Teams von repetitiven Routineaufgaben und ermöglichen ihnen, sich auf die Lösung komplexerer Probleme sowie anspruchsvolle strategische Aktivitäten zu konzentrieren. Und auch dabei kommen intelligente Systeme bereits zum Einsatz: Die virtuellen Assistenten unterstützen bei der Auswertung großer Datenmengen. Sie bringen Transparenz in heterogene IT-Landschaften und helfen, existierende Informationen (etwa aus einer Configuration Management Database (CMDB)) besser zugänglich zu machen. IT-Teams profitieren demzufolge von einer besseren Informationsbasis bei strategischen Entscheidungen und können Risiken, zum Beispiel beim Change Management, deutlich besser beurteilen.

Von reaktiv zu proaktiv

Doch so beeindruckend diese frühen Anwendungsfälle auch sein mögen, so stehen wir doch erst am Anfang: Es ist zu

erwarten, dass KI fortlaufend komplexere und anspruchsvollere Aufgaben übernehmen wird – nicht nur im Support, sondern auf allen Ebenen des IT Service Managements. Dies wird die Arbeitsweise sowohl von IT-Fachleuten als auch von Endanwendern grundsätzlich verändern.

Ein spannendes Szenario ist dabei der Wandel von einem reaktiven zu einem proaktiven IT Service Management. Denn mit ihren analytischen Fähigkeiten kann KI potenzielle Probleme frühzeitig erkennen und präventive Maßnahmen entwerfen, noch bevor Schwierigkeiten auftreten (Predictive Maintenance). Kurz- und mittelfristig sollten wir aber keinen flächendeckenden Einsatz von autonom agierenden, selbstheilenden Systemen erwarten. Allein aus Sicherheits- und Governance-Gründen wird nach wie vor menschliche Expertise bei der Verifizierung und Umsetzung dieser Maßnahmen nötig sein. Klar ist jedoch, dass sich der Wandel hin zu einem proaktiven IT Service Management sehr positiv auf die Leistungsfähigkeit und Verfügbarkeit der IT-Infrastruktur auswirken wird.

KI unterstützt dabei nicht nur bei Betrieb und Wartung, sondern leistet auch einen entscheidenden Beitrag zu IT-Governance und -Sicherheit. So ermöglichen Echtzeitanalysen und intelligentes Monitoring eine präzise Bedrohungserkennung und Schwachstellenanalyse. Risiken können dadurch effizienter und mit weniger manuellem Aufwand gemindert werden. Automatisierte Compliance-Prüfungen sowie schnellere Reaktionsmechanismen bei Störungen sorgen sowohl für verbesserten Schutz als auch für vereinfachte Verwaltung digitaler Vermögenswerte. Damit ändert sich die Rolle der IT-Fachleute: von reaktiven Problemlösern zu strategischen Partnern, die durch digitale Prozesse zunehmend zum Unternehmenserfolg beitragen.

Doch so wie KI die Arbeitsweise von IT-Teams verändert, steigen auch die Erwartungen der Mitarbeitenden an ein intelligentes, personalisiertes Service-Erlebnis. Anwender, die aus dem Privatleben mit der Effizienz von KI-gestützten persönlichen Assistenten und Anwendungen vertraut sind, erwarten ähnliche Funktionen und Annehmlichkeiten bei ihren Arbeitswerkzeugen. Daraus ergibt sich eine neue Herausforderung für IT-Leiter: Schatten-KI. Denn Mitarbeiter, die von langsamen IT-Prozessen oder eingeschränktem Zugang zu KI-Tools frustriert sind, greifen möglicherweise auf nicht genehmigte Lösungen zurück und schaffen dadurch neue Sicherheitsrisiken und Compliance-Probleme.

Zwischen Innovation und Verantwortung

Ob durch die sich verändernde Erwartungshaltung der Mitarbeitenden oder die steigenden Anforderungen an die Wettbewerbsfähigkeit, IT-Entscheider geraten zunehmend in Zugzwang, intelligente Systeme nutzbar zu machen. Deren Einführung stehen allerdings auch klare Bedenken gegenüber: Insbesondere Fragen zur Sicherheit, Compliance und regulatorischen Komplexität sind bedeutende Hürden, die Unternehmen bei der Einführung berücksichtigen müssen. Und so finden sich Unternehmen auf dem Weg zu einem KI-gestützten IT Service Management im Spannungsfeld zwischen Innovationsdruck und der verantwortungsvollen Implementierung.

Hinzu kommt, dass die bisweilen undurchsichtige Natur der KI-Entscheidungsfindung zu mangelnder Transparenz und verzerrten Ergebnissen (KI-Bias) führen kann. Somit ist ungewiss, inwieweit den Empfehlungen einer KI vertraut werden kann oder sollte. Eine menschliche Instanz zur Qualitätssicherung, klare Richtlinien und Verantwortlichkeiten sind daher immens wichtig, um diese Risiken wirksam zu mindern.

Es bleibt also die Frage: Werden Unternehmen in der Lage sein, die Vorteile und Versprechungen von KI im ITSM vollumfänglich zu nutzen? Unzweifelhaft bietet die Verwendung klare Wettbewerbsvorteile, die das Potenzial haben, ITSM-Prozesse zu transformieren und deren strategische Rolle zu festigen. Die bereits verfügbaren sowie künftig zu erwartenden Anwendungsfelder unterstreichen dies. Allerdings bleiben zahlreiche Fragestellungen, insbesondere bezüglich Sicherheit, Datenschutz und Rechenschaftspflicht, zu klären. Ungeachtet dieser Herausforderungen ist KI kein „Nice-to-have" mehr, sondern ein wesentliches Element, die Handlungsfähigkeit von IT-Abteilungen zu verbessern, die Verfügbarkeit von IT-Infrastrukturen zu gewährleisten und insgesamt überhaupt wettbewerbsfähig zu bleiben. Denn die Möglichkeiten der KI nicht nutzende Unternehmen laufen Gefahr, in puncto Effizienz, Agilität und Innovation ins Hintertreffen zu geraten.

Dr. Kürsad Gögen

KI IST KEIN „NICE-TO-HAVE" MEHR, SONDERN EIN WESENTLICHES ELEMENT, DIE HANDLUNGSFÄHIGKEIT VON IT-ABTEILUNGEN ZU VERBESSERN, DIE VERFÜGBARKEIT VON IT-INFRASTRUKTUREN ZU GEWÄHRLEISTEN UND WETTBEWERBSFÄHIG ZU BLEIBEN.

Dr. Kürsad Gögen,
Portfolio Manager, REALTECH AG,
www.realtech.com

Mit ITSM zur digitalen Exzellenz

STRUKTURIERTE PROZESSE ALS SCHLÜSSEL

Mit der zunehmenden Komplexität moderner IT-Infrastrukturen und den gestiegenen Anforderungen an die Betriebsstabilität, Agilität und Resilienz im Rahmen digitaler Transformationsprojekte sind strukturierte IT-Prozesse unverzichtbar geworden. Ein IT Service Management (ITSM) unterstützt Unternehmen dabei, die Qualität ihrer IT-Dienste kontinuierlich zu verbessern, Kosten zu senken und auf Veränderungen schneller reagieren zu können – sogar mit künstlicher Intelligenz (KI).

Mit der Einführung der Information Technology Infrastructure Library (ITIL) Ende der 80er Jahre begann auch der Siegeszug von ITSM als ganzheitlicher Ansatz, um IT-Dienstleistungen effizienter, nutzungsorientierter und kundenfreundlicher zu gestalten. Insbesondere in großen, regulierten und dienstleistungsorientierten Unternehmen entwickelte sich ITSM rasch zum Schlüsselfaktor, um die IT zu einem echten Wertschöpfungsfaktor zu entwickeln.

Im Kern steht ITSM für die Überführung der IT-Abteilung in eine servicezentrierte Organisationseinheit, die ihre Leistungen in direkter Abstimmung mit den Geschäftsprozessen des Unternehmens erbringt. IT-Dienste werden hier also als maßgeschneiderte Leistungen konzipiert, die anhand klarer Service-Level-Agreements (SLAs) definier- und messbar werden. Diese serviceorientierte Ausrichtung stellt sicher, dass die Bereitstellung von IT-Diensten nicht isoliert, sondern in Abhängigkeit zu den Unternehmenszielen und den Bedürfnissen von Endanwendern erfolgt.

Rasche Identifizierung von Störungen

Zu den wichtigsten Anwendungsfeldern eines ITSM gehört das Incident Management. Es zielt darauf ab, auftretende Störungen schnellstmöglich zu identifizieren, zu dokumentieren und zu beheben, um die Verfügbarkeit geschäftskritischer Systeme sicherzustellen. Eng verwoben mit dem Incident Management ist das Problem Management, das sich mit der strukturierten Ursachenanalyse wiederkehrender Störungen beschäftigt. Ziel ist es, durch systematische Root-Cause-Analysen wiederholte Ausfälle langfristig zu vermeiden und die allgemeine Stabilität der IT-Infrastruktur zu verbessern. Zusätzlich unterstützt ITSM das Change Management, das alle Änderungen innerhalb der IT-Landschaft streng kontrolliert und koordiniert. Im Bereich des Asset- und Konfigurationsmanagements ermöglicht ITSM darüber hinaus eine transparente Verwaltung der eingesetzten IT-Ressourcen. Ein Service-Level-Agreement stellt zudem sicher, dass IT-Dienste den vertraglich vereinbarten Standards hinsichtlich Verfügbarkeit, Leistung und Support entsprechen.

ITSM: Effizienzsteigerung und Compliance im Fokus

„Einer der größten Effekte von ITSM ist die Steigerung der betrieblichen Effizienz", so die Erfahrungen von Robert Schmid, Market Development Manager bei noris network. Durch standardisierte und klar definierte Prozesse seien IT-Abteilungen nicht nur in der Lage, schneller und präziser auf Anfragen und Störungen zu reagieren. Die stärkere Automatisierung und Minimierung von manuellen Eingriffen reduzieren nach den Worten Schmids auch das Risiko von Fehlern. Anders als in nicht-strukturierten, reaktiven Verwaltung von IT-Diensten ermögliche es die strukturierte Vorgehensweise nämlich, Probleme zielgerichtet auf ihre Ursachen zu erforschen und Erkenntnisse für die Zukunft daraus abzuleiten. Ein weiterer zentraler Vorteil von ITSM: die Kosteneffizienz. Die Standardisierung von Prozessen ermögliche eine systematische Analyse der Ressourcennutzung, wodurch redundante Aufgaben identifiziert und eliminiert werden könnten. „Dies führt vor allem in großen und komplexen IT-Umgebungen zu erheblichen Einsparpotenzialen", so der ITSM-Experte weiter.

Neben diesen operativen Vorteilen bietet ITSM allerdings auch im Bereich der Compliance und des Risikomanagements entscheidende Verbesserungen. Durch die standardisierten Prozesse und die kla-

ITSM-DEFINITION

Das IT Service Management (ITSM) stellt einen systematischen und prozessorientierten Ansatz zur Steuerung und Bereitstellung von IT-Dienstleistungen dar. Es orientiert sich an dem Ansatz, IT-Dienste nicht nur effizient, sondern auch unternehmens- und nutzerorientiert zu gestalten. Dabei umfasst ITSM eine Reihe von klar definierten Prozessen, Verfahren und Richtlinien, die eine konsistente und transparente Serviceerbringung gewährleisten. Anders als in rein technikorientierten IT-Management-Ansätzen, die sich auf die Verwaltung von Infrastrukturen wie Hardware, Netzwerke oder Software konzentrieren, setzt ITSM den Fokus auf die Erfüllung von Serviceanforderungen, die sich aus den strategischen und operativen Zielen des Unternehmens ableiten.

re Dokumentation der Serviceaktivitäten können Unternehmen sicherstellen, dass sie gesetzliche und regulatorische Vorgaben einhalten. Dies ist insbesondere in stark regulierten Branchen wie dem Finanz- oder Gesundheitswesen von zentraler Bedeutung. „Unternehmen in diesen Bereichen sind häufig verpflichtet, strenge Compliance-Vorgaben einzuhalten und detaillierte Nachweise über ihre IT-Prozesse zu erbringen. Hier bietet ITSM durch seine dokumentierten und standardisierten Methoden die notwendige Transparenz und Nachvollziehbarkeit, um regulatorischen Anforderungen gerecht zu werden", sagt Schmid.

ITSM per Dienstleistung

Dreh- und Angelpunkt für ein reibungsloses ITSM ist heute zunehmend auch der IT-Dienstleister – besonders dann, wenn Unternehmen die volle Konzentration auf ihr Kerngeschäft legen. Hier spielen vor allem Faktoren wie die Verfügbarkeit und Sicherheit ihre Trümpfe aus. Schmid: „Die Entwicklung und der Betrieb einer skalierbaren ITSM-Lösung ist in der Regel kosten- und personalintensiv. Es braucht modernste Technologien, höchste Sicherheitsmaßnahmen und Verfügbarkeit, gleichzeitig aber auch niedrigen Latenzen und die Rechtssicherheit durch deutsche Cloud-Dienste." noris network hat dafür mit ServiceNow seit 2023 eine cloudbasierte und eine On-Premises Plattform im Portfolio. „ServiceNow hat sich zu einer umfassenden Plattform für Enterprise Service Management (ESM) weiterentwickelt, die verschiedene Anwendungsfälle außerhalb der IT abdeckt, wie zum Beispiel das Personalwesen, das Kundenservice-Management und das Facility-Management. Es umfasst heute sogar KI-Funktionen, um beispielsweise bei der Störungsbeseitigung behilflich zu sein und so die Komplexität für Endanwender zu reduzieren."

Anders als die standardmäßig als SaaS-Lösung verfügbare Variante hat noris network mit der On-Premises-Lösung eine Option etabliert, bei der Daten und Informationen nicht auf externen Servern gehostet, bereitgestellt und verwaltet werden müssen. Stattdessen liegen die geschäftskritischen Assets für Geschäftsanforderungen wie IT- und HR Service Management, Kundenbetreuung, Sicherheit, Governance und Risikomanagement, Performance Analytics oder Reporting unter der vollständigen Kontrolle des Kunden, wie Schmid weiter ausführt. „Das ist vor allem dann relevant, wenn gesetzliche und aufsichtsrechtliche Anforderungen bestehen. Dafür bürgen bei noris network zahlreiche Zertifizierungen wie ISO 27001 auf Basis der IT-Grundschutzkataloge des BSI, PCI DSS 4.0, TÜViT Level 4, EN 50600 VK4/SK4 oder ISAE 3402."

www.noris.de

EINER DER GRÖSSTEN EFFEKTE VON ITSM IST DIE STEIGERUNG DER BETRIEBLICHEN EFFIZIENZ.

Robert Schmid, Senior Market Development Manager (Application), noris network AG, www.noris.de

Der Schlüssel zu mehr Agilität und Innovation

AUTOMATISIERUNG UND EFFIZIENZSTEIGERUNG DURCH LOW-CODE

In einer Zeit, in der sich die Marktbedingungen im rasanten Tempo wandeln und Unternehmen sich fortwährend neuen Herausforderungen stellen müssen, erweist sich die Fähigkeit, schnell und effizient auf Veränderungen zu reagieren, als entscheidender Wettbewerbsvorteil. Viele Organisationen haben erkannt, dass die klassischen Methoden der Softwareentwicklung den aktuellen Anforderungen nicht mehr gerecht werden. Die Lösung liegt in der Implementierung moderner Entwicklungsplattformen, welche nicht nur eine Beschleunigung der Entwicklungszeiträume ermöglichen, sondern auch die Automatisierung von Geschäftsprozessen fördern. Hierzu zählen insbesondere Plattformen auf Basis von Low-Code.

LOW-CODE BIETET UNTERNEHMEN EINE LEISTUNGSSTARKE LÖSUNG, UM DIE EFFIZIENZ IHRER INTERNEN ABLÄUFE ZU STEIGERN UND GESCHÄFTSPROZESSE ZU AUTOMATISIEREN.

Thomas Lorenz, Director Solutions Consulting for Central Europe, Appian, www.appian.com/de

Der Terminus „Low-Code" bezeichnet eine Entwicklungsumgebung, in welcher der Entwicklungsprozess durch den Einsatz von visuell orientierten Werkzeugen, wie beispielsweise Drag-and-Drop-Editoren, vereinfacht wird.

Ein Paradigmenwechsel in der Softwareentwicklung

Low-Code-Plattformen stellen ein neues Paradigma in der Softwareentwicklung dar. Sie ermöglichen sowohl IT-Experten als auch Geschäftsanwendern die Erstellung von Anwendungen und Automatisierungslösungen ohne die Notwendigkeit tiefgreifender Programmierkenntnisse. Im Gegensatz zur traditionellen Softwareentwicklung, die einen hohen Grad an technischem Wissen und Programmieraufwand erfordert, ermöglichen Low-Code-Werkzeuge die Nutzung visueller und intuitiver Tools zur schnelleren Erstellung von Anwendungen. Sie eröffnen Unternehmen damit die Möglichkeit, ihre Geschäftsprozesse zu automatisieren und dadurch die Effizienz ihrer internen Abläufe zu steigern. Dies erlaubt Unternehmen eine schnellere Reaktion auf Kundenanforderungen, eine schnellere Umsetzung von Innovationen sowie eine Schonung von Ressourcen.

Die visuelle Programmierung wird durch wiederverwendbare Module und Vorlagen unterstützt, sodass die Erstellung und Implementierung von Anwendungen beschleunigt wird. Low-Code zielt darauf ab, den Entwicklungsprozess zu standardisieren und zu vereinfachen. Dadurch werden Unternehmen flexibler und gleichzeitig verringert sich die Abhängigkeit von hochspezialisierten IT-Entwicklern.

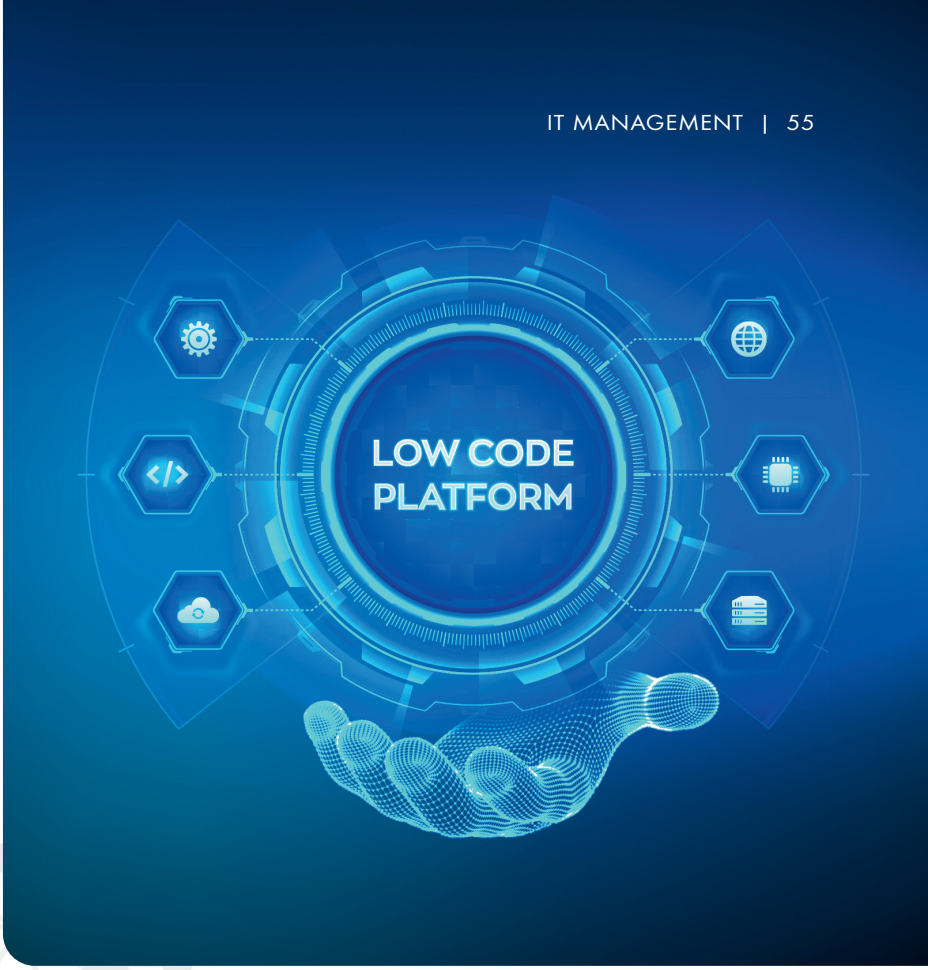
Plattformen wie die von Appian kombinieren die genannten visuellen Entwicklungstools mit leistungsstarken Integrations- und Automatisierungsmöglichkeiten. Infolgedessen können Unternehmen Prozesse automatisieren, die zuvor manuell oder durch fragmentierte Systeme abgewickelt wurden. Gleichzeitig wird durch den Einsatz von Low-Code-Technologien sichergestellt, dass die Anwendungen jederzeit mit geringem Aufwand anpassbar und skalierbar sind.

Wie Low-Code die Automatisierung beschleunigt

Eine der größten Herausforderungen, der Unternehmen heute gegenüberstehen, ist die Automatisierung ihrer internen Abläufe. Prozesse, die traditionell manuell abgewickelt wurden – wie etwa die Genehmigung von Anträgen, die Bearbeitung von Bestellungen oder die Verwaltung von Lieferketten – können durch Low-Code-Plattformen vollständig automatisiert werden.

Konkrete Anwendungsfälle, bei denen Low-Code einen wesentlichen Beitrag zur Automatisierung leisten kann, umfassen unter anderem die folgenden:

- **Genehmigungsprozesse:** In zahlreichen Organisationen sind Genehmigungsprozesse oftmals durch eine geringe Effizienz und eine lange Dauer gekennzeichnet. Dies ist darauf zurückzuführen, dass sie in der Praxis über mehrere Abteilungen hinweg manuell abgewickelt werden. Die Automatisierung der Prozesse kann mittels Low-Code-Lösungen realisiert werden, indem Regeln und Workflows definiert werden, die anschließend automatisch Aktionen auslö-



sen. Ein Beispiel für einen solchen automatisierten Workflow wäre die unmittelbare Weiterleitung von Dokumenten an die zuständige Abteilung nach deren Einreichung sowie die Versendung von Benachrichtigungen, sofern eine Genehmigung aussteht.

➤ **Bestell- und Lieferkettenmanagement:** Unternehmen, die mit globalen Lieferketten arbeiten, sehen sich mit der Herausforderung konfrontiert, ihre Bestellungen und Lieferungen effizient zu verwalten. Die Integration von Low-Code-Plattformen in bestehende ERP-Systeme ermöglicht eine nahtlose Zusammenarbeit. Die Automatisierung von Prozessen, die eine manuelle Bearbeitung überflüssig macht, stellt eine erhebliche Erleichterung dar. Dies betrifft zum Beispiel die automatische Bearbeitung von Bestellungen, die Aktualisierung von Lagerbeständen sowie die Verfolgung von Lieferungen.

➤ **Kundensupport und Serviceprozesse:** Ein weiterer wichtiger Bereich, in dem Low-Code zur Automatisierung beiträgt, ist der Kundenservice. Anfragen können durch intelligente Automatisierungslösungen schneller bearbeitet werden. Automatisierte Workflows können Anfragen direkt an den richtigen Ansprechpartner weiterleiten oder Chatbots einsetzen, um wiederkehrende Kundenfragen zu beantworten. Dies erhöht die Kundenzufriedenheit und entlastet gleichzeitig das Support-Team.

Effizienzsteigerung durch schnellere Entwicklungszeiten

Die Fähigkeit, Anwendungen und Automatisierungslösungen schneller zu entwickeln, ist ein entscheidender Faktor für Unternehmen, die wettbewerbsfähig bleiben wollen. Die traditionelle Entwicklung von Unternehmenssoftware erfordert oft Monate oder sogar Jahre, bis eine funktionsfähige Lösung implementiert werden kann. Dies führt zu hohen Kosten und einer langsamen Reaktionszeit auf Marktveränderungen.

Mit Low-Code können Unternehmen den Entwicklungsprozess drastisch beschleunigen. Anwendungen, die zuvor monatelange Entwicklungszyklen durchlaufen mussten, können nun in Wochen oder sogar Tagen erstellt werden. Diese verkürzten Entwicklungszeiten haben unmittelbare Auswirkungen auf den Return on Investment (ROI), da Unternehmen schneller von neuen Automatisierungslösungen profitieren können.

Ein weiterer Aspekt ist die Möglichkeit, Iterationen und Anpassungen schneller durchzuführen, denn in dynamischen Märkten müssen Anwendungen oft regelmäßig angepasst oder erweitert werden, um mit neuen Anforderungen Schritt zu halten.

Governance und Sicherheit

Trotz der vielen Vorteile von Low-Code gibt es auch einige Herausforderungen, insbesondere im Bereich IT-Governance und Sicherheit. Da Low-Code es Geschäftsanwendern ermöglicht, Anwendungen zu erstellen, besteht das Risiko, dass unkontrollierte Entwicklungen zu Problemen führen können, wenn sie nicht durch klare Governance-Strukturen reguliert werden.

Durch rollenbasierte Zugriffssteuerungen, zentrale Überwachungsfunktionen und integrierte Sicherheitsmaßnahmen können Unternehmen sicherstellen, dass ihre Low-Code-Entwicklungen sicher und konform sind.

Low-Code als Schlüssel zur Effizienzsteigerung

Low-Code bietet Unternehmen eine leistungsstarke Lösung, um die Effizienz ihrer internen Abläufe zu steigern und Geschäftsprozesse zu automatisieren. Plattformen wie die von Appian ermöglichen es, Anwendungen schneller zu entwickeln, Prozesse nahtlos zu integrieren und repetitive Aufgaben zu automatisieren – alles mit einem hohen Maß an Sicherheit und Governance.

Die Rolle von Low-Code bei der Automatisierung wird in den kommenden Jahren weiter zunehmen. Experten prognostizieren, dass Low-Code-Plattformen zu einem festen Bestandteil der IT-Landschaft werden, da sie es Unternehmen ermöglichen, schneller, effizienter und flexibler zu agieren.

Thomas Lorenz

Es ist nicht alles Gold, was glänzt

DIE DUNKLE SEITE DER FÜHRUNG UND WIE MAN IHR AM BESTEN BEGEGNET

Stärke, Verführung oder Gefahr? Oft werden Führungskräfte aufgrund von Charisma und Selbstbewusstsein ausgewählt – und scheitern später an Arroganz und Selbstüberschätzung. Erfahren Sie, wie Unternehmen Leadership Derailment frühzeitig erkennen und gezielt gegensteuern können.

Warum eine gute Führung unentbehrlich ist

In der dynamischen Geschäftswelt von heute stehen Unternehmen zunehmend vor der Herausforderung, die richtigen Führungskräfte zu identifizieren und zu entwickeln, denn schlechte Führung hat weitreichende negative Folgen. Nicht alle Führungskräfte, die auf den ersten Blick kompetent, selbstbewusst oder gar beeindruckend wirken, sind tatsächlich effektiv. Wenn einst vielversprechende Führungspersönlichkeiten in ihrer Rolle scheitern, oft aufgrund von Überheblichkeit, Egozentrik oder mangelnder Anpassungsfähigkeit, sehen wir die ursprünglichen Stärken plötzlich als überzogene Entgleisungstendenzen – oder „Leadership Derailment". Der wachsende Druck auf Führungskräfte, nicht nur Visionäre zu sein, sondern auch Ergebnisse zu erzielen und gleichzeitig die Balance zwischen starker Führung auf der einen Seite und Ermächtigung zur Verantwortungsübernahme auf der anderen Seite zu gestalten, macht die Identifikation und Auswahl der richtigen Talente zu einem komplexen Unterfangen.

UNTERNEHMEN STEHEN IN DER VERANTWORTUNG, WIRKLICH GEEIGNETE FÜHRUNGSKRÄFTE AUSZUWÄHLEN UND ZU ENTWICKELN.

Dr. René Kusch, Gründer, RELEVANT Managementberatung, www.relevant-mb.de

Studien zufolge fühlen sich bis zu 75 Prozent der Mitarbeitenden gestresst durch ihren Vorgesetzten, was zu einem höheren Burnoutrisiko und verminderter Arbeitszufriedenheit führt. Laut aktueller Gallup-Studien fühlen sich beinahe ein Fünftel der 20 Prozent der Arbeitnehmer nicht emotional an das Unternehmen gebunden, was die deutsche Wirtschaft jährlich über 130 Milliarden Euro an Produktivitätsverlusten kostet. Gleichzeitig zeigen „engagierte Teams" nicht nur weniger Fluktuation, sondern auch eine um bis zu 18 Prozent höhere Produktivität und 23 Prozent mehr Profitabilität.

Gute Führung hat also nicht nur einen positiven Einfluss auf das Wohlbefinden der Mitarbeitenden, sondern wirkt sich direkt auf den Geschäftserfolg aus. Doch woran erkennt man die richtige Führungskraft? Und warum fallen viele hochkarätige Kandidaten, die zunächst überzeugen, im Laufe der Zeit zurück? Diesen Fragen widmet sich die Untersuchung des Leadership Derailments.

Charisma: Ein zweischneidiges Schwert

Charisma gilt in der Geschäftswelt oft als eine herausragende Eigenschaft, die Führungskräfte von der Masse abhebt. Eigenschaften wie Selbstbewusstsein, Kreativität und Sozialkompetenz sind entscheidend, um Einfluss auszuüben, ein starkes Netzwerk aufzubauen und Menschen zu begeistern. Doch Charisma allein ist nicht genug – vielmehr kann es ein zweischneidiges Schwert sein. Was anfangs als positive Eigenschaft erscheint, kann sich schnell in negative Tendenzen wie Arroganz, Narzissmus und übermäßige Risikobereitschaft verwandeln.

Ein zentrales Konzept im Zusammenhang mit Charisma ist der sogenannte „Gradient of Delusion". Studien zeigen, dass die Einschätzung der eigenen Leistung bei Personen mit hohem Charisma nicht zu der Einschätzung der Leistung durch andere passt. Während sich Personen mit zunehmendem Charisma selber als zunehmend leistungsstark bewerten, ist das Gegenteil in der Fremdbewertung der Fall: Ab einem gewissen Level wird die Leistung mit weiter zunehmendem Charisma als geringer bewertet. Je cha-

rismatischer eine Führungskraft, desto größer wird das Risiko, dass sie den Kontakt zur Realität verliert. Diese Selbstüberschätzung kann nicht nur die persönliche Karriere, sondern auch die Leistung des gesamten Teams negativ beeinflussen. Es gilt, sich nicht zu sehr von Charisma blenden zu lassen.

Leadership Emergence vs. Leadership Effectiveness

Im Bereich der Führungsforschung unterscheidet man außerdem zwei zentrale Konzepte: Leadership Emergence und Leadership Effectiveness.

#1 Leadership Emergence beschreibt die Fähigkeit eines Individuums, als Führungskraft wahrgenommen zu werden. Faktoren wie Selbstbewusstsein, Extraversion und das weiter oben beschriebene Charisma spielen hier eine große Rolle. Menschen, die stark in diesen Bereichen sind, fallen auf, knüpfen Netzwerke und beeindrucken ihre Vorgesetzten – sie werden als Führungspersönlichkeiten gesehen, unabhängig davon, ob sie tatsächlich effektiv sind.

#2 Leadership Effectiveness hingegen bezieht sich auf die Fähigkeit, nachhaltig Ergebnisse zu erzielen. Effektive Führungskräfte bauen leistungsstarke Teams auf, setzen klare Ziele und unterstützen ihre Mitarbeitenden dabei, diese zu erreichen. Während Emergence oft eine Voraussetzung dafür ist, überhaupt in eine Führungsposition zu gelangen, bedeutet dies nicht automatisch, dass die Person auch tatsächlich effektiv in ihrer Rolle ist. Untersuchungen zeigen, dass viele Unternehmen die falschen Personen in Führungspositionen befördern, da sie sich zu sehr auf Emergence-Eigenschaften konzentrieren und Effectiveness vernachlässigen.

Dabei ist wichtig, dass keine der beiden Eigenschaften besser oder schlechter ist, als die andere. Eine Führungskraft mit starken Effectiveness-Fähigkeiten entfaltet ihr Potenzial wahrscheinlich nicht, wenn sie zu wenig Emergence-Verhalten zeigt und es nicht schafft, andere für sich zu gewinnen und positiv zu beeinflussen.

Fehler bei der Auswahl von Führungskräften

Die Auswahl von Führungskräften ist ein kritischer Prozess, bei dem oft Fehler gemacht werden. Ein häufiger Fehler ist die Überbewertung charismatischer Merkmale, die in Vorstellungsgesprächen und Assessment-Centern oft positiv hervorstechen. Diese „Emerging"-Verhaltensweisen führen jedoch oft dazu, dass Kandidaten ausgewählt werden, die später nicht so effektiv sind, wie es andere gewesen wären.

Zahllose Forschungsergebnisse zeigen, dass der Einsatz von fundierter Diagnostik dazu beitragen kann, solche Fehlgriffe zu vermeiden. Gerade die Persönlichkeitsdiagnostik liefert wertvolle und objektive Marker zur Beurteilung des Führungsvermögens, ohne die Entscheidungen zu oft auf der Grundlage von Oberflächlichkeiten getroffen zu haben. Gute Diagnostik ermöglicht es, die Personen zu identifizieren, die zwar wenig auf sich aufmerksam machen, aber gut für die Führungsposition geeignet sind. Ein angenehmer Nebeneffekt: Unternehmen vergrößern die Pools an Kandidaten für eine Führungsposition und müssen sich nicht aus Mangel an Kandidaten auf einen Kompromiss einlassen.

Wie Unternehmen bessere Führungskräfte identifizieren können

Zu einem guten Methodenbaukasten, der die Entscheidungsqualität im Recruiting bei Beförderungsentscheidungen erhöht, gehören unter anderem eine saubere Anforderungsanalyse, strukturierte Interviews, Simulationen und bestenfalls kognitive Leistungstests. Persönlichkeitsdiagnostik ist ein weiterer zentraler Baustein, um die Auswahl von Führungskräften zu optimieren. Während strukturierte Interviews und Assessment-Center wichtige Werkzeuge sind, reicht dies allein nicht aus, um die zukünftige Leistung einer Führungskraft zu prognostizieren. Wissenschaftlich fundierte Persönlichkeitsassessments, die darauf ausgelegt sind, beruflich relevantes Verhalten vorherzusagen, bieten eine tiefgehende Analyse und identifizieren nicht nur Stärken, sondern auch potenzielle Schwächen, die in Stresssituationen zu Leadership Derailment führen können.

GUTE DIAGNOSTIK MACHT ES MÖGLICH, DIE ECHTEN TALENTE UND RISIKEN EINER POTENZIELLEN FÜHRUNGSKRAFT ZU IDENTIFIZIEREN.

Niels Frommeyer, Senior Berater, RELEVANT Managementberatung, www.relevant-mb.de

Der Schlüssel liegt darin, objektive, verlässliche und inhaltlich relevante Tools zu nutzen und zu kombinieren, die eine umfassende Einschätzung ermöglichen. Dies reduziert nicht nur subjektive Verzerrungen, sondern erhöht auch die Wahrscheinlichkeit, die tatsächlich besten Kandidaten auszuwählen.

Warum Emergence nicht ausreicht

Nur etwa 10 Prozent der Führungskräfte vereinen in ihren zugrundeliegenden Persönlichkeitseigenschaften sowohl Leadership Emergence als auch Leadership Effectiveness. Dies zeigt, dass die bloße Auswahl von charismatischen und selbstbewussten Kandidaten nicht ausreicht, da diese mit großer Wahrscheinlichkeit nicht die Eigenschaften mitbringen, die es für Führungseffektivität braucht. Unabhängig von Emergence und Effectiveness Ausprägungen bedürfen alle Führungskräfte gezielter Entwicklungsprogramme, um sicherzustellen, dass sie auch langfristig effektiv und anpassungsfähig bleiben.

Ein Schlüsselkonzept in der Führungskräfteentwicklung ist die sogenannte Versatility – die Fähigkeit, sich unterschiedlichen Situationen anzupassen und ein breites Verhaltensspektrum abzudecken. Diese Vielseitigkeit wird zunehmend als entscheidender Faktor für den Führungserfolg anerkannt, besonders in einer Welt, die immer unvorhersehbarer wird. Mit dem Einsatz von 360°-Feedbacks und der Entwicklung strategischer Selbsterkenntnis können Unternehmen einen großen Beitrag leisten, dass ihre Führungskräfte nicht nur in guten Zeiten glänzen, sondern auch in Krisensituationen souverän agieren.

Objektivität als Auftrag an Unternehmen

Es sind nicht nur charismatische Eigenschaften, sondern vielmehr die oben als Leadership-Effectiveness beschriebene Fähigkeit, Teams zu inspirieren, klare Visionen zu formulieren, sich zu unterstützen und langfristig Ergebnisse zu erzielen. Um langfristig erfolgreiche Führungskräfte zu identifizieren und zu entwickeln, müssen Diagnostik und Entwicklung Hand in Hand gehen. Unternehmen, die sich weniger von charismatischen Oberflächlichkeiten blenden lassen und stattdessen auf wissenschaftlich fundierte Auswahl- und Entwicklungsprozesse setzen, entwickeln einen entscheidenden Wettbewerbsvorteil.

Dr. René Kusch, Niels Frommeyer

How to Select an Assessment

MEHR WERT

Führungserfolg

Spitzenzeiten im eCommerce meistern

DIE SCHLÜSSELROLLE VON ORDER MANAGEMENT SYSTEMEN FÜR DIE SKALIERBARKEIT VON ONLINESHOPS

Manche eCommerce-Unternehmen erleben zu saisonalen Spitzenzeiten, wie beispielsweise dem Weihnachtsgeschäft, der Black Friday-Week oder gestiegenen Verkaufszahlen in Folge von Marketingkampagnen unangenehme Zwischenfälle: Obwohl die Shop-Plattform in der Lage sein sollte, das Besucheraufkommen zu bewältigen, scheint sie mit dem Auftragsvolumen überfordert und es kommt technisch bedingt zu einer Vielzahl an Bestellabbrüchen, die schließlich für eine Zusatzbelastung bei der Kundenbetreuung sorgen. Für Shop-Betreiber ein ernüchterndes Ereignis, weist es doch darauf hin, dass sich ihr Shop-Modell nur begrenzt skalieren lässt. Die Verkaufszahlen bleiben weit hinter den Erwartungen zurück und das Erreichen unternehmerischer Wachstumsziele scheint in weiter Ferne.

Während Kunden im stationären Handel bei Rabattaktionen bei sichtbar großem Andrang verständnisvoll Wartezeit in Kauf nehmen mögen, haben sie online weniger Geduld. Durch die Benutzerzentrierung versprechen Onlineshops ihren Kunden standardmäßig bei jedem Einkauf stets das bestmögliche Einkaufserlebnis. Haben diese an irgendeinem Punkt ihres Onlinebesuchs das Gefühl, dass dieses Versprechen nicht gehalten wird, verlassen sie den Shop, womöglich sogar dauerhaft.

Die Bedeutung von Skalierbarkeit im eCommerce

Die Skalierbarkeit ihres Shop-Modells ist für eCommerce-Unternehmen eine Voraussetzung für weiteres Wachstum und das Erschließen neuer Märkte und Kunden. Skalierbare Unternehmen können wachsen, indem sie Leistung und Effizienz bei nahezu gleichbleibenden Betriebskosten steigern. Sie sind in der Lage, zusätzliche Kunden oder Aufträge zu bedienen, ohne proportional mehr Ressourcen – wie Personal oder IT-Infrastruktur – einzusetzen.

Um einer wachsenden Zahl an Kunden eine erfüllende Einkaufserfahrung bieten zu können, muss eine Vielzahl an Backend-Prozessen nahtlos ineinandergreifen. Doch in der Realität bleiben viele Onlineshops hinter ihren Erwartungen zurück, sobald sie ein deutlich höheres Besucheraufkommen verzeichnen. Bei der Suche nach den Ursachen treten in der Regel folgende Probleme auf:

#1 Zu große zeitliche Abstände bei der Aktualisierung von Bestandsdaten:

Zu Spitzenzeiten, wenn Bestellungen in schneller Folge eingehen, werden in Sekundenbruchteilen neue Bestandsabfragen generiert. Wenn Bestände nicht in Echtzeit aktualisiert werden, können Produkte als verfügbar angezeigt werden, obwohl sie bereits ausverkauft sind. Dies führt zu enttäuschten Kunden und erhöht den Verwaltungsaufwand durch Rückerstattungen und Stornierungen.

#2 Fehlende Datenintegration:

In der Regel nutzen E-Commerce-Unternehmen für Prozesse wie Bestellabwicklung, Lagerverwaltung und Kundenservice verschiedene Systeme. Wenn

Ein OMS ermöglicht Unternehmen, große Datenmengen zu verarbeiten und zu analysieren, wodurch wertvolle Einblicke in Verkaufs- und Bestelltrends gewonnen werden.

(Quelle: Fluent Commerce)

diese jedoch nicht nahtlos miteinander kommunizieren, entstehen Informationssilos. Dies führt zu ineffizienten Prozessen, da Daten manuell übertragen werden müssen, was das Fehlerpotenzial erhöht und die Geschwindigkeit der Bestellabwicklung verlangsamt.

Diese Faktoren verweisen auf das zugrunde liegenden Problem, das einigen Shops bei hoher Auslastung zum Verhängnis wird: Der mangelnden, unmittelbaren Verfügbarkeit relevanter Informationen und in dessen Folge lückenhafte Prozesse. Dieser Umstand verhindert hohe Performanz und damit die Skalierbarkeit des Shop-Modells.

Der Beitrag von Order Management Systemen

Für die Leistungsfähigkeit von Onlineshops war lange Zeit entscheidend, ob sie ein gewisses Auftragsvolumen bewältigen können. Dieser Indikator entstand im Zusammenhang mit On-Premises-Software und genügt gegenwärtig nicht mehr, um die Performanz von Onlineshops während Spitzenzeiten sicherzustellen. Mittlerweile sind IT-Umgebungen komplexer geworden. So stehen hinter jeder „Transaktion", wie zum Beispiel einer Bestellung, Dutzende oder Hunderte von Datenaufrufen und Ereignissen, die im Hintergrund ablaufen. Einige stehen in direktem Zusammenhang mit der Transaktion, andere unterstützen sie lediglich. Erfolgt zeitgleich eine hohe Zahl an Transaktionen, kann es zu einem massiven Rückstau kommen, wenn Prozesse zum benötigten Zeitpunkt lediglich unvollständige oder fehlerhafte Daten erhalten.

Um dieses Problem zu eliminieren, können als Ergänzung zu bestehenden Onlineshop-Plattformen moderne Order Management Systeme (OMS) eingesetzt werden. Bei einem modernen OMS handelt es sich um eine so genannte Headless-Lösung, die auf einer API-first-Technologie beruht. Sie ist in der Lage, alle mit dem Sourcing und Fulfillment verbundenen Prozesse zu orchestrieren und die relevanten Informationen an das Shop-Frontend zu übermitteln. Dies bietet verschiedene Vorteile:

- Flexibilität: Mit skalierbarem Coding, das durch einen modularen Aufbau äußerst anpassungsfähig ist, bietet ein OMS hohe Flexibilität. Mit dieser Art von Programmierung können Entwickler kurzfristig neue Funktionen und Integrationen hinzufügen, ohne die gesamte Infrastruktur überarbeiten zu müssen.

- Echtzeit-Sichtbarkeit: Die bedeutendste Fähigkeit eines OMS ist die Echtzeit-Sichtbarkeit von Beständen und Bestellungen. Durch die kontinuierliche Aktualisierung von Bestandsdaten können Unternehmen sicherstellen, dass ihre Kunden stets korrekte Informationen erhalten. Dies minimiert das Risiko von Überverkäufen und hilft, die Kundenzufriedenheit zu verbessern.

- Integration mit anderen Systemen: Ein OMS lässt sich nahtlos in bestehende ERP-, CRM-, oder Lagerverwaltungssysteme integrieren. Diese Interoperabilität fördert einen reibungslosen Informationsfluss und vereinfacht die Datenanalyse erheblich.

- Effizienzsteigerung: Mit einem OMS lassen sich Prozesse, die bislang manuell durchgeführt werden mussten, automatisieren. Dies beseitigt Fehlerquellen und schafft flüssige Abläufe, was nicht nur die Kosten senkt, sondern sich auch positiv auf die Kundenzufriedenheit auswirkt.

- Kosteneffizienz: Ein skalierbares OMS bietet in der Regel eine kosteneffiziente Alternative zu anderen Lösungen, da es die Prozesskosten signifikant reduziert und die Notwendigkeit verringert, in neue Systeme zu investieren oder bestehende manuell anzupassen.

- Bessere Entscheidungsfindung: Da ein OMS große Datenmengen verarbeiten und analysieren kann, eröffnen sich Unternehmen wertvolle Einblicke in Verkaufs- und Bestelltrends. Dies unterstützt fundierte Entscheidungen und strategische Planungen – auch im Demand Planning-Bereich.

Skalierbarkeit durch verbessertes Informationsmanagement

Order Management Systeme sorgen für einen nahtlosen, zuverlässigen Informationsfluss zwischen allen für das Sourcing und Fulfillment relevanten Prozessen. Ihre Fähigkeit zur Aktualisierung von Bestandsdaten in Echtzeit erlaubt es Onlineshops, auch in Spitzenzeiten ihren Kunden die versprochene Servicequalität zu bieten und den Abverkauf von Waren nach ihren individuellen Vorgaben steuern. Indem sie E-Commerce-Unternehmen helfen, bislang ungenutzte Ressourcen freizusetzen, unterstützen Order Management Systeme die Skalierbarkeit von Onlineshops. Damit sind sie in der Lage, agiler auf neue Marktanforderungen zu reagieren und Geschäftsziele zu erreichen.

Frank Logen

EINE ECHTZEIT-VERFÜGBARKEIT ALLER BESTANDSDATEN IST VORAUSSETZUNG FÜR ERFOLGREICHE ONLINESHOPS.

Frank Logen, Senior Account Executive EMEA, Fluent Commerce, www.fluentcommerce.com

Bereits beim Projektstart gescheitert

12 THESEN ZUR FRÜHZEITIGEN SCHIEFLAGE VON PROJEKTEN

Wird ein Fußballspiel bereits mit einem Stand von 0:5 angepfiffen ist für jeden klar, dass ein erfolgreiches Spiel eine geringe Wahrscheinlichkeit hat. Gleiches gilt, wenn eine Mannschaft in der Anfangsphase eines Fußballspiels mit 5 Toren zurückliegt. Leider ist diese Transparenz bei Projekten nicht immer und jedem gegeben. Dennoch sind solche Handicaps nicht selten der Fall.

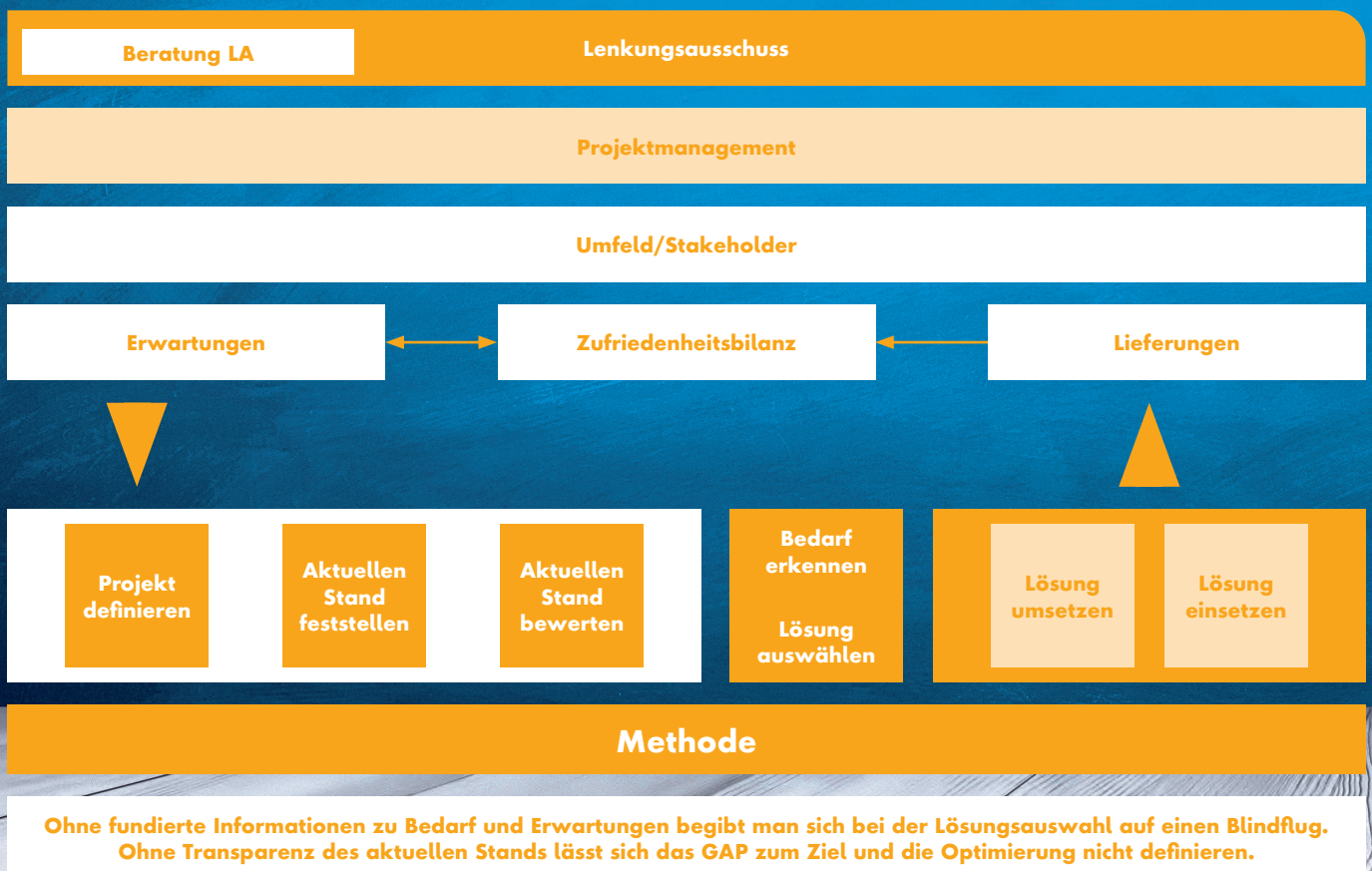
Bevor tiefe Analysen bemüht werden, gibt es bereits Begründungen in einfachen und offensichtlichen Punkten. Diese Gründe finden sich in strategischen Grundlagen und dem operativem Projektstart.

Ähnlich wie beim Fußball gibt es bei Projekten keine allgemein gültige Standardlösung. Beim Fußball würden sonst einfach alle wie der Weltmeister spielen. Warum dies nicht für alle Mannschaften funktioniert, liegt auf der Hand und ist sehr transparent. Einfach dargestellt sind dies unterschiedliche Ressourcen, Stakeholder und Ziele. Bei Projekten ist dies ähnlich, sonst könnte man ein beliebiges erfolgreiches Projekt kopieren und der Erfolg wäre garantiert.

Beachtet man folgende 12 Thesen mit der notwendigen Sorgfalt lassen sich nicht alle, aber viele Probleme reduzieren.

#1 Wenn man sieht, wie Projekte anfangen, weiß man wie sie verlaufen und welche Erfolgschancen sie haben

Fängt ein Projekt ohne ausreichende Unterstützung und professionelle Planung an, stellt sich die Frage, warum dies im Verlauf besser werden sollte. Ist die Organisationsstruktur falsch durchdacht und besetzt, eine professionelle Zieldefinition fehlt und die Auswirkungen der Veränderungen sind nicht betrachtet, wie soll sich dann ein erfolgreicher Ablauf ergeben? Fehlt eine realistische Einschätzung zu Umfang und notwendigen Ressourcen und auch eine Methodik ist nicht



Ohne fundierte Informationen zu Bedarf und Erwartungen begibt man sich bei der Lösungsauswahl auf einen Blindflug. Ohne Transparenz des aktuellen Stands lässt sich das GAP zum Ziel und die Optimierung nicht definieren.

erkennbar, wie soll ein erfolgreiches Projektergebnis entstehen?

#2 Die Projektkultur und das Ansehen des Projektmanagements innerhalb eines Unternehmens geben eine vorentscheidende Richtung

Werden Projekte nur als notwendiges Übel gesehen und professionelles Projektmanagement vernachlässigt, ist die Grundlage für Misserfolge bereits nachhaltig gegeben bevor neue Projekte überhaupt angedacht sind. Diese als ungewollte „Stiefkinder" zu behandeln, wirkt auf die Entstehung und damit bereits auf das Ergebnis der Projekte und die Rendite von eingesetzten Ressourcen.

#3 Die falsche Projektmethode kann zum Scheitern des Projektes führen

Eine generelle Standardmethode für alle Projekte vorweg festzulegen, ist falsch. Es gibt keine „one fits all" Projektmethodik, die für jedes Projekt passt. Ziele, Projektinhalte, Projektverantwortliche, Projektteilnehmer, Nutzer des Ergebnisses und Projektpartner sind unterschiedlich. Die Veränderung einer dieser Punkte kann die Auswahl der richtigen Methode beeinflussen. Ein Klassiker im Methodendilemma ist der Spagat, wenn ein agiles Vorgehen in der Produktherstellung angewendet wird und das Management ein Reporting angelehnt an eine klassische Vorgehensweise erwartet, um Entscheidungen zu treffen.

#4 Eine falsche Definition der Projektleiterrolle senkt die Effizienz und Effektivität des Projektes signifikant

Wenn ein Projektleiter in der Praxis eher eine Assistentenrolle ausführt, weil seine Kompetenz beschnitten wird, kann er kein Projekt leiten, sondern nur weisungsgebunden verwalten. Das schwächt die Position nicht nur intern, sondern auch bei externen Partnern. Weiterhin ergibt sich das Risiko der ungewollten Einflussnahme von hierarchisch höher angesiedelten Stakeholdern auf das Projekt. Ein Projektleiter sollte in der Hauptsache dem Projekt verpflichtet sein. Das ist durch interne Linienabhängigkeit nicht unbedingt gegeben. Die Besetzung der Position sollte sich nicht auf die „billigste" Variante fokussieren, da an dieser Stelle entscheidende Beiträge zur Effizienz und Effektivität geleistet werden.

#5 Eine mangelnde Übersicht über das Projektportfolio erhöht das Risiko aller Projekte

Zu viel oder zu wenig Projekte und damit Ressourcenkonkurrenz oder Ineffizienz belasten Projekte und reduzieren Entwicklungspotenziale für Unternehmen. Fehlende Transparenz über Beiträge einzelner Initiativen zu Gesamtzielen belastet die Performance des Gesamtportfolios und einzelner Projekte. Die Möglichkeiten zur Entscheidung über die sachgerechte Zuteilung von Ressourcen und Aufmerksamkeit werden reduziert.

#6 Mangelnde Beratung für Lenkungskreise führt zu signifikanten Fehlentscheidungen

Basierend auf zeitlichen Einschränkungen und ausreichender Tiefe in den jeweiligen Themen ist es klar, dass kompetente Unterstützung den Mitgliedern eine gute Entscheidungshilfe bietet. Wenn fehlende Zeit und/oder fehlendes Spezialwissen in Lenkungskreisen nicht seriös ausgeglichen und delegiert werden, kommt es zu verzögerten oder falschen Entscheidungen. Alibiberater mit reduziertem Fachwissen und mangelnder Erfahrung im Projektmanagement, dafür vielleicht gutem Standing, werden Lenkungskreisen und Projekten nicht helfen. Aus einem Berater wird auf Basis von Überschriftenwissen im Projektmanagement keine ausreichende Hilfe eines Lenkungskreises oder eines Managers.

#7 Eine fehlende Umfeldanalyse gefährdet nicht nur das eigene Projekt

Was wirkt auf das Projekt ein und welche Schnittstellen gibt es zu anderen Projekten oder Organisationen? Gerade bei Arbeitsteilung in einem Gesamtkontext kann mangelnde Information zu Schwierigkeiten fachlicher und menschlicher Art führen.

Wer liefert und wer empfängt welches Element zu welcher Zeit, speziell in abhängigen Projekten oder Programmen? Je nach Projekt kann dies sehr komplex werden. Missverständnisse oder fehlende Informationen wirken sich im Verlauf des Projektes aus.

Das Projektumfeld ist eine wichtige Grundlage der Projektplanung, weil es nicht nur wichtige Einflüsse auf das eigene Projekt offenlegt, sondern auch Aufschluss zu übergreifenden Themen bringt. Von großer Bedeutung ist hier auch die Identifizierung aller relevanten Stakeholder, die nicht immer umfänglich transparent sind. Ohne diese Informationen begibt man sich auf einen Blindflug.

#8 Die Lösungsauswahl vor der Anforderungsanalyse bringt nur zufallsbedingte Erfolge

Etwas auszuwählen, ohne genau zu wissen, was real gebraucht wird und dies am besten abdeckt, ist objektiv gesehen nicht nur schwer, sondern Glückssache. Keine Zeit in eine grundlegende Analyse zu stecken, mag auf den ersten Blick eine Abkürzung sein. Das Risiko, dass diese vermeintliche Abkürzung in eine falsche Richtung und damit zu einem Umweg oder gar einer Sackgasse führt, ist nicht gering. Beispiel wäre die Auswahl einer neuen Softwarelösung, die auf Basis eines populären Namens oder einer guten Vertriebsarbeit ausgewählt wird, aber für die individuellen Anforderungen suboptimal bis hoch ineffizient oder ganz ungeeignet ist.

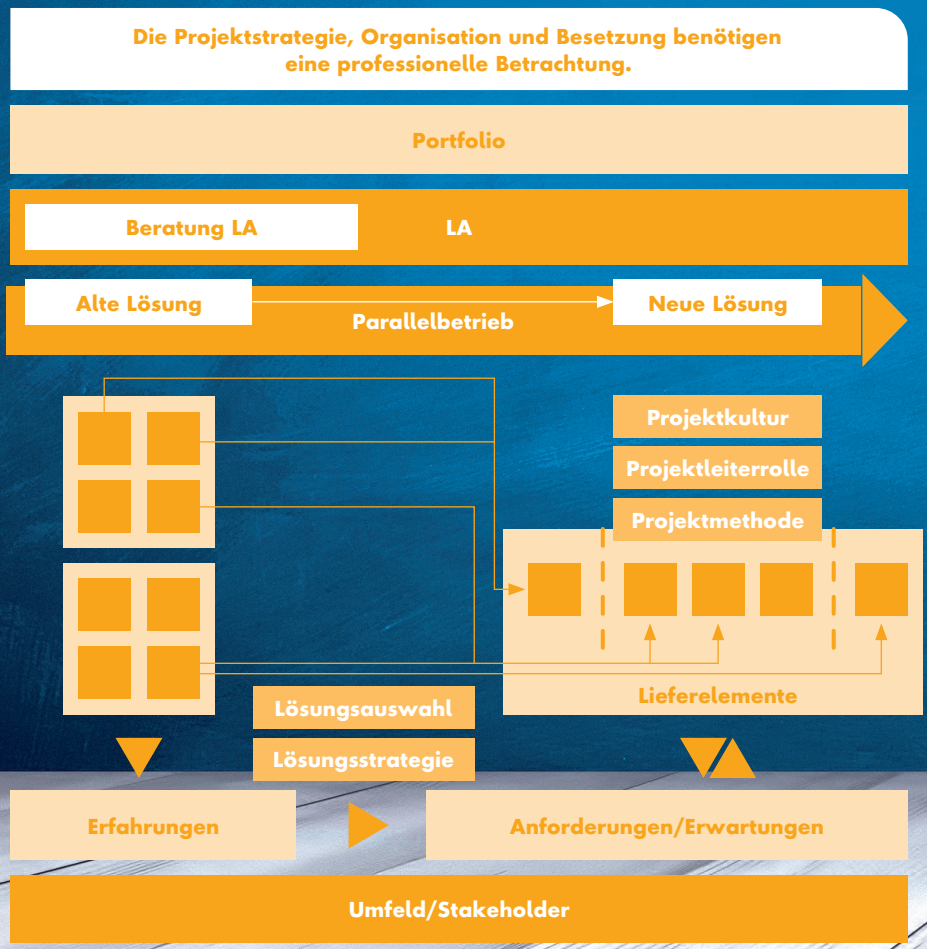
#9 Eine neue Softwareapplikation allein ist nicht die Lösung, sondern zunächst ein Problem

Bevor der erste Nutzen entsteht, stehen Aufwand für Beschaffung, Einführung und Parallelbetrieb der abzulösenden Variante im Blickfeld der Betrachtung.

Ohne Abbildung der notwendigen Prozesse nützt eine neue Software nichts. CRM-Software allein ist kein Customer Releationship Management, ein neues ERP-System unterstützt keine kaufmännischen Prozesse, die es noch nicht kennt und gleiches gilt für diverse andere Systeme, ob ITSM, E-Commerce oder ähnliche Werkzeuge. Die Erwartungen und die Ungeduld der Stakeholder steigen, bis ein vertretbares Ergebnis zu präsentieren ist. Spätestens mit der Erkenntnis, dass die reine Standardsoftware keine Lösung ist und die notwendigen Ressourcen zur Einführung größer sind als geplant, steigt auch das Problempotenzial.

#10 „Am Standard der Software bleiben" ist ein Vorsatz, der schwer einzuhalten ist

Die Vorteile dieses Vorsatzes liegen auf der Hand. Der Vorsatz ist aber nur dann nicht oberflächlich, wenn im Vorfeld der Auswahlentscheidungen die Anforderungen detailliert bekannt und mit den Möglichkeiten der Standardsoftware abgeglichen sind. Hinzu kommt die Sicherheit, die daraus resultierenden organisatorischen Änderungen anwenderfreundlich durchsetzen zu können. Diese notwendige Entscheidung unter-



streicht nochmal die Bedeutung, im Vorwege Bedarf und Angebot verglichen zu haben.

#11 Ein Ausblenden der Erwartungen von Stakeholdern verlangsamt das Projekt

Sind die entscheidenden Stakeholder nicht ausreichend in das Projekt eingebunden, gibt es Widerstände. Die Definition, wer entscheidend ist und wer nicht, ist wesentlich für den Projektverlauf und Erfolg. Schon die fehlende Wertschätzung durch mangelnde Beteiligung bringt zusätzlich zu den weiterhin bestehenden Anforderungen des vernachlässigten Personenkreises schlechte Stimmung und Abwehrhaltung. Dies beginnt vor dem Projekt, zieht sich über den Projektverlauf und gefährdet den Projektnutzen. Ein Beispiel ist konsequentes Boykottieren des Projektoutputs wie das Umgehen von neuen Prozessen. Die vermeintliche Zeitersparnis multipliziert sich durch notwendige Nachbesserungen.

#12 Es gibt keine zweite Chance auf den ersten Eindruck bei der Einführung von neuen Lösungen

Ist die erste Sicht auf eine neue Lösung negativ, bedeutet dies für das Projekt deutlich erhöhten Aufwand, um diesen Nachteil aufzuholen und trotzdem das gewünschte Ergebnis zu erzielen.

Meist gibt es schon eine bestehende Lösungsvariante, die aus verschiedenen Gründen abgelöst wird. Auch mit einer solchen gewachsenen Lösung findet ein Vergleich der Stakeholder statt. Damit steht das Projekt vor der Herausforderung, den richtigen Zeitpunkt für eine erste Ergebnispräsentation zu finden. Dabei kann es sehr nachteilig sein, ein erstes – noch zu schlechtes - Produkt durch einen gut gemeinten iterativen Vorsatz zu früh zu präsentieren. Das komplette Gegenteil, zu lange zu warten und erst nach zu langer Zeit an die Oberfläche zu kommen, ist auch problematisch. In dieser Zeit verändern sich Anforderungen und das angestrebte Ergebnis ist überholt und viele Ressourcen verschwendet. Dies sollte in der Projektstrategie am Anfang beachtet werden.

ALLE THESEN FÜR SICH HABEN INHALTLICH DAS POTENZIAL, PROJEKTE IN SIGNIFIKANTE SCHWIERIGKEITEN ZU BRINGEN.

Martin Besemann,
Berater und zertifizierter Projektmanager,
www.conpromas.de

Ergebnisoffene Analyse und Restrukturierung

Läuft ein Projekt nicht wie gewünscht, ist dies nicht vorteilhaft, aber die Erkenntnis ist ein erster Schritt. Veränderungen im Projektablauf kosten Ressourcen, vor allem zunächst einmal Zeit. Es ist nur eine sehr kurzfristige Sicht, eine notwendige Veränderung mit diesem Argument abzuwehren. Weiter in die falsche Richtung oder Umwege zu laufen, um ein Projekt wie bisher am Laufen zu halten, ist keine nachhaltige Lösung. Ausgegebene Budgets gehören der Vergangenheit an. Zukünftig Ressourcen zu investieren, macht nur Sinn, wenn daraus eine Rendite entsteht. Daher ist eine offene Analyse sinnvoll, ob gutes (neues) Geld schlechtem (bereits ausgegebenen) Geld hinterherzuwerfen ist, statt eine konsequente Entscheidung wie Sanierung oder Abbruch zu treffen.

Fazit

Ein gut gestartetes Projekt ist keine Garantie für einen erfolgreichen Verlauf und ein gutes Ergebnis. Es gilt, die anfängliche Professionalität durchgängig zu liefern. Das Zutrauen, dass sich ein solches Vorgehen fortsetzt, ist aber eher gegeben als in ein Projekt, welches schon schlecht gestartet ist. Wobei letzteres schon das Problem hat, gleich mit einem negativen Image versehen zu sein und zunächst dagegen anzukämpfen hat.

Es ist nicht ungewöhnlich, aber teilweise intransparent und unterschätzt, dass ein Projekt unter einem Methodenproblem oder problematischen strategischen Grundlagen statt technischen Problemen leidet. Letztere ergeben sich teilweise daraus.

Die Zeit, die nicht zu Beginn in die methodische Definition des Projektmanagements investiert wird, vervielfacht sich im Projektverlauf.

Alle Thesen für sich haben inhaltlich das Potenzial, Projekte in signifikante Schwierigkeiten zu bringen. Es gibt für sie keine allgemeingültigen Lösungen. Natürlich umfassen sie auch nicht jedes individuelle Risiko vor oder während des Starts. Die Thesen geben den Anreiz, diese mit den eigenen Projekten zu vergleichen und eine individuell passende Lösung zu finden. Keine Zeit für Veränderungen zu haben, ist oft eine Fehleinschätzung. Weiter die falsche Richtung zu beschreiten und dafür unnötige Ressourcen zu verschwenden, ist keine Lösung. Es bietet sich an, hier auch neutrale Betrachter hinzuzuziehen. Das bringt den Vorteil, dass eine unvoreingenommene Analyse gefördert wird.

Martin Besemann

it management

AUSGABE 01-02/2025
ERSCHEINT
AM 27. JANUAR 2025

UNSERE THEMEN

Fokusthema: Office 4.0
Schwerpunktthemen unter anderem: AI/KI, ITSM, Cloud Computing, Unified Communications

it security

AUSGABE 01-02/2025
ERSCHEINT
AM 27. JANUAR 2025

UNSERE THEMEN

Die Cybersecurity-Landschaft wandelt sich permanent – und wir wandeln uns mit. Statt starrer Themenplanung folgen wir dem Puls der Security-Welt und bleiben so immer aktuell.

INSERENTENVERZEICHNIS

IMPRESSUM

Herausgeber: Ulrich Parthier (08104-6494-14)

Geschäftsführer: Ulrich Parthier, Vasiliki Miridakis

Chefredaktion: Silvia Parthier (-26)

Redaktion: Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke: Eva Neff (-15)

Autoren: Lars Becker, Martin Besemann, Philipp von der Brüggen, David Cohen, Vincent Effertz, Lennard Everwien, Niels Frommeyer, Felix Glowatzka, Dr. Kürsad Gögen, Peter van Harten, Volker Hettich, Yannik Jodehl, Raphael Kelbert, Bastian Kempe, Dr. René Kusch, Martin Landis, Frank Logen, Thomas Lorenz, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Simone Schiffgens, Robert Schmid, Dominic Scholl, Dr. Kai A. Simon, Nikolas Strommenger, Dr. Sylvia Trage

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH
Ludwig-Ganghofer-Str. 51, D-83624 Otterfing
Tel: 08104-6494-0, Fax: 08104-6494-22
E-Mail für Leserbriefe: info@it-verlag.de
Homepage: www.it-daily.net

Alle Autoren erreichen Sie über die Redaktion.Wir reichen Ihre Anfragen gerne an die Autoren weiter.

Manuskripteinsendungen: Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programmteilen führen, übernimmt der Verlag keine Haftung. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

Layout und Umsetzung: K.design | www.kalischdesign.de
mit Unterstützung durch www.schoengraphic.de

Illustrationen und Fotos:
Wenn nicht anders angegeben: shutterstock.com

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 31.
Preisliste gültig ab 1. Oktober 2023.

Mediaberatung & Content Marketing-Lösungen
it management | it security | it daily.net:
Kerstin Fraenzke, 08104-6494-19, fraenzke@it-verlag.de
Karen Reetz-Resch, Home Office: 08121-9775-94, reetz@it-verlag.de
Marion Mann, +49 152-3634 1255, mann@it-verlag.de

Online Campaign Manager:
Roxana Grabenhofer, 08104-6494-21, grabenhofer@it-verlag.de
Head of Marketing:
Vicky Miridakis, 08104-6494-15, miridakis@it-verlag.de

Objektleitung: Ulrich Parthier (-14), ISSN-Nummer: 0945-9650

Erscheinungsweise: 6 x pro Jahr

Verkaufspreis: Einzelheft 20 Euro
Jahresabopreis 100 Euro (Inland), 110 Euro (Ausland)
Probeabo 20 Euro für 2 Ausgaben, PDF-Abo 40 Euro für 6 Ausgaben

Bankverbindung: VRB München Land eG,
IBAN: DE90 7016 6486 0002 5237 52, BIC: GENODEF10HC
Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Abonnementservice: Eva Neff,
Telefon: 08104-6494-15, E-Mail: neff@it-verlag.de
Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Beträge.


Steampunk
und BTP Summit 2025
5. und 6.
März 2025
Heidelberg
SAP Business Technology Platform, BTP,
wird nach Meinung der SAP-Community
die bestimmende ERP-Strategie.
Der Summit 2025 präsentiert Abap, CAP,
RAP und Steampunk sowie SAP BTP als
Basisplattform und S/4-Hana-Nachfolger.
e3mag.com/de/steampunk-summit
Eine Veranstaltung des E3-Magazins:
e3mag.com

Excellence in
Digital Security.

genua.

Wir misstrauen ALLEM.
Aus Berufung.

Zero Trust ist für uns nicht nur ein Paradigma, sondern das genua Mindset.

Wir investieren all unsere Skepsis zugunsten Ihrer Sicherheit.
Wir forschen, entwickeln, testen und hinterfragen alles zu jeder Zeit.
Jeden Tag aufs Neue.

Steffen Ullrich & Sebastian Rassel
Zero-Trust-Evangelisten

Ihr Weg zu Zero Trust.

genua.de

Teil der Bundesdruckerei-Gruppe

bdr.

genua ist made in Germany – für Ihre digitale Souveränität.

it security

Detect. Protect. Respond.
November/Dezember 2024

WIDERSTANDSFÄHIGE LIEFERKETTE

Risk Assessments als Schlüssel

Sudhir Ethiraj, TÜV SÜD GmbH

KÜNSTLICHE INTELLIGENZ

Chance für die Cybersicherheit?

EINFÜHRUNG IN DATA FABRICS

Kontinuierliches Monitoring

CYBERSECURITY AWARENESS

Mit Sensibilisierung zu mehr Sicherheit

Cyberkriminelle überall

da tut Hilfe not

Mehr Infos dazu im Printmagazin

itsecurity

und online auf **www.it-daily.net**

Inhalt

COVERSTORY

IT SECURITY

Widerstandsfähige Lieferkette

RISK ASSESSMENTS ALS SCHLÜSSEL FÜR RESILIENZ UND NIS2 COMPLIANCE

NIS2 kommt – und damit werden auch Risikomanagementmaßnahmen für die Lieferkette als eine der zentralen Maßnahmen für mehr Cyberresilienz gesetzlich vorgeschrieben. Unmittelbar von NIS2 betroffene KRITIS-Unternehmen sollten sich daher spätestens jetzt damit auseinandersetzen. Mithilfe von Risk Assessments können Unternehmen Schwachstellen in ihrer Lieferkette identifizieren, beheben und im Falle eines erfolgreichen Angriffs den Schaden begrenzen. Aber auch von NIS2 nur mittelbar betroffenen Zulieferer und Partner sollten sich gut vorbereiten.

it-security hat dazu mit Sudhir Ethiraj, Global Head of Cybersecurity Office (CSO) & CEO Business Unit Cybersecurity Services bei TÜV SÜD, gesprochen.

it security: *NIS2 rückt auch die Absicherung der Lieferkette in den Fokus. Warum ist das für den Gesetzgeber so wichtig?*

Sudhir Ethiraj: Sogenannte Supply-Chain-Angriffe zielen darauf ab, Schwachstellen in der Lieferkette auszunutzen, um Zugang zu sensiblen Daten und Systemen zu erlangen. Ob durch das Einfügen von Schadsoftware in legitime Software-Updates, durch das Kompromittieren von Drittanbietern, die Zugang zu den Netzwerken eines Unternehmens haben, einen Insider-Angriff oder gar infizierte Hardware – die Wege für Cyberkriminelle über die Lieferkette sind vielfältig. Das bekannte Beispiel SolarWinds, bei dem die Angreifer über ein Software-Update in die Netzwerke zahlreicher Organisationen eindringen konnten, hat gezeigt, dass die Gefahr von Supply-Chain-Angriffen in ihrer Heimtücke und der Schwierigkeit, sie zu erkennen, liegt.

Da die Angriffe oft über vertrauenswürdige Partner oder Lieferanten erfolgen, können sie lange unentdeckt bleiben und erheblichen Schaden anrichten. Deshalb verlangt NIS2 von Unternehmen, Maßnahmen zu ergreifen, um ihre Lieferketten sorgfältig zu überwachen. So sollen potenzielle Bedrohungen frühzeitig erkannt und abgewehrt und Vorkehrungen für den Fall eines erfolgreichen Angriffs ergriffen werden.

it security: *Was genau schreibt NIS2 und der aktuelle Stand des deutschen NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz vor?*

Sudhir Ethiraj: Die europäische Network-and-Information-Security-Richtlinie, kurz NIS2, schreibt in Artikel 21 Absatz 2 vor, dass sich besonders wichtige und wichtige Einrichtungen mit Cybersicherheitsrisiken ihrer Lieferketten befassen müssen. Der Entwurf für das deutsche NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz greift das in §30 auf. Dort heißt es, dass besonders wichtige und wichtige Einrichtungen zu bestimmten Risikomanagementmaßnahme verpflichtet sind. Diese Maßnahmen betreffen unter anderem auch die Sicherheit der Lieferkette. Im Fokus stehen dabei die sicherheitsbezogenen Aspekte der Beziehung zwischen den einzelnen Einrichtungen und ihren direkten Anbietern und Dienstleistern.

Im Gesetzesentwurf heißt es, dass KRITIS-Betreiber dazu verpflichtet sind, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen. Das Ziel ist dabei natürlich, die Cyberresilienz dieser Einrichtungen zu erhöhen und die Auswirkungen von Sicherheitsvorfällen gering zu halten.

it security: *Was bedeutet das nun konkret für die IT-Manager der KRITIS-Betreiber?*

Sudhir Ethiraj: Unternehmen sollten mittlerweile herausgefunden haben, ob sie zu den sogenannten „besonders wichtigen" und „wichtigen" Einrichtungen nach NIS2 zählen. Wenn nicht, ist das der erste, längst überfällige Schritt. Und dann müssen IT-Manager ihre Lieferkette genau in den Blick nehmen. Der Gesetzentwurf für das NIS2 Umsetzungsgesetz verlangt auch, die Verhältnismäßigkeit der Risikomanagementmaßnahmen zu prüfen. Folgende Kriterien müssen in diese Betrachtung einfließen: das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen.

it security: *Das klingt aber sehr zeitaufwendig. Wie kann man das am besten angehen?*

Sudhir Ethiraj: Das ist es in der Tat. Deshalb raten wir Unternehmen jetzt zu handeln. Risk Assessments, die von

neutralen Dritten durchgeführt werden, können IT-Managern bei dieser zeitintensiven Aufgabe helfen. Damit holt man sich Cybersecurity-Audit-Erfahrung und Expertise in den entsprechenden Gesetzestexten ins Haus. Das Assessment deckt die in NIS2 genannten Schlüsselaspekte ab. Um den aktuellen Status seiner Organisation und den Handlungsbedarf zu verstehen, ist es wichtig, die relevanten Interessensgruppen innerhalb des Unternehmens zu identifizieren und mit ihnen Gespräche zu führen. IT-Manager bekommen so Lücken aufgezeigt, die geschlossen werden müssen, um die Cyber-Resilienz in der Lieferkette zu gewährleisten.

> MIT NIS2 WIRD DAS BEWUSSTSEIN FÜR CYBERSECURITY IN DER LIEFERKETTE GESTÄRKT.
>
> **Sudhir Ethiraj, Global Head of Cybersecurity Office (CSO) & CEO Business Unit Cybersecurity Services, TÜV SÜD GmbH, www.tuvsud.com/de-de**

it security: *Und was ist mit den mittelbar von NIS2 betroffenen Zulieferern und Dienstleistern – heißt das, dass sie unbedingt nach ISO 27001 zertifiziert sein müssen?*

Sudhir Ethiraj: Nein, das heißt es nicht zwangsläufig. Aber auch auf die mittelbar betroffenen Unternehmen kommt einiges an Arbeit zu. So kann es sehr wohl KRITIS-Einrichtungen geben, die eine ISO 27001-Zertifizierung verlangen. Grundsätzlich ist ISO 27001 immer eine gute Grundlage für Cyberresilienz, denn sie ermöglicht Unternehmen, ein effektives Information Security Management System (ISMS) zu etablieren und zu pflegen. Mit einer Zertifizierung nach ISO 27001 kann also ein effektives Risikomanagement von Zulieferern und Dienstleistern gegenüber KRITIS-Betreibern durchaus demonstriert werden.

Je nach Anwendungsfall gibt es noch weitere Standards und Best Practices, die berücksichtigt werden müssen, um Cyber-Resilienz zu erreichen und zu belegen, etwa das NIST Cybersecurity Framework oder IEC 62443.

it security: *Was passiert zukünftig, wenn doch einmal etwas passiert?*

Sudhir Ethiraj: Es kann niemals ganz ausgeschlossen werden, dass Cyberangriffe erfolgreich sind. Davon geht auch NIS2 nicht aus. Es ist ein dreistufiges Melderegime vorgesehen mit einer Erstmeldung spätestens 24 Stunden nach Kenntniserlangung, einer Bestätigung oder Aktualisierung nach 72 Stunden und einer Abschlussmeldung nach einem Monat, die auch die getroffenen und laufenden Abhilfemaßnahmen beinhalten muss.

Die implementierten Risikomanagementmaßnahmen sollen im Falle eines erfolgreichen Angriffs negative wirtschaftliche und gesellschaftliche Folgen minimieren. Dabei sollte man nicht eine der wichtigsten Änderungen von NIS2 vergessen: die Richtlinie definiert direkte Verpflichtungen der Geschäftsführung und macht ihr gegenüber Haftungsansprüche in Bezug auf die Umsetzung der erforderlichen Risikomanagementmaßnahmen im Bereich Cybersecurity geltend. Das heißt für IT-Manager, dass sie mit ihren Geschäftsführungen Hand-in-Hand bei der Erarbeitung und Umsetzung der Risikomanagementmaßnahmen arbeiten müssen. Denn nach NIS2 müssen Geschäftsführungen diese Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung überwachen.

Doch bei all diesem Aufwand sollten wir eines auch positiv sehen: Mit NIS2 wird das Bewusstsein für Cybersecurity in der Lieferkette gestärkt. Denn die Angriffe werden nicht weniger. Und auch Organisationen, die nicht direkt von NIS2 betroffen sind, sollten auf jeden Fall Risikomanagementmaßnahmen in Betracht ziehen, um ihre Cyber-Resilienz zu verbessern. Auch hier kann ein Risk Assessment ein wertvoller erster Schritt sein.

it security: *Herr Ethiraj, wir danken für dieses Gespräch.*

Europas erstes KI-Abwehrzentrum: Cyberabwehr neu definiert

WIE KÜNSTLICHE INTELLIGENZ DAS SOC DER ZUKUNFT ANTREIBT

Die digitale Revolution hat unzählige Vorteile für Unternehmen und die Gesellschaft gebracht. Gleichzeitig verschärft die fortschreitende Digitalisierung die Bedrohungslage drastisch weiter. Angreifer sind heute in der Lage, Künstliche Intelligenz (KI) zu nutzen, um bestehende Angriffsmethoden zu perfektionieren und hochentwickelte Cyberangriffe zu starten, die traditionelle Sicherheitssysteme eher überfordern. Reaktive Systeme und Security Operations Center (SOC), die erst nach einem Angriff Alarm schlagen, sind längst nicht mehr ausreichend. Ein Umdenken ist erforderlich – und Europas erstes KI-Abwehrzentrum ist die Antwort auf diese Herausforderung.

Das KI-Dilemma – Angstgegner und Hoffnungsträger in einem

Angst entsteht aus dem Unbekannten. Organisationen haben Prozesse und Verfahren zur Verteidigung gegen bekannte Angriffe wie Datenschutzverletzungen entwickelt, aber sie wissen bisher eher nicht, wie sie mit KI-gesteuerten Angriffen umgehen. Böse Zungen mögen behaupten, viele KMU wüssten es auch bei den altbekannten Bedrohungen nicht oder täten zu wenig.

So oder so: Gegen KI-basierte Angriffe reichen die bisherigen Maßnahmen nicht mehr aus. Die Angreifer nutzen KI bereits aktiv, um Phishing-E-Mails und Fake-Videos zu erstellen, die so realistisch sind, dass sie kaum noch von echten zu unterscheiden sind. Sie verfeinern bösartige Skripte mittels KI etc.

> UNSER ZIEL IST ES, DIE POSITIVEN SEITEN VON KI ZU NUTZEN, UM DIE NEGATIVEN ZU BEKÄMPFEN.

Alexander Sowinski, Gründer des KI-ABWEHRZENTRUMS und CEO, ASOFTNET GmbH & Co. KG, www.asoftnet.de, www.ki-abwehrzentrum.de

Welche Bedrohungen sie mittels KI künftig noch generieren werden, möchte man sich eigentlich gar nicht ausmalen. Die Möglichkeiten scheinen endlos; und machen Angst. Sind die mehrheitlichen Zweifel, dass es gelingen kann, durch KI die Oberhand im Cyberkrieg zu behalten[1], also gerechtfertigt?

Sollten wir davon ausgehen, dass die Angreifer den größten Nutzen aus KI ziehen werden und uns kampflos ergeben? Wohl kaum! Es ist Zeit, dass wir die Macht von KI in unsere eigenen Hände nehmen! Unternehmen, die KI-Technologien sinnvoll in ihre Abwehr integrieren, haben eine realistische Überlebenschance. Sind Sie dabei, oder bleiben Sie in der Defensive?

Reaktive SOC-Systeme reichen nicht mehr aus

Die durchschnittliche Zeit, die ein Unternehmen ohne SOC benötigt, um eine Sicherheitslücke zu erkennen, beträgt 165 Tage[2]. Ein halbes Jahr – das ist eine Ewigkeit in der Cyberwelt! Unternehmen mit einem SOC sind da besser aufgestellt und können eine Sicherheitslücke innerhalb eines Tages entdecken. Doch auch hier gilt: Ausruhen gibt's nicht! SOC ist nicht gleich ein SOC. Traditionelle, reaktive Systeme sind schon längst nicht mehr das Nonplusultra.

Fragen Sie sich: Können Sie es sich leisten, erst zu reagieren, wenn der Schaden schon da ist? Ohne proaktive, vorausschauende Maßnahmen – die wir eigentlich nur mittels KI erreichen können – bleibt es ein gefährliches Spiel. Sind Sie bereit, das Risiko einzugehen?

Der Wandel: Proaktive IT-Sicherheit durch KI

Proaktive Cybersicherheit bedeutet mehr als blanke Reaktion. Sie bedeutet, Sicherheitslücken aktiv zu suchen und zu schließen, bevor Angriffe geplant werden. KI macht das tatsächlich möglich. Künstliche Intelligenz verarbeitet in Echtzeit riesige Mengen an Daten aus verschiedenen Quellen – darunter das Darknet und soziale Medien. Fortgeschrittene Algorithmen erkennen Anomalien und berechnen die Wahrscheinlichkeit eines Angriffs, bevor er stattfindet.

[1] Laut Splunk (State of Security The Race to Harness AI, 2024) gehen 45 Prozent der Befragten gehen davon aus, dass die Angreifer den größten Nutzen ziehen werden. Im Vergleich dazu glauben 43 Prozent glauben, dass die Verteidiger die Oberhand behalten werden.
[2] Bitkom 2023

Warum KI der Schlüssel zur Abwehr moderner Angriffe ist:

- **Frühzeitige Erkennung:** Angriffe werden schon in der Planungsphase erkannt.
- **Effizienz:** Bedrohungen werden automatisiert analysiert und abgewehrt.
- **Flexibilität:** KI lernt in Echtzeit dazu und passt sich neuen Bedrohungen an.

Die Zeit der Ausreden ist vorbei. Unternehmen, die jetzt nicht handeln, sind dem Untergang nah.

Europas erstes KI-Abwehrzentrum

Die Bedrohungen durch KI-gestützte Cyberangriffe sind real und wachsen. Europas erstes KI-Abwehrzentrum in Zusammenarbeit mit führenden deutschen IT-Sicherheitsunternehmen setzt neue Maßstäbe in der Bedrohungsabwehr, nicht nur für Enterprise-Unternehmen.

Technische Umsetzung: So arbeitet das KI-Abwehrzentrum

Das KI-Abwehrzentrum nutzt modernste Technologien, um Daten aus verschiedenen Quellen zu sammeln und auszuwerten. Informationen aus dem Darknet, Social Media und speziellen Kommunikationskanälen von Cyberkriminellen werden kombiniert, analysiert und durch maschinelles Lernen optimiert. So wird eine ganzheitliche Bedrohungsanalyse in Echtzeit ermöglicht. Das KI-Abwehrzentrum übernimmt neben der Überwachung & Früherkennung auch die Entwicklung von Schutzmechanismen, die Krisenmanagement & Koordination sowie Forschung & Ethik.

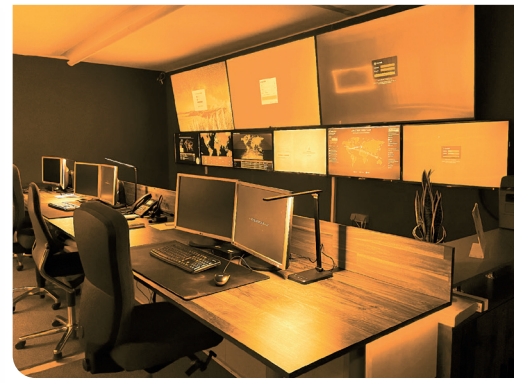
Was bedeutet das für Sie? – Sie haben endlich Klarheit über die Bedrohungslage, anstatt nur auf Vermutungen zu setzen plus die bestmögliche, proaktive Abwehr bisher unbekannter Bedrohungen, noch bevor diese Ihnen gefährlich werden.

Vorteile von KI-Abwehr im Vergleich zu herkömmlichen SOC-Lösungen:

- **Schnelle Analyse und Alarmierung:** Bedrohungen werden erkannt, bevor ein Angriff erfolgt.
- **Wahrscheinlichkeitsberechnung:** KI-Systeme berechnen kontinuierlich die Wahrscheinlichkeit eines Angriffs.
- **Tiefere Einblicke:** Sie erhalten eine objektive Sicht auf Ihre IT-Sicherheitslage.
- **Stetiges Training und Lernen** der KI im KI-ABWEHRZENTRUM sichert die Weiterentwicklung.

Fazit: Die Zukunft der Cybersicherheit heißt KI-Abwehrzentrum

Die Bedrohungen durch Cyberangriffe werden immer ausgeklügelter und gefährlicher. Haben Sie wirklich noch die Illusion, dass Ihre alten Abwehrstrategien ausreichen? Reaktive Methoden gehören der Vergangenheit an. Nur eine proaktive Abwehrstrategie, die künstliche Intelligenz mit Expertenwissen kombiniert, wird den entscheidenden Vorteil bringen. Unternehmen, die dies nicht begreifen: Viel Glück!



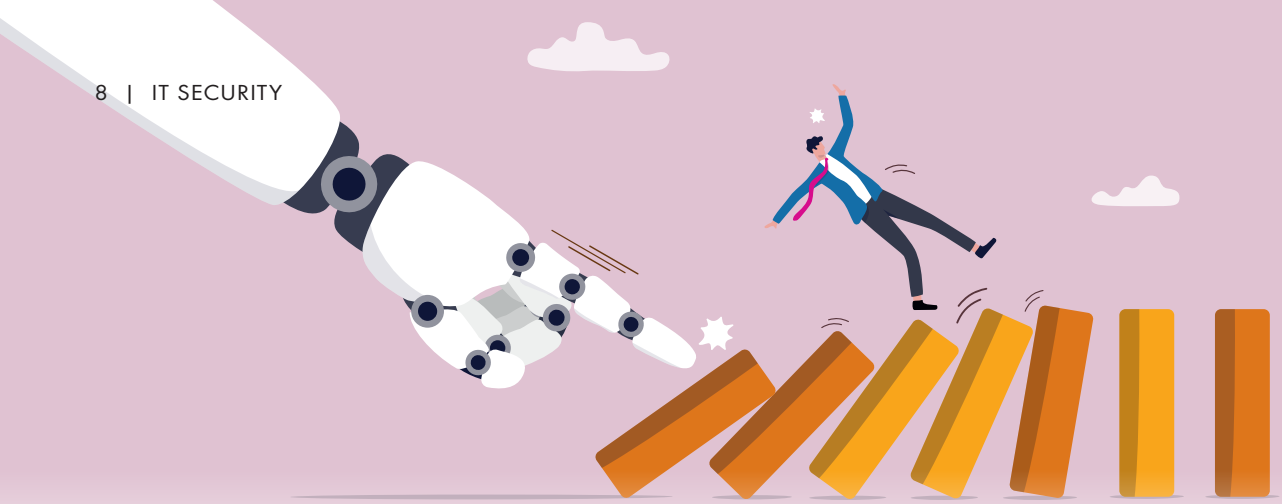
Die Lösung gegen die Cyberangriffe von heute und morgen ist da – und sie heißt KI-Abwehrzentrum. Sind Sie bereit, oder warten Sie weiter?

Alexander Sowinski | www.asoftnet.de

ASOFTNET Security-Step-up

Security-Audit	MDR	SOC as a Service	KI-ABWEHRZENTRUM
Regelmäßiger Security-Statusreport	24/7/365 Managed Security		
	Überwachung der IT-Systeme	Proaktive Threat-Analyse	
	Auswertung der Alarme	Auswertung mit mehreren Tools	
	Erste Gegenmaßnahmen	Playbooks & erste Gegenmaßnahmen	
		30 Minuten Reaktionszeit	
		Forensische Analyse	
		Incident Response	
		Threat-Hunting	
		Darknet-Analyse	
		Aufklärung im Internet + Darknet	
			Automatisierte Erkennung KI-basierter Angriffe
			KI-basierte Gegenmaßnahmen + Angriffsabwehr
			Vorhersage der nächsten Angriffe

Quelle: ASOFTNET GMBH & CO.KG



Datensicherheit

VERBRAUCHER SEHEN KI ALS RISIKO FÜR DATENSICHERHEIT

Weltweit sind Verbraucher sehr besorgt über die Menge an Daten, die Unternehmen über sie sammeln, den Umgang damit und sehen auch deren Sicherheit gefährdet – insbesondere durch die den zunehmenden Einsatz von künstlicher Intelligenz. Das belegt eine Umfrage von Cohesity, für die weltweit mehr als 6.000 Verbraucher befragt wurden. Demnach kritisieren 79 Prozent der weltweit Befragten, dass Unternehmen zu viele persönliche oder finanzielle Daten über sie sammeln. Neben der Kritik am Datenhunger verdeutlichen die Ergebnisse, dass Verbraucher eine größere Sorgfalt der Unternehmen beim Schutz der erhobenen persönlichen Daten erwarten. Das bestätigen 82 Prozent der weltweit Befragten.

In Deutschland sorgt sich ein ähnlich hoher Anteil der Internetnutzer um die Sicherheit ihrer persönlichen Daten im Netz. Laut einer Bitkom-Umfrage aus dem Januar 2024 halten 77 Prozent der Befragten ihre Daten online für eher unsicher oder sehr unsicher. Dabei ist es heute wichtiger denn je, den Erwartungen der Kunden an einen wirksamen Schutz ihrer sensiblen Daten gerecht zu werden. Denn über 90 Prozent der Befragten gaben an, dass sie nicht mehr Kunden eines Unternehmens sein möchten, wenn dieses Opfer eines Cyberangriffs wird. Verbraucher sind also bereit, den Anbieter zu wechseln, wenn sie das Vertrauen verlieren.

Die häufigsten Ängste

International äußern laut der Cohesity-Befragung viele Verbraucher die Befürchtung, dass sich KI negativ auf die Sicherheit ihrer Daten auswirkt, und beklagen die mangelnde Transparenz der Unternehmen hinsichtlich ihrer KI-Prozesse.

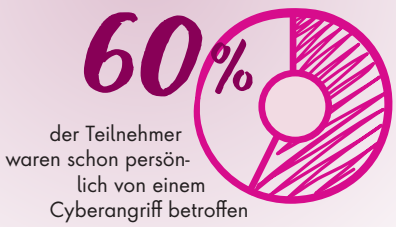
- Fast alle Verbraucher (90 %) weltweit sind besorgt, dass KI die Sicherung und Verwaltung ihrer Daten erheblich erschweren wird.
- Die meisten gehen sogar noch einen Schritt weiter und stufen KI als Risiko für den Datenschutz und die Datensicherheit ein (71 %).
- Mehr als drei Viertel der Verbraucher (78 %) haben ernsthafte Bedenken hinsichtlich der uneingeschränkten oder unkontrollierten Nutzung ihrer Daten durch KI.
- Weltweit wollen Nutzer (82 %) zumindest um Erlaubnis gefragt werden, bevor ihre persönlichen oder finanziellen Daten in KI-Modelle eingespeist werden.

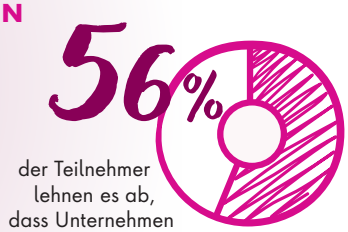
Die Erwartung einer größeren Transparenz gilt auch für die gängige Praxis der gemeinsamen Nutzung von Daten mit Drittanbietern.

- Die große Mehrheit der Befragten weltweit (85 %) möchte wissen, mit wem ihre Daten geteilt werden.
- Die meisten Befragten (84 %) fordern außerdem, dass Unternehmen die Datensicherheit und die allgemeinen Verwaltungsprozesse von Drittanbietern überprüfen.

www.cohesity.com/de

WENN VERBRAUCHERDATEN KOMPROMITTIERT WERDEN





(Quelle: Cohesity)

IT-Sicherheit mit generativer KI

AKTUELLE UND ZUKÜNFTIGE CHANCEN FÜR IT-SECURITY

GENERATIVE KI BIRGT ENTSCHEIDENDES POTENZIAL, WIRD CYBERSICHERHEITSPRODUKTE JEDOCH NICHT VON JETZT AUF GLEICH NEU ERFINDEN.

Michael Haas, Regional Vice President Central Europe, WatchGuard Technologies, www.watchguard.de

KI-Technologien sind inzwischen ein elementarer Baustein vieler moderner „Detection and Response"-Lösungen. Die Produkte nutzen oftmals Machine Learning (ML) und Deep Learning, um anomale Verhaltensweisen zu erkennen, die auf eine potenzielle Bedrohung oder einen Angriff innerhalb einer IT-Umgebung hinweisen.

GenAI noch im Reifeprozess

Im Gegensatz dazu ist generative KI (GenAI) das Nesthäkchen im KI-Umfeld. Tools wie ChatGPT gibt es erst seit zwei Jahren. Während sich andere KI-Technologien vor allem auf das Lernen aus großen Datensätzen konzentriert haben, zeigt GenAI seine Stärken bei der Erstellung schriftlicher, visueller und auditiver Inhalte unter Verwendung von Prompts oder Eingabedaten. Hier steht die Security-Branche noch am Anfang, den Mehrwert im Zuge unterschiedlicher Anwendungsfälle dediziert auf Herz und Nieren zu prüfen. Entsprechende Ansatzpunkte sind jedoch offensichtlich:

➤ **E-Mail:** Möglicherweise liefert GenAI eine stichhaltige Antwort auf die Frage, wie sich Phishing-Versuche blockieren lassen, bevor entsprechende Mails im Posteingang landen. Bestehende Lösungen verlassen sich noch stark darauf, dass Mitarbeitende Phishing-Nachrichten identifizieren und melden. GenAI-basierte Produkte, die darauf trainiert sind, Anomalien in geschriebener Sprache und E-Mail-Adressen zu erkennen, könnten die von Spam- und Phishing-Nachrichten ausgehende Gefahr drastisch reduzieren. Leider nutzen auch Hacker GenAI, um die Qualität ihrer Nachrichten zu verbessern, so dass wir wohl einige einfache Möglichkeiten, die heute bei der Erkennung von Phishing-Nachrichten Wirkung entfalten, verlieren werden.

➤ **Identität:** Cyberkriminelle verwenden inzwischen GenAI-basierte Werkzeuge, um andere Menschen zu imitieren, einschließlich der Nachahmung ihrer Stimme, ihres Bildes und Schreibstils. Die Ergebnisse sind oftmals nicht hundertprozentig exakt. Daher kann es helfen, GenAI auch in Sicherheitsprodukten einzusetzen, um genau die abweichenden Details zu beleuchten.

➤ **Reporting:** Bei der Erstellung individueller Berichte kann GenAI klar punkten. Mit wenigen Eingaben sind benutzerdefinierte Reports generierbar, die die Einhaltung von Sicherheitsprotokollen aufzeigen. Selbst wenn die heutigen GenAI-Funktionen noch nicht so weit ausgereift sind, um diesen Prozess vollständig zu automatisieren und händische Nacharbeit erforderlich ist: Schneller geht es allemal.

➤ **Verbesserte Assistenten zur Sicherheitsanalyse:** Mit GenAI-Tools lassen sich identifizierte Vorfälle oder sicherheitsrelevante Erkenntnisse zusammenzufassen. Technische Sprache kann in verständliche Formulierungen gegossen werden, empfohlene Maßnahmen werden dadurch nachvollziehbarer.

Fazit

GenAI birgt entscheidendes Potenzial, wird Cybersicherheitsprodukte jedoch nicht von jetzt auf gleich neu erfinden. Es sollte nicht vergessen werden, wie positiv sich etabliertere KI- und ML-Technologien schon heute im Rahmen einer modernen Cyberabwehr auswirken. Da Bedrohungsakteure ähnliche Technologien einsetzen, um ihre Angriffe zu verstärken, sind KI-gestützte Funktionen zur Erkennung von und Reaktion auf Bedrohungen mittlerweile ein Muss.

Michael Haas

Bild: GettyImages

Risiken von KI für die Cybersicherheit

MASSNAHMEN ZUR VERBESSERUNG DER SECURITY DURCH NETZWERKSICHERHEIT

Laut dem Bundeskriminalamt (BKA) wurden im Jahr 2023 insgesamt 146.363 Fälle von Cyberkriminalität registriert, was einem Anstieg von mehr als zwölf Prozent gegenüber dem Vorjahr entspricht. Die Zahl der Straftaten, die aus dem Ausland oder von einem unbekannten Ort aus verübt werden und zu Schäden in Deutschland führen, stieg 2023 um 28 Prozent gegenüber dem Vorjahr.

Die wirtschaftlichen Schäden durch Cyberangriffe in Deutschland beliefen sich im Jahr 2023 auf etwa 148 Milliarden Euro. Diese Zahlen verdeutlichen die anhaltend hohe Bedrohungslage und die Notwendigkeit, effektive Sicherheitsmaßnahmen zu implementieren.

Aktuell gibt es keine spezifischen Statistiken, die den genauen Anteil von Straftaten, die mit Hilfe von KI verübt wurden, in Deutschland ausweisen. Das Bundeskriminalamt (BKA) und andere Sicherheitsbehörden haben jedoch erkannt, dass der Einsatz von KI in der Cyberkriminalität zunimmt. Insbesondere bei Phishing-Angriffen, der Erstellung von Schadsoftware und der Nutzung von Deepfakes wird KI vermehrt eingesetzt.

Europol und das BKA warnen vor den Möglichkeiten, die künstliche Intelligenz Kriminellen bietet, und betonen, dass die Qualität und Vielfalt der kriminellen Anwendungen von KI stetig zunehmen. Es wird erwartet, dass in Zukunft detailliertere Statistiken und Berichte erstellt werden, um das Ausmaß und die Auswirkungen von KI-gestützten Straftaten besser zu erfassen.

KI generierte Malware

Böswillige Akteure können die Vorteile der KI auf verschiedene Weise nutzen. Mit KI lassen sich beispielsweise Muster in Computersystemen identifizieren, die Schwachstellen in Software oder Sicherheitsprogrammen aufdecken, und so Hackern ermöglichen, diese neu entdeckten Schwachstellen auszunutzen. In Kombination mit gestohlenen persönlichen Informationen oder gesammelten Open-Source-Daten wie Social-Media-Posts können Cyberkriminelle KI nutzen, um eine große Anzahl von Phishing-E-Mails zu erstellen, um Malware zu verbreiten oder wertvolle Informationen über das Unternehmen und Mitarbeitende zu sammeln.

Sicherheitsexperten haben festgestellt, dass KI-generierte Phishing-E-Mails tatsächlich eine höhere Öffnungsrate aufweisen, um mögliche Opfer dazu zu bringen, darauf zu klicken und so Angriffe zu generieren, als manuell erstellte Phishing-E-Mails. KI kann auch verwendet werden, um Malware zu entwickeln, die sich ständig verändert, um eine Erkennung durch automatisierte Abwehrtools zu vermeiden.

Mit Zero Trust gegen KI-gestützte Malware

Ständig wechselnde Malware-Signaturen können Angreifern helfen, statische Abwehrmaßnahmen wie Firewalls und Pe-

MASSNAHMEN ZUM SCHUTZ VOR KI-BASIERTEN BEDROHUNGEN

1. Netzwerksicherheit: Implementierung fortschrittlicher Netzwerksicherheitslösungen, um verdächtige Aktivitäten frühzeitig zu erkennen und zu blockieren.
2. KI-basierte Sicherheitslösungen: KI kann helfen, Anomalien im Netzwerkverkehr zu identifizieren und potenzielle Angriffe zu verhindern.
3. Mitarbeiterschulung: Regelmäßige Schulungen erhöhen das Bewusstsein für Cyberrisiken
4. Sicherheitsrichtlinien und -verfahren: Entwicklung und Implementierung umfassender Sicherheitsrichtlinien und -verfahren, die regelmäßig überprüft und aktualisiert werden.

rimeter-Erkennungssysteme zu umgehen. In ähnlicher Weise kann KI-gestützte Malware in einem System sitzen, Daten sammeln und das Benutzerverhalten beobachten, bis sie bereit ist, eine weitere Phase eines Angriffs zu starten, oder gesammelte Informationen mit relativ geringem Entdeckungsrisiko zu versenden. Dies ist zum Teil der Grund, warum sich Unternehmen in Richtung eines "Zero-Trust"-Modells bewegen, bei dem Abwehrmaßnahmen so eingerichtet sind, dass sie den Netzwerkverkehr und die Anwendungen ständig hinterfragen und überprüfen, um sicherzustellen, dass sie nicht schädlich sind.

Chancen & Herausforderungen

Die zunehmende Nutzung von Künstlicher Intelligenz (KI) bringt sowohl Chancen als auch Herausforderungen mit sich, insbesondere im Bereich der Cybersicherheit. Hier sind einige der wichtigsten Herausforderungen und Maßnahmen, die Unternehmen zur Steigerung der Resilienz ergreifen können:

- Herausforderungen durch KI im Bereich Cybercrime und Unternehmensspionage
- Automatisierte Angriffe und automatisierte Skalierung erhöhen die Geschwindigkeit und Effizienz von Cyberangriffen.
- KI-Modelle können genutzt werden, um Schadsoftware zu generieren, die schwerer zu erkennen und zu bekämpfen ist.
- KI kann personalisierte Phishing-Angriffe und Deepfakes erstellen (Social Engineering), die schwerer zu identifizieren sind.

Rolle der Netzwerksicherheit

Network Access Control (NAC)-Lösungen bieten eine umfassende Sicherheitsarchitektur, die durch die Integration von Künstlicher Intelligenz (KI) und maschinellem Lernen eine neue Ebene der Kontrolle und Sicherheit erreichen kann.

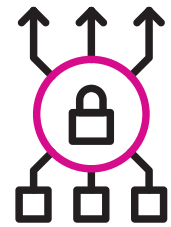
Dazu Malte Marquardt, Solution Sales Cybersecurity Lead, EMEA Belden:

„Es ist wichtig, dass Unternehmen proaktiv handeln und ihre Sicherheitsmaßnahmen kontinuierlich prüfen und anpassen, um den sich ständig weiterentwickelnden Bedrohungen durch KI gerecht zu werden. Netzwerk-Sicherheitslösungen für IT- und OT-Infrastrukturen stellen dabei als technische Maßnahme eine wichtige Säule dar, denn sie sorgen für eine robuste und dynamische Sicherheitsinfrastruktur, die den Schutz vor modernen Cyber-Bedrohungen erheblich verbessert. Jedoch lösen Technologien nicht alle Herausforderungen der Digitalisierung, sondern müssen immer einher mit organisatorischen Maßnahmen gehen, die klar definierten Abläufen und Zuständigkeiten folgen."

BEWÄLTIGUNG AKTUELLER CYBERSECURITY-HERAUSFORDERUNGEN

mit Hilfe von Network Access Control (NAC):

- Umfassende Netzwerktransparenz
- Automatisierte Sicherheitsrichtlinien
- Einhaltung von Compliance-Vorgaben
- Integration mit bestehenden Sicherheitslösungen
- Skalierbarkeit und Flexibilität



- **Automatisierte Anomalie Erkennung:** Network Access Control-Systeme sind in der Lage, Anomalien, Sicherheitslücken und Angriffsmuster automatisch zu erkennen. Sie erstellen ein Normalmodell des Netzwerks und identifizieren Abweichungen, die auf potenzielle Cyber-Angriffe hinweisen.
- **Echtzeitüberwachung und -reaktion:** Durch die kontinuierliche Überwachung des Netzwerkverkehrs kann verdächtiges Verhalten frühzeitig erkannt, und sofortige Gegenmaßnahmen eingeleitet werden. Dies beschleunigt die Erkennung und Neutralisierung von Bedrohungen erheblich.
- **Zugriffskontrolle und Authentifizierung:** NAC-Lösungen fungieren als erste Verteidigungslinie, indem sie sicherstellen, dass nur autorisierte Geräte und Benutzer tatsächlichen Zugang zum Netzwerk erhalten. Dies wird durch strenge Authentifizierungs- und Autorisierungsprozesse gewährleistet.
- **Datenintegration und -analyse:** NAC-Lösungen sammeln und analysieren umfangreiche Datenmengen aus dem Netzwerk. Durch den Einsatz von maschinellem Lernen können diese Daten genutzt werden, um Prozesse zu optimieren und Sicherheitsmaßnahmen zu verstärken.
- **Effiziente Problemlösung:** Bei Netzwerkproblemen ermöglicht die Analyse eine schnelle Identifizierung und Behebung von Fehlerursachen. Dies verbessert die Netzwerkstabilität und reduziert Ausfallzeiten.

Sabine Kuch | www.macmon.eu

Künstliche Intelligenz

WELCHE CHANCEN DIE KI FÜR DIE CYBERSICHERHEIT BIETET

Künstliche Intelligenz hat längst auch im Bereich der Cybersicherheit Einzug gehalten – und sie kann dort Gutes bewirken. Die Technologie bietet viel Potenzial, insbesondere für effizientere Abläufe bei der Cyberabwehr. Dr. Jens Schmidt-Sceery, Partner bei der M&A-Beratung Pava Partners, und Frank Brandenburg, Chairman bei DataExpert, glauben jedoch, dass die Chancen der KI für die Cybersicherheit einerseits über- und andererseits unterschätzt werden.

it security: *Künstliche Intelligenz (KI) hat längst auch in der Cybersecurity Einzug gehalten. Aber hat die KI das Zeug dazu, menschliche Intelligenz in diesem Bereich schon bald zu ersetzen?*

MITHILFE DER KI KÖNNEN AUSSERDEM EINE 24/7 ÜBERWACHUNG DER SYSTEME REALISIERT UND SICHERHEITS-LÜCKEN IN ECHTZEIT IDENTIFIZIERT WERDEN.

Frank Brandenburg, Chairman, DataExpert, www.dataexpert.eu/

Jens Schmidt-Sceery: Es stimmt, dass heute schon viele Cybersecurity-Unternehmen KI in ihre Anwendungen integrieren. Das sind zum Beispiel intelligente Thread-Detection-Systeme oder Analyse-Programme, die in der Lage sind, Anomalien zu detektieren. Bei genauerem Hinsehen stellt man jedoch schnell fest, dass es sich bei solchen Tools um Machine Learning (ML)-Anwendungen handelt. Zwar ist ML quasi ein Teilbereich von KI, aber dennoch gibt es deutliche Unterschiede.

it security: *Welche Unterschiede sind das genau?*

Jens Schmidt-Sceery: Die größten Unterschiede gibt es beim Ziel, aber auch in der Methodik der Anwendung. Die Künstliche Intelligenz soll Maschinen erschaffen, die dazu befähigt sind, die menschliche Intelligenz zu kopieren und anzuwenden. Das Ziel von Maschine Learning ist es dagegen, Algorithmen zu schaffen, die aus großen Datenmengen lernen und so die Leistung bei speziellen Aufgaben optimieren können. Die Unterscheidung in der Methodik liegt darin, dass KI auf verschiedene Techniken zurückgreift, unter anderem auf ML, regelbasierte Systeme und Wissensrepräsentationen. ML-Systeme arbeiten dagegen mit statistischen Modellen und Algorithmen, mit deren Hilfe sie aus Daten lernen können. Diese Unterscheidungsmerkmale beider Technologien muss man kennen, wenn man verstehen will, warum die Möglichkeiten der KI im Bereich der Cybersecurity aktuell eher überschätzt werden.

it security: *Könnte man also sagen, es fehlt der KI (derzeit noch) die Kreativität, die bislang nur der Mensch in der Lage ist, zu entwickeln?*

Frank Brandenburg: Wirft man einen Blick auf die aktuelle Bedrohungslage im Bereich der Cybersicherheit, so lässt sich Folgendes feststellen: Die am häufigsten durchgeführten Angriffe auf Unternehmen und öffentliche Einrichtungen basieren noch immer auf Phishing oder Social Engineering. Angreifer mit krimineller Energie haben es heute durch den Einsatz von zuverlässigen KI-basierten Rechtschreibprogrammen deutlich leichter, glaubwürdige und offiziell anmutende Fake-Mails zu kreieren und verschicken. Anfang des Jahres 2024 wurden etwa gefälschte E-Mails in der Aufmachung der Plattform ELSTER der deutschen Finanzbehörden versendet.

Auf der anderen Seite bietet die KI, zumindest derzeit, keine neuen, kreativen Ansätze, um Zero-Day-Angriffe in komplexen Anwendungen zu entdecken. Denn eine KI kann nur auf vorhandene Daten trainiert werden oder anders formuliert nur bereits vorhandenes Wissen für neue Herausforderungen zum Einsatz bringen. Wie Sie bereits richtig vermutet haben, ist eine KI bislang nicht in der Lage Kreativität zu entwickeln.

it security: *Das heißt, dass die Abwehr von Cyberangriffen ohne menschliches Zutun auf absehbare Zeit nicht möglich sein wird?*

Frank Brandenburg: Korrekt, die fehlende Kreativität einer KI ist für die Cy-

berabwehr ein Problem. Ein Algorithmus kann zwar Anomalien in großen Datenvolumina leicht erkennen, dieser Prozess basiert jedoch letztendlich auf Machine Learning. Um Abweichungen im System zu erkennen, genügt der Einsatz statistischer Methoden. Dank dieser Unterstützung können Cyberangriffe wesentlich schneller entdeckt werden, eine KI kann jedoch selbständig keine passenden Gegenmaßnahmen ergreifen, zumindest heute noch nicht. Dafür ist menschliches Eingreifen notwendig, denn kreative Angriffe erfordern kreative Lösungen. Und es gehört zu den Eigenheiten der Cybersicherheit, dass auch kurzfristig auf immer wieder neue Bedrohungen reagiert werden muss. Bekannte Angriffsmethoden sollten bei geeigneter Vorsorge von Unternehmen sowieso nicht zu einer Bedrohung werden.

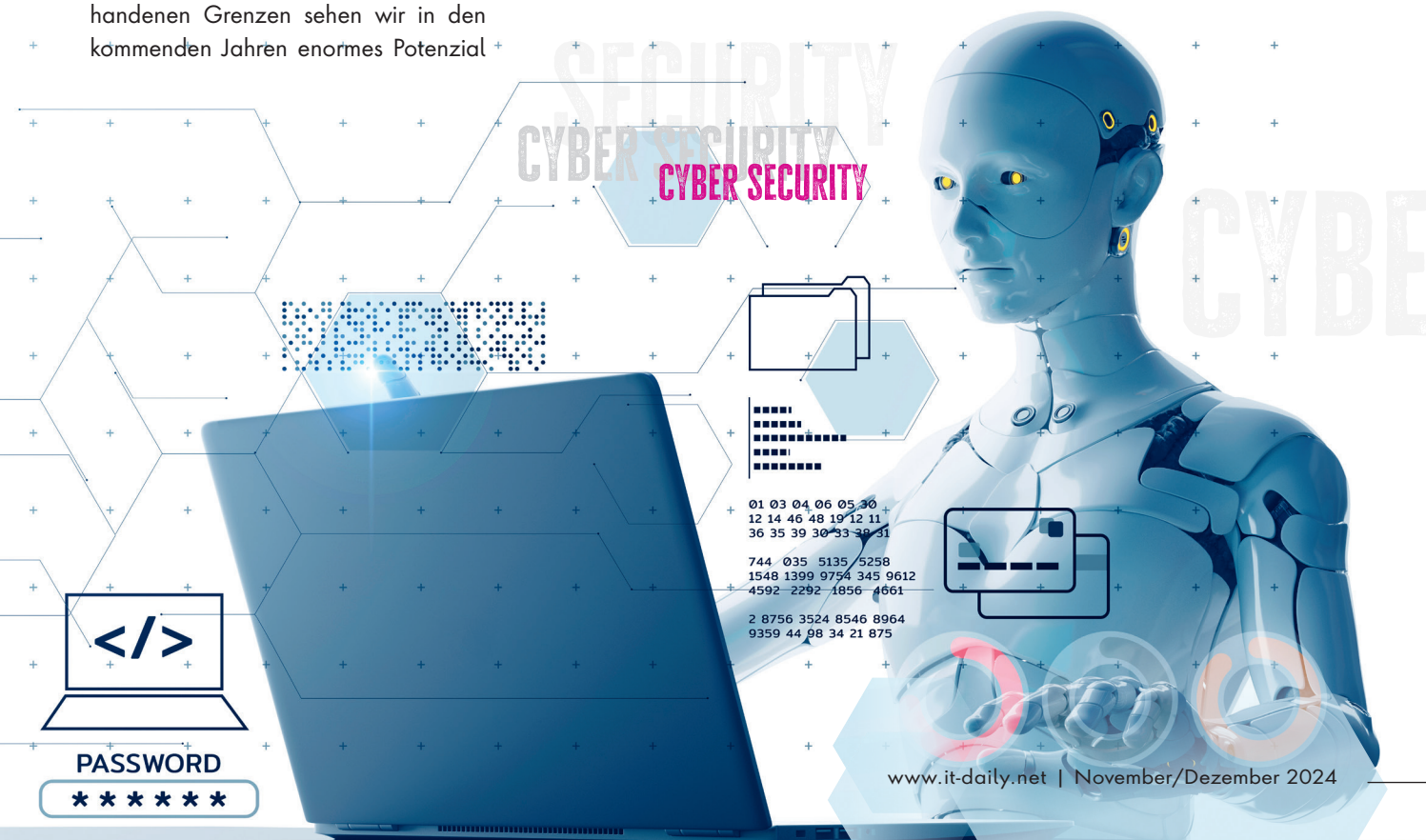
it security: *Aber welches Potenzial sehen sie in Zukunft für die Cyberabwehr mit KI-Unterstützung?*

Jens Schmidt-Sceery: Trotz der eben beschriebenen und aktuell noch vorhandenen Grenzen sehen wir in den kommenden Jahren enormes Potenzial für KI in der Cyberabwehr. Zurzeit arbeiten viele Cybersecurity-Unternehmen bei etlichen Schritten noch manuell. Sicherheitsteams sind oft noch für das Aufspüren und die Analyse von Bedrohungen zuständig. Sie müssen Warnmeldungen und potenzielle Vorfälle händisch überprüfen und analysieren, um einen falschen Alarm auszuschließen und echten Bedrohungen herauszufiltern. Das ist sehr zeitraubend. Auch das Reagieren auf Cyberangriffe erfordert manuelle Schritte, etwa das Scannen und die Quarantäne attackierter Systeme sowie das Sammeln von Daten. Nach einem Angriff wird zudem eine umfangreiche Untersuchung nötig, um die Schwachstellen zu finden und die Schadenshöhe zu bestimmen. Auch die regelmäßigen Sicherheitschecks der IT-Infrastruktur oder Audits werden heute oft noch manuell durchgeführt.

it security: *Welche Einsparungen sind durch den KI-Einsatz im Bereich Cybersecurity aus ihrer Sicht möglich?*

> NACH UNSERER EINSCHÄTZUNG DÜRFTE ES NOCH EINIGE ZEIT IN ANSPRUCH NEHMEN, BIS EINE KI „OUTSIDE-THE-BOX" DENKEN KANN.
>
> **Dr. Jens Schmidt-Sceery, Partner, Pava Partners, https://pava.eu/**

Frank Brandenburg: Wenn jeder der von Herrn Schmidt-Sceery eben beschriebenen Schritte durch KI optimiert wird, können Ressourcen im hohen zweistelligen Prozentbereich einge-



spart werden. Und es gibt noch einige weitere Vorteile: Durch Einsatz von KI können reale Bedrohungen präziser erkannt und falsche Alarme deutlich reduziert werden. So sparen Sicherheitsteams viel Zeit für die Analyse von Warnmeldungen und unnötigen Alarmen. Mithilfe der KI können außerdem eine 24/7 Überwachung der Systeme realisiert und Sicherheitslücken in Echtzeit identifiziert werden. Eine solche proaktive Überwachung entlastet Cybersecurity-Verantwortliche in den Unternehmen von manuellen Audits und Überprüfungen.

it security: *Wie sehen Sie die Chancen, dass die Abwehr von Cyberangriffen irgendwann komplett in die „Hände" einer KI übergeben werden kann?*

Jens Schmidt-Sceery: Eine „echte" KI, im Sinne der vorhin gegebenen Beschreibung, bietet eine Vielzahl von Einsatzmöglichkeiten, die über die von aktuellen ML-Anwendungen weit hinaus geht. Wir sehen aber nicht, dass die Cyberabwehr in absehbarer Zeit komplett an eine KI übergeben werden kann. Einige Bereiche der Cyberabwehr werden auch in Zukunft in Menschenhand bleiben. Nach unserer Einschätzung dürfte es noch einige Zeit in Anspruch nehmen, bis eine KI „outside-the-box" denken kann. Solange wird auch der menschliche Verstand gefragt sein, um auf kreative Angriffe kreativ antworten zu können.

Hinzu kommen strategische und ethische Fragen, die nicht an eine KI übertragen werden sollten.

Schlussendlich bleibt eine effiziente Cyberabwehr jedoch immer auch abhängig von guter Kommunikation zwischen allen relevanten Playern. Dazu gehören andere Sicherheitsteams ebenso wie die unterschiedlichen Geschäftsbereiche, die Geschäftspartnern und Kunden eines Unternehmens. Diese soziale Interaktion wird für KI-Systeme noch lange eine anspruchsvolle Aufgabe bleiben. Das dürfte sich erst ändern, wenn Unternehmen irgendwann nicht mehr von Menschen geführt werden, was wir nicht hoffen wollen.

CYBER SECURITY

it security: *Herr Schmidt-Sceery, Herr Brandenburg, vielen Dank für dieses Gespräch.*

THANK YOU

3. - 5. Dezember 2024
Frankfurt

cyberevolution 2024

Cybersecurity in an AI Powered Digital World

Die Zukunft der digitalen Sicherheit und Identität

500
Experten und Anwender
CEO, CISO's, Entscheidungsträger und Fachexperten aus nationalen und internationalen Unternehmen

120
Redner*innen
aus Cybersicherheit, KI, Datenschutz und Unternehmensberatung

100
Sessions
plus viele Networking-Möglichkeiten

Die digitale Welt entwickelt sich in rasantem Tempo, und mit ihr auch die Herausforderungen und Chancen im Bereich der Cybersecurity und Identity Management.

KuppingerCole präsentiert die cyberevolution 2024, das zentrale Event für alle Fachleute, Innovatoren und Entscheidungsträger aus den Bereichen Cybersecurity, Datenschutz und digitale Identität.

Be part of the experience!

Erleben Sie spannende Keynotes führender Experten, interaktive Workshops und Networking-Möglichkeiten mit den renommiertesten Köpfen der Branche. Die cyberevolution 2024 bietet Ihnen tiefgreifende Einblicke in die neuesten technologischen Entwicklungen und Trends wie Zero Trust, künstliche Intelligenz, Dezentralisierung und mehr.

Nutzen Sie diese einzigartige Gelegenheit, um sich mit anderen Fachleuten auszutauschen, Ihre Cybersecurity-Strategien zu optimieren und die Zukunft der digitalen Welt aktiv mitzugestalten.

Seien Sie dabei und sichern Sie sich jetzt Ihr kostenfreies Ticket unter:
kuppingercole.com/cyberevolution2024

Modernes Bot-Management

SCHRITT HALTEN MIT AUTOMATISIERTEN BEDROHUNGEN

Mit der fortschreitenden Automatisierung des Internets verändern sowohl nützliche als auch bösartige Bots die Sicherheitslandschaft für Webanwendungen und APIs. Denn einerseits sind die technischen (und finanziellen) Hürden für fortschrittliche Bot-Angriffe gesunken, wodurch mehr Angreifer Dienste stören, Daten stehlen oder den Ruf von Unternehmen schädigen können. Andererseits werden Bots durch KI und Machine Learning immer intelligenter und damit besser darin, bestehende Abwehrmechanismen zu umgehen. Unternehmen stehen nun vor der dringenden Frage: Wie können sie ihre Netzwerke schützen, während Bot-Angriffe immer ausgefeilter werden?

Evolution der Bots

Die Integration von KI und maschinellem Lernen in die Entwicklung schädlicher Bots stellt Unternehmen vor immer größere Herausforderungen. Angreifer können nicht nur schneller mehr Bots erstellen und damit Wellen automatisierter Angriffe starten. Diese Bots - verantwortlich für Aktivitäten wie DDoS-Angriffe, Credential Stuffing oder Datenexfiltration - sind zudem zunehmend in der Lage, menschliches Verhalten zu imitieren und so herkömmliche Abwehrmechanismen zu umgehen. Früher reichte es aus, verdächtigen Datenverkehr durch IP-Adressen oder User-Agent-Strings zu identifizieren und zu blockieren. Doch diese Ansätze sind überholt. Methoden wie IP-Spoofing oder die Nutzung von Proxys verschleiern ihre Herkunft und machen das Blockieren basierend auf IP-Adressen unwirksam. CAPTCHAs, einst eine effektive Barriere, können nun ebenfalls von modernen Bots überwunden werden.

Die Grenze zwischen legitimen Nutzern und Bots verschwimmt zunehmend, wodurch False Positives häufiger auftreten können. Dies führt zu einer negativen User Experience und Frustration bei legitimen Nutzern. Die eigentliche Herausforderung besteht also darin, zwischen legitimem und bösartigem automatisiertem Datenverkehr zu unterscheiden. Diese Unterscheidung wird noch schwieriger, wenn es um die Grauzone zwischen eindeutig guten und eindeutig bösen Bots geht. Eine falsche Identifizierung oder Blockierung von nützlichen

Bots kann den Partnerverkehr, die Integration von Drittanbietern und letztendlich die Einnahmen eines Unternehmens beeinträchtigen. Der Schlüssel zur Bewältigung dieses Dilemmas liegt in der Transparenz, das heißt, wie viel Einblick man in die Daten bekommt. Sicherheitsteams müssen über die nötigen Tools verfügen, um Verkehrsmuster genau zu überwachen, Anomalien zu erkennen und fundierte Entscheidungen darüber zu treffen, welche Bots zu blockieren und welche zuzulassen sind.

Was Unternehmen jetzt tun sollten

Viele ältere Sicherheitslösungen, die vor dem Aufkommen moderner automatisierter Bedrohungen entwickelt wurden, reichen heute nicht mehr aus. Unternehmen müssen über diese traditionellen Abwehrmechanismen hinausdenken und anpassungsfähige Sicherheitslösungen implementieren.

#1 Verhaltensbasierte Erkennung:
Unternehmen sollten in Systeme investieren, die das Verhalten von Nutzern und Bots in Echtzeit analysieren.

#2 Dynamische Bot-Management-Lösungen:
Machine-Learning-gestützte Ansätze passen sich an neue Bedrohungen an und verbessern ihre Erkennungsfähigkeit.

#3 Multi-Layer-Sicherheit:
Eine Kombination verschiedener Sicherheitslösungen wie Verhaltensanalysen und Challenge-Response-Mechanismen ist notwendig.

#4 Datenschutz und Benutzerfreundlichkeit im Fokus: Zu viele Sicherheitsprüfungen frustrieren Nutzer. Lösungen wie Private Access Tokens (PATs) bieten Sicherheit, ohne die Benutzererfahrung zu beeinträchtigen.

Investitionen in Lösungen der nächsten Generation, wie zum Beispiel fortschrittliche Web Application Firewalls (WAFs) und intelligente Bot-Management-Tools, sind mittlerweile für die automatische Erkennung und Eindämmung von Angriffen unerlässlich. Diese Lösungen sind zunehmend in vernetzte Threat-Intelligence-Plattformen integriert, die Echtzeit-Datenüberwachung und KI-gestützte Analysen kombinieren. Gleichzeitig verringern sie die Notwendigkeit von manuellem Eingreifen, was es den Sicherheitsteams ermöglicht, sich auf Aufgaben mit höherer Priorität zu konzentrieren, wodurch wertvolle Ressourcen für Innovation und Produktentwicklung frei werden.

Ständige Anpassung als Schlüssel zum Erfolg

In einer Welt, in der Bot-Angriffe immer ausgefeilter werden, dürfen Unternehmen nicht auf traditionelle Sicherheitsmechanismen allein vertrauen. Modernes Bot-Management muss proaktiv, dynamisch, lern- und anpassungsfähig sein, um der sich stetig verändernden Bedrohungslage gerecht zu werden. Es gilt, die richtigen Technologien und Ansätze zu wählen, die nicht nur bösartige Bots abwehren, sondern gleichzeitig die Nutzererfahrung optimieren. Nur so können Unternehmen ihre Netzwerke und Anwendungen langfristig sicher und benutzerfreundlich gestalten.

Goodwill N'Dulor

IN EINER WELT, IN DER BOT-ANGRIFFE IMMER AUSGEFEILTER WERDEN, DÜRFEN UNTERNEHMEN NICHT ALLEIN AUF TRADITIONELLE SICHERHEITSMECHANISMEN VERTRAUEN.

Goodwill N'Dulor,
Senior Security Strategist EMEA, Fastly,
www.fastly.com/de

Massive Angriffe aus Russland

LIDL-MUTTERKONZERN: „WERDEN 350.000-MAL AM TAG ATTACKIERT"

(Quelle: www.sueddeutsche.de; „KI ist die Grundlage für den Wohlstand künftiger Generationen"; 06.10.2024)

Die Schwarz Gruppe, Mutterkonzern der bekannten Einzelhandelsketten Lidl und Kaufland sieht sich nach eigenen Angaben mit einer Flut von bis zu 350.000 Cyberattacken täglich konfrontiert.

Gerd Chrzanowski, Chef der Schwarz Gruppe, nannte diese Zahlen in einem Gespräch mit der Süddeutschen Zeitung. „Wir als Schwarz-Gruppe hatten etwa 3500 Angriffe täglich vor dem Ukraine-Krieg. Jetzt werden wir 350.000-mal am Tag attackiert, vor allem aus Russland", sagte Chrzanowski.

Um dieser Bedrohung zu begegnen, habe die Schwarz Gruppe eine umfassende Strategie entwickelt. Das Unternehmen setzt dabei auf die Entwicklung eigener KI-basierter Sicherheitslösungen in Zusammenarbeit mit dem US-amerikanischen Unternehmen ServiceNow. Diese Software soll nicht nur dem eigenen Schutz dienen, sondern auch anderen Unternehmen im Einzelhandel zur Verfügung gestellt werden: „Wir konkurrieren bei Eiern, Bananen und Milch. Aber nicht bei Cybersecurity. Hier müssen wir zusammenarbeiten. Wenn einer von uns attackiert wird, trifft uns das alle", sagte Chrzanowski.

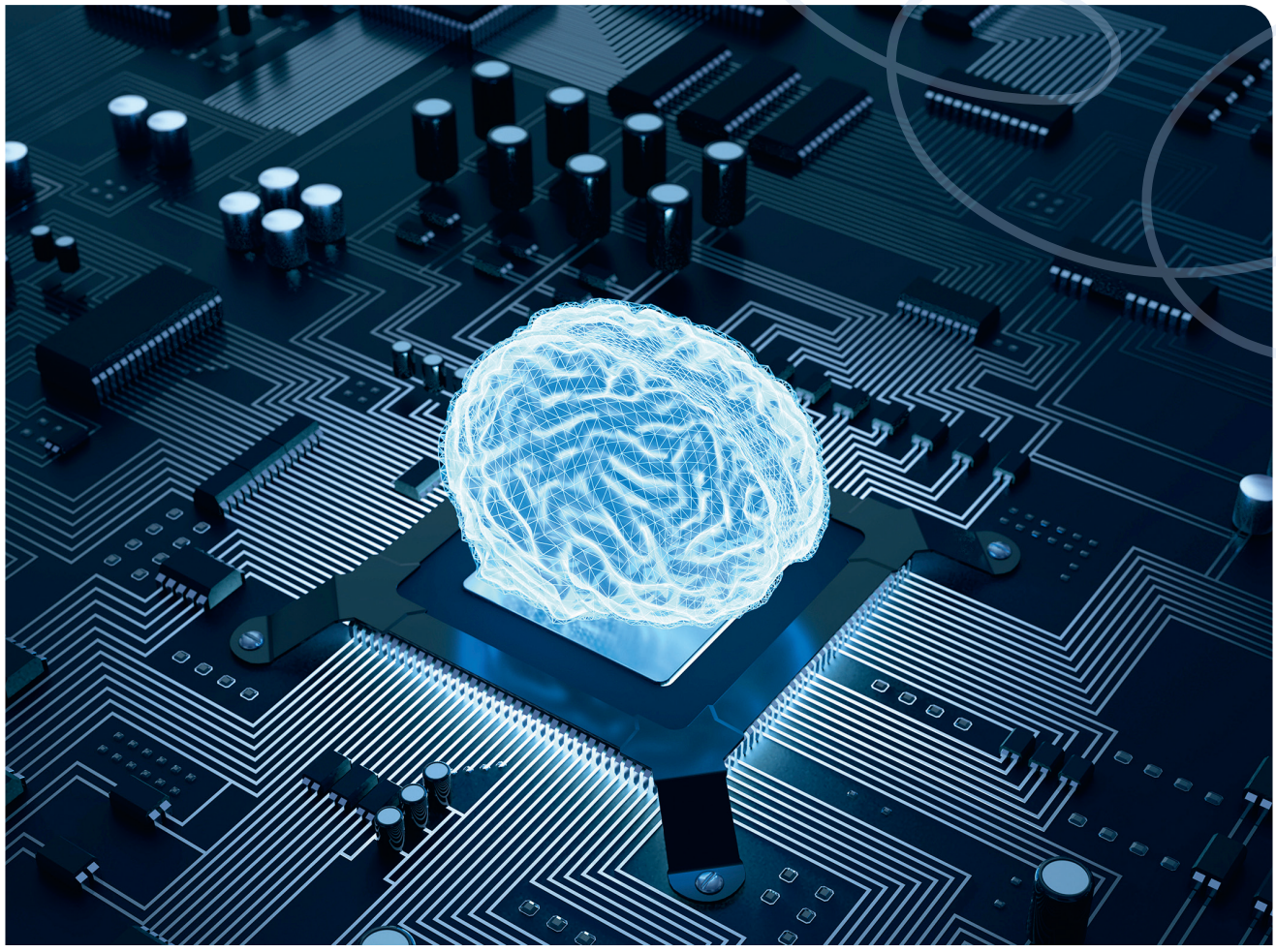
Lars Becker | www.it-daily.net

KI-Server: Haben oder nicht haben?

WANN ES FÜR UNTERNEHMEN SINN MACHT, IN EIGENE KI-SERVER ZU INVESTIEREN

KI entwickelt sich zu einer allgegenwärtigen Technologie, die Hochleistungsserver erfordert, die speziell für KI-Training und Inferencing entwickelt wurden. Unternehmen stehen vor der Frage, ob sie die Angebote von KI-Cloudanbietern nutzen sollen, um Zugang zu KI-Training und -Inferencing zu erhalten, oder ob sie besser in eigene KI-Server investieren sollten. Hierbei müssen mehrere Faktoren bedacht werden, die es Unternehmen ermöglichen, eine optimale Wahl zu treffen und die Rentabilität unter dem Gesichtspunkt der Implementierung und der Kosten zu maximieren.

Da das Training von KI-Modellen auf vorhandenen Daten basiert, muss sich dieser Prozess in einem Unternehmen auf Unternehmensdaten stützen. Viele dieser Daten sind möglicherweise für das Unternehmen von großer Wichtigkeit, entsprechend vertraulich und hinter einer Firewall mit spezifischen Berechtigungen gesichert. Die Implementierung eines KI-Trainingssystems mit Unternehmensdaten in einem On Premises-Rechenzentrum ist daher oft sinnvoll. Ein Unternehmen hat möglicher-



weise strengere Anforderungen an seine Daten als ein KI-Cloudanbieter und verfügt über andere oder maßgeschneiderte Cybersicherheitsmaßnahmen.

Datensouveränität

In vielen Branchen können Daten nur an bestimmten geografischen Standorten gespeichert werden. Wenn Daten vor Ort gespeichert werden, hat man die volle Kontrolle darüber, wo die Daten aufbewahrt und archiviert werden. Bei der Nutzung von KI-Cloudanbietern, wo Daten hochgeladen werden müssen, gibt es möglicherweise keine Garantie, dass die Daten an dem angegebenen Ort aufbewahrt werden, insbesondere wenn Cloud-basierte Backups in Betracht gezogen werden.

Es gibt viele GPU-Optionen, die von verschiedenen Serveranbietern angeboten werden. Für einige Workloads in der KI-Pipeline sind GPUs möglicherweise gar nicht erforderlich. Die neuesten CPUs verfügen über eine erhebliche KI-Verarbeitungsleistung auf der CPU selbst, was zu einer akzeptablen Leistung und niedrigeren Kosten für die Server führen kann. Darüber hinaus können Unternehmen möglicherweise die neuesten KI-Beschleuniger vom Anbieter erwerben und in ihre IT-Umgebung integrieren, bevor ein Cloudanbieter dazu in der Lage ist.

Die Wahl der richtigen Server

Die Anschaffung von GPU-Servern kann korrekt budgetiert werden, und die Betriebskosten können sehr genau geschätzt werden. Umgekehrt kann die Nutzung einer Reihe von Servern bei einem KI-Cloudanbieter zu unvorhersehbaren Rechnungen führen. Die Datenmenge, die in die Cloud gesendet und aus der Cloud zurückgeschickt werden muss, kann die Kosten erheblich in die Höhe treiben. Auch die Reservierung von GPU-Instanzen, ohne sie zu nutzen, kann die Kosten in die Höhe treiben.

Auf dem Markt sind heute viele verschiedene Arten von KI-Servern erhältlich. Die spezifisch benötigte Konfiguration und Leistung eines KI-Servers ist möglicherweise aber nicht bei einem KI-Cloudanbieter verfügbar. Die Anschaffung von KI-Servern, die für die benötigte Art von Training oder Inferencing-Workflows konfiguriert sind und den spezifischen Anforderungen eines Unternehmens entsprechen, kann die Gesamtkosten senken.

Es gibt zwar verschiedene Methoden zur Schätzung der Kosten für das Training eines KI-Modells einer bestimmten Größe und Anzahl benötigter GPUs, aber viele KI-Modelle müssen ständig mit neuen Parametern trainiert werden. Um die Genauigkeit der Schlussfolgerungen zu gewährleisten, muss das KI-Modell mit aktualisierten und neueren Daten neu trainiert werden, was je nach der Menge der verwendeten neuen Daten genauso lange dauern kann wie das ursprüngliche Training. In einem On Premise-Rechenzentrum können die Systeme wiederholt verwendet werden, während in der öffentlichen Cloud die Kosten mit jeder Iteration und Neutrainierung des KI-Modells ansteigen.

Fundierte Entscheidungsfindung

Die Cloud ist zwar dafür bekannt, dass sie eine erhebliche Skalierung von Anwendungen ermöglicht, aber die angeforderten Server sind möglicherweise nicht immer verfügbar. Mit der Investition in eigene KI-Server können Unternehmen die eigenen Skalierungsrichtlinien umsetzen, ohne mit einem Drittanbieter verhandeln zu müssen und möglicherweise mehr für ungenutzte Reservierungen zu zahlen.

Es gibt eine Reihe von Herstellern, die KI-Server anbieten, was den Einkauf günstiger macht. Wenn zudem KI-Server verschiedener Anbieter mit derselben Software zertifiziert sind, ist ein Wechsel von einem Anbieter zum anderen möglich. Der Wechsel von einer Cloud in eine andere ist komplexer und zeitaufwändiger.

> MIT DER INVESTITION IN EIGENE KI-SERVER KÖNNEN UNTERNEHMEN DIE EIGENEN SKALIERUNGSRICHTLINIEN UMSETZEN, OHNE MIT EINEM DRITTANBIETER VERHANDELN ZU MÜSSEN.
>
> **Michael McNerney, Vice President Marketing & Network Security, Supermicro, www.supermicro.com/de**

Bei der Entwicklung einer effizienten und effektiven KI-Trainingslösung sind viele Softwareoptionen zu berücksichtigen. Ein öffentlicher, gemeinsam genutzter Cloud-Anbieter verfügt möglicherweise nicht über alle verfügbaren Komponenten, was zusätzliche Einstellungen und Tests für jede in einer öffentlichen Cloud-Infrastruktur erworbene Instanz erforderlich machen kann.

Eigene KI-Server können passgenau und kostengünstig konfiguriert werden, um den Anforderungen des Unternehmens gerecht zu werden. Das Verständnis der Workloads, der Datenmenge, der Feinabstimmung des KI-Workflows und der internen Expertise mit verschiedenen Softwareschichten hilft dabei, die beste Option für ein Unternehmen zu bestimmen.

Michael McNerney

Drei Säulen für bestmögliche Cybersicherheit

UNTERNEHMEN AUF HÖCHSTMÖGLICHEM NIVEAU SCHÜTZEN

Schon die alten Römer wussten um die Wichtigkeit von „Usus facit magistrum". Dass Übung den Meister macht, gilt bis heute – auch oder gerade in der hoch digitalisierten Wirtschaft. Dieser Grundsatz gilt gleichsam für die IT-Sicherheit. Weshalb? Weil die Security trotz der weit gediehenen automatischen Erkennung von Angriffsversuchen und Malware aufgrund der Raffinesse der Cyberkriminellen auch das Know-how und die Erfahrung des Menschen braucht – spätestens dann, wenn es darum geht, Angriffsmuster zu erkennen, die die Technologie noch nicht identifizieren kann oder bei der Reaktion und Bewältigung von Cyberangriffen. Dieser menschliche Teil in der Kette der Cyberbekämpfung und -abwehr sollte mit den automatischen Prozessen der Security koordiniert und erprobt sein.

EIN INTEGRIERTES SECURITY-ÖKOSYSTEM IN KOMBINATION MIT GEZIELTEM TRAINING UND SECURITY-DIENSTLEISTUNGEN SCHÜTZT UNTERNEHMEN AUF HÖCHSTMÖGLICHEM NIVEAU.

Michael Veit, Security-Experte, Sophos, www.sophos.de

Security-Ökosystem entlastet IT-Teams

In einer Umfrage, die Sophos gemeinsam mit dem Analystenhaus Techconsult im Juni 2024 durchgeführt hat, wurden IT-Verantwortliche bezüglich der Reaktion in Unternehmen im Falle einer Cyberattacke und wie gut sie darauf vorbereitet sind befragt. Durchschnittlich 43 Prozent der Befragten bejahen die Frage, ob es Cybersecurity-Vorfälle gab, die vom System zwar gemeldet, jedoch nicht wahrgenommen oder bearbeitet wurden.

Dieses Drama liegt nicht an schlechten Sicherheits-Lösungen oder am Unvermögen von IT-Administratoren. Vielmehr ist eine der ausschlaggebenden Ursachen eine ungenügend integrierte IT-Security. Nicht wenige Unternehmen verfolgen den Best-of-Breed-Ansatz, bei dem im Netzwerk, in der Cloud und an den einzelnen Endpoints das jeweils vermeintlich beste Sicherheitsprodukt zum Einsatz kommt. In einer Wirtschaft, in der alle Unternehmen auf eine stark verteilte und fragmentierte IT-Infrastruktur setzen, führen viele einzelne Sicherheitslösungen zu einem großen Security-Flickenteppich, der von Lücken geprägt und von Administratoren kaum beherrschbar ist.

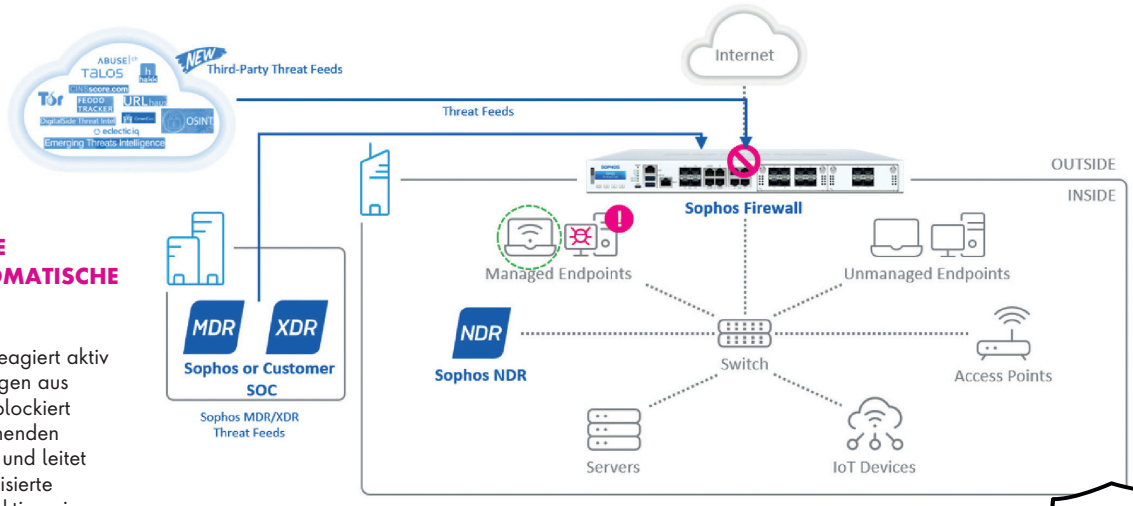
Ein integriertes Sicherheits-Ökosystem hingegen führt alle Facetten der Security, von Endpoints, Server, Mobilgeräte über Public Cloud, Firewall, E-Mails, Wireless, WAF bis hin zu Zero Trust Network Access mit Künstlicher Intelligenz (KI) sowie der stetigen Einbeziehung von menschlichen Experten und Expertinnen für das schnelle Handeln unter einem Schutzschirm zusammen. Es eliminiert das ineffiziente Abstimmen und Betreiben einzelner Security-Lösungen und schafft mit einer intelligenten Vernetzung und einem hohen Grad an automatischer Reaktion ein hohes Sicherheitslevel. Ein solches Ökosystem ist im Vergleich zum Flickenteppich zentral und einfach steuerbar. An einer zentralen Konsole wird die gesamte IT-Security-Infrastruktur gesteuert und auf Warnungen reagiert. Damit lassen sich die 43 Prozent der Unternehmen, die einen gemeldeten Cybervorfall nicht wahrgenommen und behoben haben, drastisch reduzieren.

Denn sie wissen, was sie tun

Alles der technologischen Reaktionsfähigkeit zu überlassen, ist in der Security zu kurz gedacht. Auch ein ausgeklügeltes Security-Ökosystem mit weitreichen-

SOFORTIGE UND AUTOMATISCHE REAKTION

Die Firewall reagiert aktiv auf Bedrohungen aus allen Feeds, blockiert den entsprechenden Datenverkehr und leitet eine synchronisierte Sicherheitsreaktion ein.



Quelle: Sophos

der Automation und ausgeprägter Einbindung von KI benötigt ab einer bestimmten Ereigniseskalation den menschlichen Verstand und das gezielte Handeln – gelegentlich auch mit Intuition. Um dies in der IT-Administration sowie im gesamten Unternehmen zu verankern, eignen sich Tabletop-Übungen, bei denen schrittweise alle Beteiligten involviert werden. Tabletop-Übungen haben sich in vielen Bereichen bewährt, etwa beim Militär, beim politischen oder wirtschaftlichen Krisenmanagement und eben auch in IT-Security-Bereich. Bei einer Tabletop-Übung wird ein Cyberangriff realitätsnah in unterschiedlichen Abteilungen des Unternehmens durchgespielt und anschließend die Cyber-Resilienz inklusive möglicher Schäden analysiert. Im Nachgang erkennen alle Beteiligten, inwieweit sie für den Ernstfall gewappnet sind und ob das Unternehmen insgesamt in der Lage ist, auf einen Angriff gezielt und effizient zu reagieren. Die Übungen geben wichtige Einblicke in den Status der Cybersecurity – darunter das Erkennen von blinden Flecken, die Fähigkeit der Kommunikation im Ernstfall, die Einhaltung der Compliance oder die Reaktionsfähigkeit.

Bei den Tabletop-Übungen haben sich drei Szenarien etabliert: An erster Stelle stehen die Rapid-Fire-Szenarien. Hierfür sind keine oder nur wenige Vorbereitungen nötig. An Rapid-Fire-Szenarien nehmen Mitarbeiter – sowohl in nichtleitender als auch mittlerer und leitender Funktion – aus unterschiedlichen Abteilungen teil. Dabei spielen die Teilnehmer unterschiedliche Sicherheitsszenarien durch und schlüpfen jeweils in die Rolle eines Incident-Responders (Störfall-Experten).

Im Gegensatz zu den Rapid-Fire-Szenarien liegt bei den rein technischen Szenarien der Schwerpunkt auf den für die Security spezifischen Aspekten. Diese Szenarien werden minutiös geplant, sodass die Teams die entsprechenden Einflussfaktoren eines Sicherheitsvorfalls analysieren können. Meist gehen rein technische Szenarien von einem Kernereignis aus und ermöglichen es IT-Teams, sich auf komplexe Cyberangriffe vorbereiten.

Die dritte Form der Szenarien findet mit allen Stakeholdern statt, darunter technische Teams sowie Vertreter der Rechts-, Marketing- und Personalabteilung oder das Management. Diese Szenarien bieten sich insbesondere für Unternehmen und Organisationen an, um die abteilungsübergreifende Kommunikation im Falle einer Cyberattacke zu verbessern.

Ein integriertes Sicherheits-Ökosystem und die Übung im Umgang mit Cybervorfällen löst bereits einen Großteil der Probleme, die viele Unternehmen bei Cyberattacken heute noch haben. Es löst aber nicht den Teil, den selbst die hochentwickelten technischen Lösungen inklusive KI nicht erkennen oder lösen können. Dann werden Spezialisten benötigt. Externe Services, wie beispielsweise Managed Detection and Response (MDR), helfen gezielt, ohne dass das Unternehmen die nötige Kompetenz inhouse vorhalten und fortwährend schulen muss. Durch MDR haben Unternehmen die Möglichkeit, Sicherheitsvorgänge und Reaktionen auf Gefahren je nach Bedarf und umgehend zu skalieren. Darüber hinaus helfen weitere Services wie Echtzeit-Incident-Response (IR)-Dienste solchen Unternehmen, die aktiv angegriffen werden und sofortige Hilfe bei der Neutralisierung von Angreifern benötigen.

Mit der Kombination aus einem Security-Ökosystem, einem gezielten Training und den Dienstleistungen für die rund um die Uhr verfügbare Erkennung, Untersuchung und Reaktion auf Bedrohungen komplettieren Unternehmen ihren Schutz individuell und auf dem höchstmöglichen Niveau.

Michael Veit

Cybersicherheit im Wandel

PLATTFORMLÖSUNGEN ALS ZUKUNFTSMODELL

Die digitale Transformation verändert die IT-Landschaft in rasantem Tempo. Technologien wie Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS) und generative künstliche Intelligenz (KI) prägen zunehmend die IT-Strukturen von Unternehmen. Gleichzeitig kämpfen viele Organisationen mit einem akuten Fachkräftemangel im Bereich der Cybersicherheit. Die Rekrutierung und Bindung qualifizierter Experten gestalten sich schwierig, obwohl der Bedarf stetig wächst. Hinzu kommt, dass die Zahl der auf dem Markt erhältlichen Sicherheitslösungen steigt, was zu höheren Verwaltungskosten und einer fragmentierten Sicherheitslandschaft führt.

In Reaktion auf diese Herausforderungen vollzieht sich in der Branche ein deutlicher Wandel: Unternehmen wenden sich von isolierten Sicherheitslösungen ab und setzen verstärkt auf integrierte Plattformansätze. Dieser Trend zur Plattformisierung verspricht, viele der aktuellen Probleme effektiv anzugehen.

Die Vorteile integrierter Sicherheitsplattformen

Im Vergleich zu traditionellen Einzellösungen bieten integrierte Plattformansätze mehrere entscheidende Vorteile. An erster Stelle steht die Verbesserung der Sicherheitsergebnisse: Durch die Zusammenführung mehrerer Sicherheitsfunktionen in einer einheitlichen Umgebung werden potenzielle Schwachstellen, die bei der Verwendung von Einzelprodukten entstehen können, effektiv geschlossen. Das ist besonders wichtig, da moderne Cyberangriffe oft mehrere Schwachstellen gleichzeitig ausnutzen und dabei immer häufiger auf KI und insbesondere maschinelles Lernen zurückgreifen.

Darüber hinaus bringen integrierte Plattformen auch wirtschaftliche Vorteile. Sie vereinfachen den Auswahlprozess und die Implementierung von Sicherheitslösungen erheblich, da Unternehmen nicht mehr eine Vielzahl von Einzelprodukten evaluieren und integrieren müssen. Dies beschleunigt die Entscheidungsfindung und ermöglicht eine schnellere Einführung neuer Sicherheitsmaßnahmen. Langfristig führt die Konsolidierung der Sicherheitsfunktionen auf einer einzigen Plattform zu einer deutlichen Senkung der Betriebskosten.

LANGFRISTIG FÜHRT DIE KONSOLIDIERUNG DER SICHERHEITS-FUNKTIONEN AUF EINER EINZIGEN PLATTFORM ZU EINER DEUTLICHEN SENKUNG DER BETRIEBSKOSTEN.

Arnd Gille, Senior Manager Solutions Consulting, Palo Alto Networks, www.paloaltonetworks.de

Praxisbeispiel: M&A-Prozesse

Ein Beispiel für den Nutzen integrierter Sicherheitsplattformen zeigt sich im Bereich Mergers & Acquisitions (M&A). Die Kombination einer Netzwerksicherheitsplattform mit einem Enterprise Identity and Access Management (IAM) Anbieter ermöglicht IT-Teams, Identitäts- und Nutzerkontrollen effizient in Sicherheitsrichtlinien umzusetzen. Dieser ganzheitliche Ansatz erleichtert es, die IT-Sicherheitsinfrastruktur schnell an die sich ständig wandelnden Anforderungen an die Cybersicherheit anzupassen und ermöglicht gleichzeitig Kosteneinsparungen.

Fazit: Plattformisierung als Modell der Zukunft

Angesichts der zunehmenden Komplexität der IT-Landschaft und der Herausforderungen im Bereich Cybersicherheit wird die Konsolidierung von Sicherheitslösungen auf einer Plattform zur zwingenden Notwendigkeit. Unternehmen, die sich für eine integrierte Cybersicherheitsplattform entscheiden, profitieren nicht nur von besseren Sicherheitsergebnissen, sondern auch von erheblichen wirtschaftlichen Vorteilen. Durch die Vereinfachung von Beschaffungsprozessen, die Senkung von Betriebskosten und die Beschleunigung kritischer Integrationsprozesse wie Fusionen und Übernahmen ist die Plattformisierung ein zukunftsweisender Ansatz für die Cybersicherheit.

Arnd Gille

Effizienz und IT-Sicherheit

DER UNVERMEIDLICHE BALANCEAKT

IT-SICHERHEIT MUSS TROTZ DER KOMPLEXITÄT DER RAHMENBEDINGUNGEN EINFACH UND SCHNELL VERFÜGBAR SEIN.

Andreas Fuchs, Director Product Management, DriveLock SE, www.drivelock.com

Wenn Kollegen oder Kolleginnen die Sicherheitsrichtlinien ignorieren oder umgehen, müssen sich IT-Sicherheitsverantwortliche die Frage stellen: Wie sehr schränken Sicherheitsmaßnahmen die Produktivität des Unternehmens ein? Denn der wichtigste Grund, warum Sicherheitsvorgaben nicht beachtet werden, ist der Wunsch, eine Aufgabe schneller, einfacher, effektiver zu erledigen. IT-Sicherheit ist also stets ein Balanceakt zwischen Restriktion und Freiheit. Anders gesagt: IT-Sicherheit darf nicht nerven.

Wie gelingt es IT-Sicherheitsabteilungen, diesen Balanceakt erfolgreich zu managen?

Zero Trust als Kernstrategie

Ein wirksames Sicherheitskonzept basiert auf dem Zero Trust Prinzip „Never Trust, Always Verify". Damit haben Mitarbeitende die Freiheit, von jedem Ort und Gerät aus zu arbeiten, vorausgesetzt, sie authentifizieren sich ordnungsgemäß. Das Prinzip des „Least Privilege Access" stellt sicher, dass Benutzer nur auf die Informationen zugreifen können, die sie wirklich benötigen. Zero Trust reduziert zudem die Anzahl der Passwörter und unterstützt passwortlose Authentifizierungsmethoden.

Sichere Anwendungen: Effizienz ohne Kompromisse

Kostenlose Anwendungen wie Produktivitäts- und Notiz-Apps, Messaging-Dienste und Grafik-Tools versprechen schnelles und effizientes Arbeiten. Doch unautorisierte Applikationen können Sicherheitslücken, Datenlecks oder Malware verursachen.

Eine Applikationskontrolle verhindert die Ausführung unbekannter und nicht autorisierter Anwendungen. Das Blockieren unsicherer Anwendungen sensibilisiert Nutzer zudem für potenzielle Gefahren. Flexible, kontextbasierte Zugriffsrechte sowie detaillierte Protokollierungen und Echtzeitanalysen helfen, ungewöhnliche Aktivitäten frühzeitig zu erkennen und zu unterbinden.

Schnittstellenkontrolle: Ein unverzichtbares Element

Mobile Datenträger wie USB-Sticks und Smartphones sind aus dem Arbeitsalltag kaum wegzudenken, bergen jedoch erhebliche Risiken. Externe Geräte können als Einfallstor für Malware dienen oder zum unautorisierten Export sensibler Daten missbraucht werden. Eine effektive Schnittstellenkontrolle ist daher unverzichtbar. Sie beschränkt den Zugriff auf autorisierte Geräte, überwacht alle Datenübertragungen in Echtzeit und ermöglicht schnelles Handeln bei verdächtigen Aktionen.

Daten können verpflichtend verschlüsselt werden, um das Risiko von Datenlecks weiter zu minimieren.

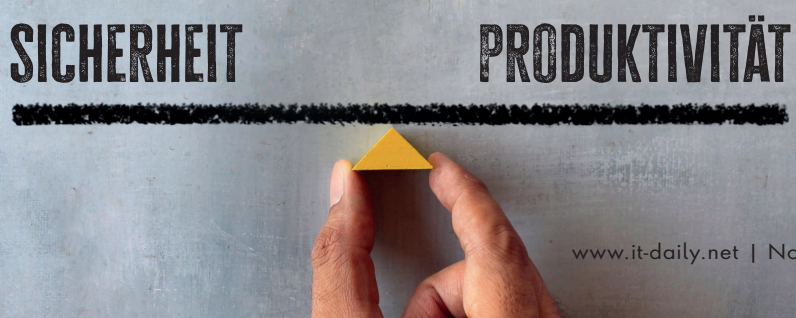
Fazit: Sicherheit und Produktivität Hand in Hand

Ein modernes IT-Sicherheitskonzept muss hohen Ansprüchen gerecht werden. Es muss dafür sorgen, dass die Belegschaft effizient arbeiten kann. Ein effektives Zero-Trust-Sicherheitsmodell hilft, diese Anforderungen zu erfüllen. Es kombiniert Zugangskontrollen mit Benutzerfreundlichkeit und schafft so eine Balance zwischen Sicherheit und Anwenderzufriedenheit.

Unternehmen sollten darüber hinaus Feedback-Kanäle einrichten, über die Mitarbeitende Probleme mit Sicherheitsmaßnahmen melden können. Solches Feedback ermöglicht die kontinuierliche Verbesserung der Sicherheitsrichtlinien und trägt dazu bei, diese benutzerfreundlicher zu gestalten. Umfragen zur Benutzerzufriedenheit mit den Sicherheitslösungen können zusätzlich die Akzeptanz und Effektivität der implementierten Maßnahmen bewerten.

IT-Sicherheit muss trotz der Komplexität der Rahmenbedingungen einfach und schnell verfügbar sein. Sie soll das sichere digitale Arbeiten ermöglichen und darf der Digitalisierung nicht im Weg stehen.

Andreas Fuchs



Sicherheit in der Software-Lieferkette

DER CYBER RESILIENCE ACT UND SEINE BEDEUTUNG FÜR HERSTELLER UND ANWENDER

Das Cyberresilienzgesetz (Cyber Resilience Act – CRA) soll die Sicherheit in der Lieferkette von Software-Produkten verbessern – und somit die IT-Security von Digitalprodukten. Was bedeutet das konkret für Hersteller, Kunden und Anwender? Wir sprachen mit Michael Barth, Abteilungsleiter Strategy bei genua.

it security: *Wie profitieren Kunden und Verbraucher vom CRA?*

Michael Barth: Der CRA verpflichtet Hersteller, die Cybersicherheit von Produkten, die digitale Elemente enthalten, zu berücksichtigen. Und zwar von Tag 1 der Konzeption und Entwicklung über den gesamten Lebenszyklus eines Produkts. Es verpflichtet Hersteller, Sicherheits-Updates für mindestens fünf Jahre auszuliefern – beziehungsweise für die erwartete Lebenszeit eines Produkts, wenn diese kürzer ist. Das Gesetz fordert also, was wir bei genua – auf einem deutlich höheren Niveau – seit jeher unter Security by Design und Security by Default verstehen und leben.

Wenn Hersteller durch aufwendige Verfahren unter anderem für ihre sicheren Entwicklungsprozesse zertifiziert sind, hilft das Kunden beim Identifizieren und Auswählen sicherer Produkte. Weiterverarbeitende Betriebe müssen zudem nachweisen, ihr Möglichstes für die Cybersicherheit getan zu haben – auch in ihrer Lieferkette. Hier gehen CRA und NIS2 Hand in Hand. Dieses Vorgehen kann die Cybersicherheit verbessern. Davon profitieren letztlich Nutzer in allen Branchen.

it security: *Woran wird man sichere IT-Produkte in Zukunft erkennen?*

Michael Barth: Der CRA definiert Mindestanforderungen in Bezug auf Security by Design für alle Produkte, die digital Daten austauschen und auf dem europäischen Markt verkauft werden sollen. Hersteller, die diese erfüllen, können ihre Hard- und Softwareprodukte mit dem CE-Zeichen versehen.

DER CRA DEFINIERT MINDESTANFORDERUNGEN IN BEZUG AUF SECURITY BY DESIGN FÜR ALLE PRODUKTE, DIE DIGITAL DATEN AUSTAUSCHEN UND AUF DEM EUROPÄISCHEN MARKT VERKAUFT WERDEN SOLLEN.

Michael Barth, Abteilungsleiter Strategy, genua, www.genua.de

Damit nicht genug: Es werden auch höhere Security-Level definiert und in Zukunft europaweit angeglichen. Konkret wird es drei Klassen geben: Nicht kritische, kritische und hochkritische Produkte mit digitalen Elementen. Dabei orientiert sich die EU an den Kriterien der Agentur der Europäischen Union für Cybersicherheit ENISA und den EU Common Criteria, kurz EUCC.

Eine der Folgen wird die einfachere Anerkennung von Zertifizierungen über Landesgrenzen hinweg sein – sofern die Bewertungskriterien vergleichbar sind. Das BSI schließt bereits bilaterale Abkommen mit anderen Ländern für die gegenseitige Anerkennung im Rahmen von Common-Criteria-Zertifizierungen. Dieses Vorgehen wird in Zukunft vereinfacht.

it security: *Inwiefern wird der CRA genua betreffen?*

Michael Barth: genua ist weitreichend zertifiziert, seine IT-Security-Produkte unterliegen regelmäßigen externen Überprüfungen, die auch Anforderungen an den Entwicklungs- und Produktdesign-Prozess haben. Damit können wir im Vergleich zu anderen Anbietern wahrscheinlich bereits zahlreiche

Anforderungen erfüllen. Wir blicken daher entspannt auf den CRA. Für uns erwächst daraus eher ein Wettbewerbsvorteil.

Andererseits wird wohl der Konkurrenzdruck steigen, weil auch andere Anbieter ihre Standards erhöhen müssen. Auf der anderen Seite wird die Vergleichbarkeit auf einem gemeinsamen europäischen Binnenmarkt Absatzchancen erhöhen. Für die Nutzer bedeutet das voraussichtlich: Mehr Auswahl, niedrigere Preise und bessere Qualität, weil sich die Produkte und Zertifizierungen besser vergleichen lassen.

it security: *Gibt es Bereiche, in denen der CRA nicht greift?*

Michael Barth: Ja, die gibt es. Was der CRA zum Beispiel nicht vereinheitlicht, sind die Vorgaben für den Geheimschutz. Das bleibt zurecht Sache der nationalen Regulierungen.

it security: *Birgt der CRA möglicherweise auch Risiken?*

Michael Barth: Besonders bei den im CRA geforderten Software-Stücklisten, kurz SBOMs, muss man hinterfragen, ob sie Anwender nicht in falscher Sicherheit wiegen. Die wenigsten SBOMs werden detailliert alle Informationen enthalten, sondern eher einen Überblick geben. Selbst wenn sehr viele oder sogar alle Details aufgeführt sind, ist immer noch keine Aussage darüber möglich, ob eine Schwachstelle in einer Komponente tatsächlich Auswirkungen auf das eingesetzte Produkt hat. Auf der anderen Seite haben uns IT-Security-Zwischenfälle der letzten Zeit deutlich vor Augen geführt, wie wichtig es ist, auch die eigene Software-Lieferkette genau im Blick zu halten.

Daher sind Zertifizierungen so wichtig: Nutzer gehen damit sicher, dass Produkte genau auf diese Fragen hin abgeklopft wurden und bestmögliche IT-Security bieten.

it security: *Herr Barth, wir danken für dieses Gespräch.*

Passkeys

REVOLUTION DER AUTHENTIFIZIERUNG

Die Ära der Passwörter neigt sich dem Ende zu. Passkeys sind auf dem Vormarsch und bieten eine wegweisende Lösung für sichere und komfortable Benutzerauthentifizierung. Was macht Passkeys so besonders und welche Herausforderungen bringen sie mit sich?

Was Passkeys bieten

Passkeys setzen auf moderne Authentifizierungsmethoden wie biometrische Daten oder lokale PINs. Der Vorteil: Der Nutzer muss sich keine Passwörter mehr merken, und sensible Daten bleiben sicher auf dem jeweiligen Gerät. Das Risiko von Phishing oder Passwortdiebstahl wird so drastisch reduziert.

Besonders im Vergleich zu traditionellen Login-Methoden haben Passkeys klare Vorteile:

- Maximale Sicherheit: Passkeys eliminieren Schwachstellen wie Passwortdiebstahl und Phishing-Angriffe, da keine sensiblen Daten übertragen werden.
- Hohe Benutzerfreundlichkeit: Der umständliche Prozess von SMS-TANs oder Multi-Faktor-Authentifizierung entfällt. Der Login erfolgt schnell und unkompliziert.
- Unabhängigkeit von Drittanbietern: Im Gegensatz zu SMS-TAN oder Hardware-OTP arbeiten Passkeys direkt auf dem Gerät des Nutzers.

CIAM

In der digitalen Welt setzen Unternehmen zunehmend auf CIAM (Customer Identity and Access Management) Lösungen, um den Zugang zu Nutzerkonten zu sichern und eine nahtlose User Experience zu gewährleisten. Passkeys fügen sich ideal in diese übergeordneten CIAM-Strategien ein, die darauf abzielen, Authentifizierung sicherer und gleichzeitig nutzerfreundlicher zu gestalten. Unternehmen können die Identitäten ihrer Kunden so effektiver schützen und gleichzeitig die Einstiegshürden für Nutzer senken.

Herausforderungen

Trotz der vielen Vorteile stehen Unternehmen und Nutzer vor Herausforderungen. Viele Menschen sind an das herkömmliche System aus Benutzername und Passwort gewöhnt. Studien zeigen, dass der vereinfachte Login-Prozess mit Passkeys oft als weniger sicher wahrgenommen wird. Es bedarf umfassender Aufklärung, um das Vertrauen in diese Technologie zu stärken.

Ein weiterer wichtiger Punkt ist die Interoperabilität. Damit Passkeys tatsächlich nahtlos auf allen Geräten und Browsern funktionieren, müssen verschiedene Akteure wie Browserhersteller und Softwareentwickler an einem Strang ziehen. Die gute Nachricht: Industriestandards sorgen für immer mehr Kompatibilität und erleichtern die Einführung.

Passkeys auf dem Vormarsch

Die technologische Entwicklung wird die Funktionalität und Sicherheit von Passkeys in den kommenden Jahren weiter verbessern. Nutzer haben bereits jetzt die Kontrolle über ihre Passkeys und können entscheiden, ob sie Schlüssel synchronisieren oder lokal speichern wollen. In sicherheitssensiblen Bereichen wird es in Zukunft möglich sein, gerätegebundene Schlüssel zu nutzen, die das jeweilige Gerät nie verlassen.

Passkeys sind ein entscheidender Schritt in eine sichere digitale Zukunft. Unternehmen, die diese Technologie frühzeitig in ihre CIAM-Strategien integrieren, werden nicht nur die Sicherheit ihrer Systeme erhöhen, sondern auch die Benutzererfahrung nachhaltig verbessern.

Stephan Schweizer

PASSKEYS SIND EIN ENTSCHEIDENDER SCHRITT IN EINE SICHERE DIGITALE ZUKUNFT.

Stephan Schweizer, CEO, Nevis Security, www.nevis.net/de/

Gemeinsam gegen Cyberangriffe

IT-SICHERHEIT IST TEAMSACHE

Laut einer Studie des Weltwirtschaftsforums sind Cyberangriffe eine der größten globalen Bedrohungen für Unternehmen. Jedes Jahr steigt die Zahl erfolgreicher Attacken, die immer komplexer werden. Trotz erhöhter Investitionen in die IT-Sicherheit schaffen Unternehmen es oft nicht, sich wirksam zu schützen. Das gelingt nur, indem IT-Verantwortliche und Fachabteilungen zusammenarbeiten und gemeinsam Strategien und Schutzmaßnahmen entwickeln.

Sicherheitsbedrohungen haben ein neues, verheerendes Niveau erreicht. Im Ernstfall müssen Organisationen innerhalb von Minuten reagieren, um Gefahren einzudämmen und Sicherheitslücken zu schließen. Was tun gegen die wachsende Gefahr?

Teamwork macht den Unterschied

Der erste Weg führt über den CISO. Er ist für die Entwicklung und Umsetzung der Informationssicherheitsstrategie eines Unternehmens verantwortlich. Zu seinen Aufgaben zählen beispielsweise die Erstellung und Pflege von Sicherheitsrichtlinien sowie das Risikomanagement mitsamt einer realistischen Risikoeinschätzung. Der CISO muss den Entscheidungsträgern – insbesondere dem CTO – aufzeigen, in welchen Bereichen die Sicherheitsbedrohungen am massivsten sind und wo der Nutzen einer Risikominimierung am größten wäre. Seine Aufgabe ist es, Lösungen zu finden, um diesen Bedrohungen entgegenzuwirken. Damit die Maßnahmen wirksam sind, ist die Mitarbeit aller Mitarbeiter und Abteilungen erforderlich.

Mit Technologien auf den Fachkräftemangel reagieren

Die Krux: In Zeiten fehlender Fachkräfte sind auch Sicherheitsexperten rar. Fehlendes Know-how und ein breiter Skill Gap sind die Folge. Regulatorische Anforderungen wie NIS2 setzen die Verantwortlichen zusätzlich unter Druck. Unternehmen müssen technologische und organisatorische Maßnahmen ergreifen, um sich sicher und gesetzeskonform aufzustellen. Doch wie funktioniert das im Ernstfall? Ein Fallbeispiel gibt Aufschluss.

Blick in die Praxis

Über einen Phishing-Angriff erlangen Cyberkriminelle Zugang zu den Anmeldedaten eines Mitarbeiters und installieren Ransomware. Diese verschlüsselt die Daten auf den Servern und extrahiert sensible Informationen. Die Angreifer fordern Lösegeld und drohen, die gestohlenen Daten öffentlich zu machen oder zu verkaufen – hohe finanzielle Verluste und ein erheblicher Reputationsschaden wären die Folge.

Nach dem Vorfall beschließt das Unternehmen, eine Zero-Trust-Architektur zu implementieren, bei der jeder Zugriff streng geprüft und validiert wird; sensible Daten werden standardmäßig verschlüsselt. Zusätzlich setzt die Organisation eine Anomalie-Erkennungs- und Analyse-Software ein, um Unregelmäßigkeiten zu erkennen. Das Blockieren verdächtiger Dateien und die automatisierte Erstellung unlöschbarer und unveränderbarer Snapshots sind weitere Maßnahmen.

Externe Expertise einholen

IT-Security ist keine Aufgabe für eine Person, sondern betrifft alle Bereiche eines Unternehmens. Mitarbeiter sollten daher beispielsweise durch regelmäßige Security Awareness Trainings sensibilisiert werden. Zudem braucht es Experten, die Security auf technischer Ebene beherrschen. Reichen die internen Ressourcen dafür nicht aus, können externe Spezialisten wie Logicalis unterstützen: Mit seinen Security Operation Centern (SOC) reagiert der Anbieter auf die steigende Kundennachfrage nach Managed Cyber Security Services und unterstützt Organisationen bei einer umfassenden Sicherheitsstrategie.

Markus Hahn, Malte Vollandt
www.de.logicalis.com/de

Samsung Knox Native

EINGEBAUTE SICHERHEIT FÜR VERSCHLUSSSACHEN

MEHR WERT
Samsung Knox Native

Mobiles Arbeiten verlangt umfassende Sicherheit, vor allem in Geschäftsbereichen mit hohen Sicherheitsanforderungen durch vertrauliche Daten. Mit Knox Native bietet Samsung erstmals eine Hardware-basierte und vom BSI (Bundesamt für Sicherheit in der Informationstechnik) evaluierte Sicherheitslösung, die die hohen Standards für die Verarbeitung von Verschlusssachen des Geheimhaltungsgrades „VS – Nur für den Dienstgebrauch" (VS-NfD) erfüllt.

Eingebauter Hardware-Anker

Sichere mobile Lösungen für die Speicherung von Daten gibt es schon länger – auch für die Bearbeitung von Verschlusssachen. Bisher waren dafür externe SD-Karten, zusätzliche Software und verschiedene PINs notwendig. Das brachte häufig einen großen manuellen Aufwand, hohe Kosten sowie lange Freigabe- und Evaluierungsprozesse mit sich. Samsung geht nun einen neuen Weg: Als Herzstück wird in ausgewählten mobilen Endgeräten[1] erstmals ein zertifizierter Hardware-Anker – das Samsung embedded Secure Element (eSE) – verbaut. Dieses Element ist nach dem Common Criteria Evaluation Assurance Level (CC EAL) 6+ zertifiziert und schafft einen sicheren, isolierten Bereich auf dem Gerät. Gemeinsam mit dem BSI Java Card Applet (Mobile Security Anchor) ermöglicht es die verschlüsselte Speicherung personenspezifischer und klassifizierter Daten nach den Vorgaben des BSI. Damit wurde die Lösung nun auch offiziell für die Verarbeitung von Informationen des Geheimhaltungsgrades „VS – Nur für den Dienstgebrauch" (VS-NfD) zugelassen.

Hohe Sicherheit für Standard-Applikationen

Mit der Freigabe für das VS-NfD-Umfeld kommt Samsung den wachsenden Sicherheitsanforderungen im Umfeld von Bundesbehörden entgegen. Native Funktionen wie E-Mail, Kalender oder Kontakte lassen sich auf den entsprechenden Endgeräten nun auch für die Verarbeitung von Verschlusssachen nutzen. Aber auch private Unternehmen wie Energieversorger, Banken oder andere Organisationen können von den hohen Sicherheitsstandards profitieren und Knox Native problemlos einsetzen.

Vereinfachte Sicherheitsfeatures

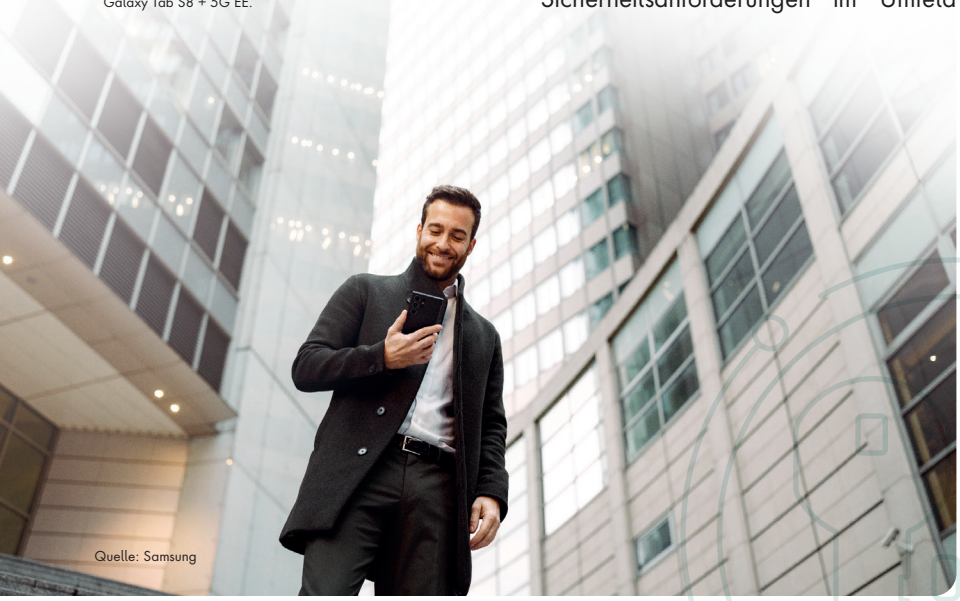
Ein Vorteil von Knox Native ist die einfache Handhabung: Die Geräte lassen sich intuitiv bedienen. Beschaffung, Inbetriebnahme, Administration und Außerbetriebstellung sind einfach und schnell umzusetzen. Besonders angenehm für die Nutzenden: Eine einzige PIN reicht zur Aktivierung aller Arbeitsbereiche. Mit Knox Native können vorinstallierte Apps in der gewohnten Android-Umgebung genutzt werden. Durch die Trennung der beiden Bereiche lassen sich die Geräte zudem geschäftlich und privat einsetzen. Auch gibt es die Möglichkeit, über spezifische Schnittstellen unternehmenseigene Apps ohne weitere aufwändige Evaluation sicher zu integrieren.

Verwaltung über Knox Suite

Zur Verwaltung der Samsung Geräte steht die Knox Suite bereit. Das Tool-Set bündelt alle Knox-Produkte wie Enrollment, Manage, E-FOTA, Asset Intelligence oder Remote Support für die IT-Administration. Damit lassen sich Prozesse von der automatischen Ersteinrichtung über die Durchsetzung geltender Sicherheitsrichtlinien bis hin zum Update-Management effektiv abdecken.

www.samsung.com/de

[1] Knox Native ist verfügbar für: Galaxy Z Fold6, Galaxy Z Fold5, Galaxy Z Flip6, Galaxy Z Flip5, Galaxy S24 5G EE, Galaxy S24 Ultra 5G, Galaxy S23 5G EE, Galaxy S23 Ultra 5G, Galaxy XCover6 Pro EE, Galaxy Tab Active4 Pro EE, Galaxy Tab Active5 EE, Galaxy Tab S8 + 5G EE.



Quelle: Samsung

Cyberresilienz

EINE PRIORITÄT FÜR KOMMUNEN

Die zunehmende Digitalisierung von Kommunen und Gemeindeverbänden dient dazu, den direkten Kontakt mit den Bürgern zu fördern und neue Dienstleistungen anbieten zu können. Dabei entstehen allerdings zwei Risiken: Die Offenlegung vertraulicher Informationen durch Cyberkriminelle und mögliche Angriffe auf die Infrastruktur gebotener Dienstleistungen. So stellt sich die Frage, wie man deren Sicherheitsniveau steigern kann, um die Betriebskontinuität zu gewährleisten und Bürger vor Cyberangriffen zu schützen. Diese Herausforderung stellte sich auch einem Gemeindeverband in Deutschland mit 200.000 Einwohnern.

Um alle Versorgungsdienstleistungen (Elektrizität, Gas, Trinkwasser, Fernwärme) und die öffentliche Infrastruktur (Beleuchtung, Parkplätze, Schwimmbäder, Transport) zu verwalten, gründete der Verband eine Gesellschaft im eigenen Besitz. Sie betreibt auch ein Webportal, über das Bürger Informationen erhalten und Anträge stellen können. Als Betreiber einer „kritischen Dienstleistung" war es gemäß der KRITIS-Verordnung für den Verband unerlässlich, für maximale Sicherheit zu sorgen.

Die „Second Line of Defence"

Zusätzlich zu vorhandenen Maßnahmen entschied sich der Verband für die Implementierung einer zweiten Firewall, um das interne Netzwerk zweifach zu schützen. Dabei wurde als zweite „Line of Defence" eine Lösung von einem anderweitigen Hersteller gewählt, um Eindringungsversuche durch unterschiedliche Technologien zu erschweren. So kamen ein Cluster aus Stormshield-Network- Security-Firewalls (SN6100) und die zentrale Verwaltungskonsole Stormshield Management Center zum Einsatz. Neben Qualitäts- und Performance-Kriterien spielte auch der Aspekt der digitalen Souveränität europäischer Einrichtungen eine Rolle und demnach die durch Zertifizierungen auf höchster europäischer Ebene belegte Vertrauenswürdigkeit der Lösungen.

Der Firewall-Cluster der nächsten Generation des europäischen Cybersicherheitsanbieters Stormshield erfüllt alle Anforderungen an Performance, Funktionalität und Skalierbarkeit des Gemeindeverbands. Die Hardware ist für kritische Infrastrukturen entwickelt und bietet einen Durchsatz von 170 Gbit/s sowie die höchste Portdichte auf dem Markt. Dies stellt sicher, dass zukünftige Sicherheitsanforderungen und Anpassungen der Netzwerkinfrastruktur frühzeitig berücksichtigt werden können.

Zusätzlich profitiert der Verband von hoher Verfügbarkeit und verbesserter Sicherheit durch die Segmentierung des Netzwerks und die Einführung strenger Policies. Sie ermöglichen es, den Datenverkehr zu kritischen Bereichen gezielt zu überprüfen und besser zu steuern. Die SN6100-Firewalls bieten zudem redundante Komponenten (Netzteil und Lüfter) und gewährleisten so einen unterbrechungsfreien Betrieb der Sicherheitslösung.

Mit der zentralen Verwaltungslösung Stormshield Management Center kann der Gemeindeverband zudem seine Aufgaben hinsichtlich der Überwachung, Konfiguration und Wartung der Firewalls optimieren. Diese Plattform ist speziell auf die Bedürfnisse von Netzwerken mit mehreren Standorten zugeschnitten, spart Zeit für Administratoren und minimiert die Fehlerwahrscheinlichkeit. Sie ist obendrein ein Teil derselben Logik, mit der sich der zukünftige Bedarf an Skalierbarkeit des Netzwerks antizipieren lässt.

Uwe Gries

DIE IMPLEMENTIERUNG MODERNER SICHERHEITSLÖSUNGEN STÄRKT NETZWERKE VON KOMMUNEN UND GEWÄHRLEISTET DEN SCHUTZ KRITISCHER INFRASTRUKTUREN VOR CYBERBEDROHUNGEN.

Uwe Gries, Country Manager DACH, Stormshield SAS, www.stormshield.com/de

Data Fabrics

FÜR DAS KONTINUIERLICHE MONITORING VON SICHERHEIT

Im Herbst 2024 ist die aktualisierte NIS2-Richtlinie in Kraft getreten. Der erweiterte Geltungsbereich der europäischen Richtlinie umfasst strenge Cybersicherheitsanforderungen, Vorschriften für die Meldung von Cybervorfällen und potenzielle Geldbußen bei Nichteinhaltung der Auflagen. Doch auch wenn die Compliance mit den Richtlinien einmal festgestellt wurde, ist die Arbeit nicht getan. Denn um das einheitlich hohe Sicherheitsniveau in kritischen Infrastrukturbereichen in Europa kontinuierlich zu überwachen, müssen große Mengen an Daten fortlaufend erfasst und analysiert werden.

In einer Mitte des Jahres vom Sicherheitsspezialisten Zscaler durchgeführten Umfrage zum Stand der NIS2-Umsetzung gaben die Befragten an, dass die NIS2-Richtlinie vielfach eine Abweichung von ihren derzeitigen Sicherheitsstrategien darstellt. Tools und Dienstleistungen wurden nicht nur als entscheidend für eine erfolgreiche Umsetzung eingestuft, sondern auch für den Nachweis der Einhaltung der Richtlinie.

Die Einhaltung der Vorschriften geht meist mit komplexen und umständlichen Verfahren zur Messung und Erfassung von Daten einher, die manuell durchgeführt werden müssen. Dementsprechend müssen die von der Richtlinie betroffenen Unternehmen Zeitaufwand einkalkulieren oder Tools zu Hilfe nehmen, die den manuellen Aufwand eindämmen. Allerdings geraten sie dabei nicht selten in das nächste Dilemma angesichts der großen Daten, die genau diese Tools generieren. Am Ende wird durch diese Datenmengen eher Verwirrung gestiftet als der Compliance-Einhaltung nachgekommen.

Ausufernde Sicherheitsdaten

Abgesehen von den gesetzlichen Anforderungen stöhnen Unternehmen bereits heute unter dem Wildwuchs von Sicherheitsdaten, die über eine Vielzahl unterschiedlicher Tools verstreut sind. Die Gründe dafür sind vielfältig: verteilte und isolierte Datenbestände im Netzwerk und in der Cloud, die Verwendung unterschiedlicher Formate und Quellen für strukturierte und unstrukturierte Daten, eine wachsende Flut von Datenschutzbestimmungen, die den Datenschutz mühsam und zeitaufwändig machen, sowie veraltete Ansätze für das Datenmanagement.

IM BEREICH DER CYBERSICHERHEIT IST DIE FÄHIGKEIT, RISIKEN EFFEKTIV ZU QUANTIFIZIEREN UND DYNAMISCH DARAUF ZU REAGIEREN VON GRÖSSTER BEDEUTUNG.

Raanan Raz, Vice President Data Analytics, Zscaler Germany GmbH, www.zscaler.de

Da sich jedes Cybersicherheits-Tool auf einen bestimmten Bereich fokussiert, fehlt den Unternehmen der ganzheitliche Überblick über die in ihre Systeme eingebundenen Entitäten (wie Mitarbeitende, Assets) und das Risiko, das mit ihnen einhergeht oder das damit verbundene Compliance-Niveau. Abhilfe aus diesem Dilemma schafft eine konsolidierte Informationsquelle, die Millionen von Daten miteinander korreliert und nicht nur einen einheitlichen Einblick in das Risiko- oder Compliance-Profil liefert, sondern auch den Kontext beisteuert. So lassen sich Reaktionen priorisieren und den besten Weg zur Behebung eines Sicherheitsproblems bestimmen.

Implementierung von Datenstrukturen

Die Antwort auf diese Herausforderung ist die Einführung von Data Fabrics für die Sicherheitsarchitektur. Mit einem solchen Designkonzept wird es möglich, Daten über eine Vielzahl potenzieller Konnektoren (inhouse und extern) zu vereinheitlichen, zu de-duplizieren, zu normieren und zu kontextualisieren und sie dann in ein verwertbares Format zu überführen. Eine solch vernetzte Datenstruktur liefert einen einzigen, aggregierten und harmonisierten Datensatz auf Knopfdruck. Damit können Sicherheitsverantwortliche Risiken priorisieren, die erforderlichen Reports für den Vorstand abliefern und Dashboards erstellen sowie Workflows zur Behebung von Problemen automatisieren.

Herkömmliche Data Lakes versagen bei der Bereitstellung von Informationen nicht selten, denn sie dienen lediglich als Repository für unstrukturierte Daten mit wenig oder gar keinen verwertbaren Erkenntnissen. Im Gegensatz dazu bie-

ten Data Fabrics nicht nur einen einheitlichen Überblick, sondern ermöglichen es, Sicherheitsteams gezielte Fragen zu stellen und präzise Antworten zu erhalten. Das manuelle Zusammenführen von Geschäftslogik und Datenelementen in Tabellenkalkulationen gehört damit der Vergangenheit an. Gartner prognostiziert, dass der Einsatz von Data Fabrics den Aufwand für das Datenmanagement um bis zu 70 Prozent reduzieren und die Zeit bis zur Wertschöpfung dementsprechend verkürzen kann.

Drei Schritte für den Aufbau von Data Fabrics

Für die erfolgreiche Erstellung brauchbarer Datenstrukturen dient ein Drei-Phasen-Ansatz:

PHASE 1: **Aufbau der Datenbasis** – Eine robuste Dateneingabefunktion und eine leistungsfähige Entity Resolution Engine sind zwei der wichtigsten Komponenten von erfolgreichen Data Fabrics. Sie ermöglichen es Unternehmen, Daten aus beliebigen Systemen zu sammeln und über unterschiedliche Quellen hinweg akkurat zu identifizieren und schließlich alle Assets (einschließlich Dubletten), Schwachstellen und Risiken zu korrelieren.

PHASE 2: **Datenanalyse** – Sobald die Data Fabric alle Entitäten aufgelöst hat, kann sie Erkenntnisse über die verschiedenen Datenpunkte korrelieren. Damit wird Einblick in erforderliche Maßnahmen geschaffen, um Compliance oder Schutz zu gewährleisten. Wenn beispielsweise ein Scanner Schwachstellen für eine Reihe von Endpunkten meldet, die Endpoint Detection and Response-Plattform einige dieser Endpunkte jedoch nicht abdeckt, kann die Data Fabric diese Lücken identifizieren.

PHASE 3: **Operationalisierung der Daten** – Das ultimative Ziel besteht in der Reaktion auf alle Erkenntnisse, die die Data Fabric generiert. Die Operationalisierung dieser Erkenntnisse umfasst die Erstellung von Reports und Dashboards, die eine fundiertere und schnellere Entscheidungsfindung ermöglichen. Die Messung benutzerdefinierter Leistungsindikatoren hilft dabei Risiken in Echtzeit zu verstehen und die nötigen Datenhygieneschritte wie die Aktualisierung der Konfigurationsmanagement-Datenbank eines Unternehmens und die Automatisierung von Korrektur-Workflows über Ticketing-Systeme auszulösen.

Auf Data Fabrics aufbauen

Aktuelle Data Fabrics bieten grundlegende Datenverarbeitungsfunktionen wie Erfassung, Analyse und Reaktionsoptionen. Aufbauend auf seiner umfangreichen Sicherheitsplattform Zero Trust Exchange ist Zscaler darüber hinaus in der Lage, weitere Anwendungen zu integrieren. Der konsolidierte Überblick über alle Tools und Datenquellen in einer Verwaltungsoberfläche ermöglicht Sicherheitsentscheidungen in Echtzeit. Diese umfassende Transparenz ist für ein effektives Risikomanagement, die strategische Entscheidungsfindung und den Nachweis der fortwährenden Einhaltung von Vorschriften wie NIS2 unerlässlich.

Im Bereich der Cybersicherheit ist die Fähigkeit, Risiken effektiv zu quantifizieren und dynamisch darauf zu reagieren von größter Bedeutung. Unternehmen können durch die Nutzung der Leistungsfähigkeit von Data Fabrics mehr Sicherheit, Effizienz und Resilienz gegenüber den sich ständig ändernden Cyber-Bedrohungen erreichen.

Raanan Raz

Sicherheits-Patching

LÜCKENLOSER SCHUTZ BEGINNT MIT SYSTEMATISCHEN SOFTWARE-UPDATES

SICHERHEITS-PATCHING IST EIN ESSENZIELLER BESTANDTEIL DER ENDPUNKTSICHERUNG UND STELLT EINEN INTEGRALEN BESTANDTEIL VON IT-SICHERHEITS-PROZESSEN IN UNTERNEHMEN DAR.

André Schindler, General Manager, EMEA, und Senior Vice President of Global Sales, NinjaOne, www.ninjaone.com/

Sicherheits-Patching ist ein essenzieller Bestandteil der Endpunktsicherung und stellt einen integralen Bestandteil von IT-Sicherheitsprozessen in Unternehmen dar. Diverse Statistiken belegen die erheblichen Risiken, die nicht gepatchte Software in sich birgt. So zeigt der Bericht zu ungepatchten Schwachstellen 2022 von Automox, dass 60 Prozent aller Verletzungen des Datenschutzes auf nicht gepatchte Sicherheitslücken zurückzuführen sind.

Warum wird Sicherheits-Patching also nicht in ausreichenden Maßen durchgeführt, obwohl es so wichtig für den Schutz vor Cyberangriffen ist?

Die Antwort: Unternehmen stufen das Installieren von Sicherheits-Patches häufig als zu komplex und zu zeitaufwändig ein.

Tatsache ist aber, dass Patchen für die Sicherheit und somit für den langfristigen Erfolg eines Unternehmens unentbehrlich ist. Fünf wesentliche Punkte sind allerdings dabei zu beachten.

5 wichtige Tipps für Sicherheits-Patching

#1 Prozesse automatisieren

Automatisierung ist der optimale Ansatz, um sicherzustellen, dass Sicherheits-Patches ohne übermäßigen Zeitaufwand installiert werden können. Mit dem Patch-Management-Tool von NinjaOne können Unternehmen ihr Sicherheits-Patching problemlos konfigurieren und dann bedenkenlos automatisch ablaufen lassen.

#2 Alle Sicherheitspatches überprüfen

Bevor Unternehmen einen Sicherheitspatch einspielen, sollten sie ihn in einer passenden Testumgebung laufen lassen und so sicherstellen, dass er ordnungsgemäß funktioniert. Obwohl das Testen Zeit und Ressourcen in Anspruch nimmt, lohnt sich dieser zusätzliche Aufwand, denn er verhindert mögliche Probleme mit Geräten oder sogar mit der gesamten IT-Infrastruktur.

#3 Proaktiv handeln und Sicherheitsaktualisierungen priorisieren

Um die Sicherheit und Aktualität aller unternehmensinternen Systeme zu gewährleisten, sollten IT-Abteilungen proaktiv handeln und Sicherheitsaktualisierungen immer ganz oben auf ihre Agenda setzen. Proaktive Benachrichtigungen und Warnmeldungen sind dafür eine wichtige Unterstützung. Sie gewährleisten, dass alle Aktualisierungen rechtzeitig und effektiv durchgeführt werden können.

#4 Einen Gesamtüberblick der IT-Ressourcen erstellen

Ein IT-Asset-Inventar listet alle IT-Ressourcen eines Unternehmens. Ein von Experten empfohlener Ansatz ist das Erstellen einer kompletten Übersicht nach Gerätetypen, Betriebssystemen, Hardware und Drittanbieteranwendungen. Hat ein Unternehmen ein klares Bild seiner IT-Ressourcen erstellt, dann kann es bereits bekannte Schwachstellen mit seinem Inventar abgleichen und eine sinnvolle Reihenfolge der Patches erstellen.

#5 Richtlinien für das Patch-Management ausarbeiten

Richtlinien strukturieren die Schritte im Patching-Prozess und helfen IT-Abteilungen, ihre Patches zu priorisieren, zu testen, zu implementieren und zu überwachen. Da es verschiedene Patching-Richtlinien gibt, sollten Unternehmen die für ihre spezifische IT-Umgebung und Bedürfnisse passende Vorgabe wählen.

Umfassendes Patching nimmt Zeit zugegebenermaßen in Anspruch. Dies wird aber durch die enorme Bedeutung für die Cyber-Sicherheit von Unternehmen aufgewogen, außerdem gibt es Lösungen, die dabei helfen können, die mühsamen Teile des Patchings zu automatisieren, um Organisationen effizienter und produktiver zu machen. Unternehmen sollten sich fortlaufend mit dem Thema Patch-Management befassen und ihre Patching-Strategie entwickeln, nicht nur um Cyberkriminalität zu verhindern, sondern auch um die reibungslosen Geschäftsabläufe ihrer Organisation zu gewährleisten.

André Schindler

SDoT Industry Gateway

EFFEKTIVE CYBERSICHERHEIT FÜR KRITISCHE INFRASTRUKTUREN

Unternehmen aus gefährdeten industriellen Sektoren und Kritischen Infrastrukturen geraten zunehmend ins Visier von Cyberkriminellen. Einen wirksamen Schutz bietet das SDoT Industry Gateway von infodas. Dieses Cybersecurity-Tool gewährleistet den bidirektionalen Datenaustausch sowie die Filterung von strukturierten und unstrukturierten Daten.

Die heutige vernetzte Welt entwickelt sich zunehmend als Zielscheibe für Cyberkriminelle und die Auswirkungen der Angriffe werden immer größer. Besonders für Kritische Infrastrukturen und gefährdete industrielle Sektoren nimmt die Bedrohungslage rapide zu. Die Folge: Erhebliche IT-Ausfälle, die teilweise komplette Wirtschaftszweige treffen. Viele Unternehmen und Einrichtungen arbeiten mit teils veralteten Systemen und verfügen über keinen oder nur eingeschränkten Zugriff auf isolierte Systeme in der Betriebstechnologie (OT), was im Falle eines Angriffs einen großen Nachteil darstellt.

Umfassender Cybersecurity-Schutz

Als Lösung für die zunehmende Gefahr der Cyberangriffe entwickelte die INFODAS GmbH das SDoT Industry Gateway. Basierend auf der SDoT Produktfamilie, die seit vielen Jahren erfolgreich im Verteidigungssektor eingesetzt wird, wurde das Cybersecurity-Tool für die spezifischen Anforderungen im Bereich der Kritischen Infrastrukturen entwickelt. Das SDoT Industry Gateway bietet dem privaten Sektor einen umfassenden Cybersecurity-Schutz, der höchsten Zertifizierungslevels entspricht sowie einen vollständig gesicherten und kontrollierten Datenaustausch zwischen verschiedenen Sicherheitsdomänen (IT/OT) gewährleistet.

MEHR WERT

SDoT Industry Gateway

www.infodas.com/de

Kontroverses US-Verbot

GOOGLE ENTFERNT KASPERSKY GLOBAL AUS DEM PLAY STORE

Nutzer berichteten vermehrt darüber, dass Kasperskys Produkte, darunter Kaspersky Endpoint Security und VPN & Antivirus by Kaspersky, im Google Play Store in den USA und anderen Regionen der Welt nicht mehr verfügbar sind.

Das Unternehmen bestätigte das Problem in den offiziellen Foren des Unternehmens und erklärte, dass derzeit untersucht werde, warum die Software nicht mehr im App Store von Google erhältlich ist.

Ein Mitarbeiter teilte zunächst mit, dass Downloads und Updates von Kaspersky-Produkten im Google Play Store vorübergehend nicht verfügbar seien und man Lösungen prüfe, um sicherzustellen, dass Nutzer weiterhin Anwendungen von Google Play herunterladen und aktualisieren können.

US-Verbot als Auslöser

Kaspersky riet daraufhin den Nutzern, sie über alternative App-Stores wie den Galaxy Store, den Huawei AppGallery und Xiaomi GetApps zu installieren. Die Sicherheits-Apps des Unternehmens können auch durch das Herunterladen der .apk-Installationsdatei von der Kaspersky-Website installiert werden. Eine Support-Seite bietet weitere Informationen zur Installation und Aktivierung der Software auf Android-Geräten.

Diese Entwicklung folgt auf die Ankündigung von Kaspersky, dass das Unternehmen seine Geschäftstätigkeit in den Vereinigten Staaten einstellen werde, nachdem die US-Regierung im Juni Sanktionen gegen das Unternehmen und 12 Führungskräfte verhängt und deren Antiviren-Software aus Gründen der nationalen Sicherheit verboten hatte.

Google bestätigte, dass das Kaspersky-Verbot in den USA zu dieser Entscheidung geführt hat, das Unternehmen und seine Produkte im Google Play Store dauerhaft zu sperren.

Lars Becker | www.it-daily.net

Mit Sensibilisierung zu mehr Sicherheit

CYBERSECURITY AWARENESS: STÄRKUNG DER ERSTEN VERTEIDIGUNGSLINIE IM UNTERNEHMEN

Mitarbeitende sind oft das größte Einfallstor für Cyberangriffe. Ein unbedachter Klick auf einen Link in einer Phishing-E-Mail, ein unbekannter USB-Stick oder das Verwenden schwacher Passwörter – und schon kann es geschehen: Schadsoftware breitet sich im Unternehmensnetzwerk aus, sensible Daten geraten in die falschen Hände oder es kommt zu einem kostspieligen Datenverlust. Aus diesem Grund wird die Sensibilisierung der Mitarbeitenden zu einer unverzichtbaren Maßnahme, um das Unternehmen vor Cyberbedrohungen zu schützen.

Cybersecurity Awareness ist nicht nur eine notwendige Compliance-Maßnahme, sondern ein essenzieller Bestandteil des ganzheitlichen Sicherheitsansatzes eines Unternehmens. Mitarbeitende sind täglich potenziellen Gefahren ausgesetzt. Ein Phishing-Angriff kann schnell erfolgreich sein, wenn die Mitarbeitenden nicht über die Risiken und die Erkennung solcher Angriffe informiert sind. Noch gefährlicher sind fremde USB-Sticks, die unachtsam ins Firmennetzwerk eingebunden werden und so Schadsoftware direkt ins System bringen können.

Wenn das gesamte Team jedoch weiß, worauf es achten muss, können viele dieser Bedrohungen von vornherein abgewehrt werden. Die Notwendigkeit für aufwendige technische Maßnahmen wird reduziert, wenn die beteiligten Personen von Anfang an sensibilisiert sind.

Herausforderungen

Eine der größten Herausforderungen bei der Einführung von Cybersecurity-Awareness-Programmen besteht darin, dass diese oft als reine Compliance-Maßnahme betrachtet werden. Unternehmen sind häufig verpflichtet, solche

Programme einzuführen, sei es aufgrund gesetzlicher Vorgaben oder branchenspezifischer Standards. Das führt dazu, dass Mitarbeitende einmal im Jahr eine Schulung durchlaufen, deren Inhalte oft schnell vergessen werden. Nachhaltige Learnings bleiben dabei auf der Strecke. Die Folge ist, dass das Team zwar formal geschult ist, jedoch das Gelernte nicht langfristig anwendet. Hier liegt eine der größten Schwächen vieler Cybersecurity-Awareness-Programme.

Effektive Maßnahmen zur Stärkung der Sicherheitskultur

Für eine nachhaltige Cybersecurity Awareness reicht es nicht aus, einmal im Jahr eine Schulung abzuhalten. Vielmehr sollten kontinuierliche und kreative Maßnahmen ergriffen werden, um das Bewusstsein zu schärfen. Unternehmen haben hier eine Vielzahl von Möglichkeiten, um die Sicherheitskultur zu fördern.

Beispielsweise können Unternehmen Sicherheitshinweise an Orten platzieren, die Mitarbeitende regelmäßig besuchen, wie Büros, Kantinen oder auf den Toiletten. Subtile Hinweise an solchen Stellen können das Sicherheitsbewusstsein unauffällig, aber effektiv stärken. Ein weiterer Ansatz sind spielerische Methoden wie Cybersecurity-Escape-Rooms, die Mitarbeitenden auf interaktive Weise zeigen, wie wichtig IT-Sicherheit ist. Ein Beispiel für einen Cybersecurity Escape Room kann die Nachstellung eines Cyberangriffs sein. Beispielsweise könnte das Szenario sein, dass das eigene Unternehmen angegriffen wurde und man keinen Zugriff mehr auf die kritischen Produktionsprozesse des Unternehmens hat. und nach Ablauf der Zeit das Werk zerstört werden würde. Man muss dann schrittweise entweder selbst den Angriff durchführen, um wieder Zugriff zu erlangen oder entsprechend herausfinden, was passiert ist und dies dann rückgängig machen (auf Rätseln basierend).

Darüber hinaus gibt es weitere Maßnahmen, die die Sicherheitskultur fördern können:

#1 Regelmäßige Phishing-Tests:
Simulierte Phishing-Angriffe, um das gesamte Team auf die Erkennung solcher Bedrohungen vorzubereiten und das Bewusstsein zu schärfen.

#2 Kurze, regelmäßige Schulungseinheiten:
Statt langer, jährlicher Schulungen sind kurze, regelmäßige Sessions effektiver, um das Wissen aufzufrischen und aktuell zu halten.

#3 Visuelle Erinnerungen:
Bildschirmschoner oder Poster in Bürobereichen, die regelmäßig Sicherheitsbotschaften und Tipps anzeigen.

#4 Interaktive E-Learning-Module:
Online-Trainings, die durch interaktive Inhalte und Quizfragen das Gelernte festigen.

#5 Security-Ambassadors:
Ausbildung von einzelnen Mitarbeitenden als Sicherheitsbotschafter, die in ihren Teams als Ansprechpersonen für IT-Sicherheitsthemen fungieren und das Sicherheitsbewusstsein weiter stärken.

Die Rolle der NIS2-Richtlinie

Die NIS2-Richtlinie bringt frischen Wind in die Cybersecurity Awareness. Sie verpflichtet nicht nur Unternehmen dazu, alle Mitarbeitenden regelmäßig zu schulen, sondern nimmt auch das Management in die Verantwortung. Führungskräfte können nicht mehr einfach nur die Verantwortung delegieren, denn ab sofort können sie bei Nichteinhaltung von Vorgaben oder Cyberangriffen selbst persönlich haftbar gemacht werden. Sie müssen also selbst verstehen, welche Risiken das Unternehmen bedrohen und wie wichtig die Sensibilisierung des gesamten Teams ist.

CYBERSECURITY AWARENESS IST EIN UNVERZICHTBARER BESTANDTEIL DES SCHUTZES VOR CYBERBEDROHUNGEN.

Christian Schlehuber, Geschäftsführer, CyberShield (CS-Consulting GmbH), https://cybershield-consulting.com/

Besonders wichtig ist, dass das Management gezielt geschult wird, um die Risiken für das Unternehmen einschätzen zu können und entsprechend qualifizierte Entscheidungen zu treffen. Dadurch wird die Cybersecurity Awareness im gesamten Unternehmen gestärkt.

Geschultes Personal, sichere Unternehmen

Cybersecurity Awareness ist ein unverzichtbarer Bestandteil des Schutzes vor Cyberbedrohungen. Die Kombination aus regelmäßiger Sensibilisierung, gezielten Schulungen und kreativen Ansätzen sorgt dafür, dass Unternehmen langfristig sicherer werden. Die NIS-2-Richtlinie verstärkt diese Bemühungen, indem sie das Management in die Verantwortung nimmt und sicherstellt, dass die Awareness-Maßnahmen nachhaltig und effektiv sind. So wird die Sicherheitskultur eines Unternehmens ganzheitlich gestärkt und Cyberbedrohungen können wirksam abgewehrt werden.

Christian Schlehuber

Cyber Threat Detection

CAASM HILFT, MIT ANGREIFERN SCHRITT ZU HALTEN

MIT CAASM KÖNNEN UNTERNEHMEN POTENZIELLE SICHERHEITSLÜCKEN IN IHREN IT-ASSETS PROAKTIV IDENTIFIZIEREN UND ENTSCHÄRFEN.

David Dahlhaus, Manager, Enterprise Sales DACH, Ivanti, www.ivanti.com/de

Hunderte von Mitarbeitergeräten, die weder erfasst noch verwaltet werden, aber zumindest geduldet auf Firmenressourcen zugreifen: Die Grauzone der hybriden Arbeit erhöht nicht nur die Angriffsfläche von Unternehmen. Sie schwächt vor allem das Risikomanagement der Security-Teams. Denn werden Assets nur lückenhaft erfasst, fällt auch eine Bewertung der potenziellen Auswirkungen von Sicherheitsverletzungen schwer. An dieser Stelle setzt ein unternehmensweites Cyber Asset Attack Surface Management (CAASM) an.

CAASM ist ein recht neues, aber wirkungsvolles Element einer modernen Cyberstrategie. Es identifiziert nicht nur Assets, sondern bewertet auch Risiken, die mit bekannten und unbekannten Geräten in einer komplexen digitalen Umgebung verbunden sind. CAASM liefert dazu einen vollständigen, aktuellen und konsolidierten Überblick über die internen und externen IT-Ressourcen einer Organisation. Dazu sammeln CAASM-Lösungen per API-Integration Daten aus bestehenden Tools für Asset Discovery, IT Asset Management, Endpoint Security, dem Schwachstellen- und Patch Management sowie aus Ticketing-Systemen.

Diese Informationen werden automatisch aggregiert, normalisiert und den IT- und Sicherheitsteams integriert dargestellt – inklusive aller Rechte und dem Geschäftskontext der jeweiligen Assets. Ziel ist es, eine transparente Übersicht über die potenzielle Angriffsfläche zu erhalten und Abhilfemaßnahmen auf Basis der größten Risiken zu priorisieren. Durch die Klassifizierung von Assets sind Teams in der Lage, sich auf risikoreichere Assets zu konzentrieren und gleichzeitig eine angemessene Kontrolle über risikoärmere Assets wie Edge-Geräte aufrechtzuerhalten.

Sicherheit von Assets gewährleisten

Der Erfolg einer funktionierenden CAASM-Strategie basiert auf gut definierten ITAM-Prozessen und leistungsfähigen Systemen für das Asset Management. Beides versorgt Security-Teams mit Informationen, die dann für die Priorisierung von Sicherheitsmaßnahmen nötig sind.

Ein effektiver CAASM-Lösungs-Stack besteht aus mehreren Komponenten:

#1 Die Asset-Datenbank der ITAM-Lösung dient als zentrales Repository für die Verwaltung aller Asset-Informationen wie Attribute, Konfigurationen und Zuordnung von Beziehungen und Abhängigkeiten.

#2 Durch regelmäßige Scans werden Sicherheitslücken in Hard- und Software sowie Konfigurationen erkannt, nach ihrem Schweregrad eingeordnet und Empfehlungen zur Behebung abgegeben.

#3 Im Rahmen der Bedrohungsanalyse liefern Tools aus dem Schwachstellenmanagement Daten über neue Gefahren und Trends. Dabei werden verschiedene Quellen überwacht, wie öffentliche und private Feeds, soziale Medien und Dark-Web-Foren, um potenzielle Angriffsvektoren zu identifizieren.

#4 Über die Configuration Management Database (CMDB) lassen sich Asset-Änderungen verfolgen, verwalten und dokumentieren.

Proaktive IT-Sicherheit

Durch die Kombination von Asset-Erkennung und -Inventarisierung, Verwaltung von Sicherheitslücken, Threat Intelligence und CMDB sind Unternehmen möglichen Cyberbedrohungen einen Schritt voraus. Mit Hilfe von CAASM können sie die Sicherheit ihrer IT-Ressourcen deutlich erhöhen.

David Dahlhaus

CYBERSECURITY REPORT 2024

Laut dem State of Cybersecurity Report 2024 von Ivanti investiert erst jeder vierte Sicherheitsverantwortliche in Deutschland in moderne Tools zur Cyberabsicherung wie Identity Threat Detection and Response (ITDR), Cyber Asset Attack Surface Management (CAASM) oder Digital Risk Protection Services (DRPS) https://bit.ly/3ZSfZ8P.

Vulnerability Management

TOOLS ZUM FINDEN UND BEURTEILEN VON SOFTWARE-SCHWACHSTELLEN

Neue Schwachstellen schnellstmöglich zu schließen, ist eine zentrale Aufgabe für IT-Sicherheitsverantwortliche. Professionelle Hacker sind mit als Erste über CVE-Lücken informiert und führen innerhalb von 24 Stunden gezielte Angriffe auf die neuen Einfallstore in das Opfernetzwerk aus, um Angriffspotenziale zu erkennen. Wer dem die passenden Riegel – Patches – vorschieben will, benötigt verschiedene Tools, um das Risiko der Schwachstellen zu bewerten, diese priorisiert zu beheben und die Maßnahmen zu dokumentieren.

Zahlreiche Werkzeuge neben dem klassischen Patch Management stehen bereit, welche wichtige Informationen für eine IT-Sicherheitsplattform zusammentragen, aber auch blinde Flecken in der Überwachung aufweisen:

➤ Configuration-Management-Datenbanken (CMDB) sammeln Informationen über Software, Hardware, Systemen, Produkte und Mitarbeitern. CMDB sind prädestiniert dafür, die Konfigurationen dieser Assets zu verwalten und zu dokumentieren. Sie bieten aber keine Sichtbarkeit über Vorgänge im Netzwerk und zu möglichen Beziehungen zwischen diesen Assets.

➤ Tools zum Sichern von Cloud-Assets wie Cloud Access Security Broker (CASB), Cloud-Security-Posture-Management (CSPM), Cloud Workload Protection Plattformen (CWPP) und Cloud–Native-Application-Protection-Plattformen (CNAPP) spielen eine wichtige Rolle, die mit jedem in die Cloud verlagerten Workload steigt. Sie lassen aber On-Premise-Systeme und die zugrundeliegende Infrastruktur außer Betracht.

➤ Vulnerability-Scanner sind von zentraler Bedeutung, um Sicherheitsschwächen zu lokalisieren und zu priorisieren. Frei verfügbare Scanner überwachen Netzwerke, Hardware, Betriebssysteme, Anwendungen und Datenbanken: Die Suchmaschine Shodan teilt Informationen zu exponierten Geräten wie Server, Router, IP-Kameras oder Smart-TVs. Leider können auch Cyberkriminelle dieses Wissen abrufen.

➤ Risk Assessment Tools werten die Informationen von Extended-Detection-and-Response (XDR)-Technologien aus. IT-Administratoren erkennen so die Gefahren fehlerhaft konfigurierter Betriebssysteme, verwundbarer Applikationen oder riskanten menschlichen Verhaltens.

➤ Eine Software Bill of Materials (SBOM) dokumentiert alle Komponenten einer Applikation. Dank ihr können IT-Sicherheitsexperten feststellen, welche Elemente einer Anwendung verwundbar, zu verbessern oder zu aktualisieren sind. Sie können die betroffenen Elemente schnell identifizieren und Angriffe eindämmen. Eine SBOM vermindert das Risiko und die Effekte einer Supply-Chain-Attacke.

➤ Der Expertenblick durch Managed Detection and Response (MDR) Services ist wichtig, um vorherzusagen, wie Cyberkriminelle CVE-Schwachstellen ausnutzen werden. Sicherheitsexperten erkennen die akuten Gefahren, die sich aus Offenlegungen ergeben und filtern die für eine IT-Infrastruktur relevanten Informationen heraus. So können die Experten den Exploits zuvorkommen, Schwachstellen schließen und im Ernstfall ein Threat Hunting starten.

Angesichts der zunehmend komplexen Angriffsfläche und kontinuierlich wachsender Softwarelücken benötigen IT-Verantwortliche eine robuste Strategie zum Verwalten und Schließen ihrer Verwundbarkeiten. Diese beruhen auf verschiedenen Tools und deren Integration in eine IT-Sicherheitsplattform. Entscheidend kommt es auf zuverlässige Wissensressourcen an, die eine Grundlage für fundierte Entscheidungen liefern.

Jörg von der Heydt

ANGESICHTS DER ZUNEHMEND KOMPLEXEN ANGRIFFSFLÄCHE BENÖTIGEN IT-VERANTWORTLICHE EINE ROBUSTE STRATEGIE ZUM VERWALTEN UND SCHLIESSEN IHRER VERWUNDBARKEITEN.

Jörg von der Heydt,
Regional Director DACH, Bitdefender,
www.bitdefender.de

it security AWARDS 2024

GEWINNER IM RAHMEN DER „IT-SA 2024“ AUSGEZEICHNET

itsecurity AWARD 2024
WWW.IT-SECURITY-AWARD.COM

DIE PREISTRÄGER DER IT SECURITY AWARDS 2024 STEHEN FEST. VERGEBEN WURDEN SIE IN DEN KATEGORIEN MANAGEMENT SECURITY, INTERNET/WEB SECURITY, CLOUD SECURITY UND IAM. AUSGEZEICHNET WURDEN DIE FOLGENDEN HERSTELLER: ABSTRACT SECURITY, LASSO SECURITY, NOKOD SECURITY UND BXC-CONSULTING.

MANAGEMENT SECURITY

Abstract Security: Sicherheitsmanagement der nächsten Generation

Die Zukunft der Security Operations-Plattformen heißt Abstract Security. Denn das SIEM der nächsten Generation wird kein SIEM mehr sein. Warum? Nur 42 Prozent der erfolgreichen Angriffe werden von einem traditionellen SIEM innerhalb einer Woche nach dem Eindringen entdeckt. Das bedeutet ihr Einsatz ist in den meisten Fällen zweifelhaft. Warum ist das so?

Bei herkömmlichen monolithischen Architekturen, die auf indexbasierten Ansätzen beruhen, sind die Alarmierungszeiten zu hoch.

Es benötigt also neuer Ansätze, um das Problem zu lösen: Abstract Security, hat eine revolutionäre Plattform mit einem KI-gesteuerten Assistenten entwickelt, um die Verwaltung von Sicherheitsanalysen besser zu zentralisieren.

Die innovative Lösung geht über SIEM-Lösungen der nächsten Generation hinaus, indem es Daten in Echtzeit zwischen Datenströmen korreliert. Dadurch können Compliance- und Sicherheitsdaten separat genutzt werden, um die Erkennungseffizienz zu erhöhen und die Kosten zu senken.

Zwischen Sicherheitsanalysen und Compliance gibt es einen grundsätzlichen Unterschied.

Sicherheitsanalysen werden gestreamt, Compliance-Daten werden durchsucht.

Die Datenverwaltung von Abstract hilft den Teams bei der Optimierung der Daten, ohne die Einhaltung von Vorschriften oder die Sicherheitseffektivität zu beeinträchtigen. Dies ermöglicht Teams sofortige Kosteneinsparungen

Colby DeRodeff, Mitbegründer, Abstract Security, www.abstract.security

bei der Speicherung, eine schnellere Erkennung und leistungsstarke Analysefunktionen.

Die „Zukunft" von SIEM ist bei vielen Anbietern nichts weiter als eine weitere Generation von Logging-Suchmaschinen mit einem neuen Dashboard und neuen Funktionen geworden. Es ist aber an der Zeit, die Fehler der Vergangenheit nicht einfach nur zu modernisieren, denn 95 Prozent der gesammelten Protokolldaten sind für die Erkennung unbrauchbar. Ein niederschmetternder Wert. Es ist Zeit für einen Paradigmenwechsel.

Anwender müssen daher ihre Daten für Compliance- und Sicherheitszwecke trennen, um Kosten zu sparen, die Effizienz zu steigern und Ihre Erkennungsfunktionen zu verbessern.

In der Vergangenheit wurde sich zu sehr auf das Data Engineering konzentriert und die Sicherheitsexperten gezwungen, die Feinheiten von ETL zu lernen. Daraus ist Abstract entstanden, eine No-Code-Lösung für die Datenerfassung, -verwaltung und -umwandlung.

INTERNET/WEB SECURITY

Lasso Security: KI-Sicherheitslösungen für die LLM-Technologie

Stellen Sie sich eine Zukunft vor, in der LLM-Technologie nicht nur produktiv, sondern auch sicher ist. Lasso Security arbeitet an genau dieser Zukunft und stattet LLM-Pioniere mit innovativen KI-Sicherheitslösungen aus.

Der unkontrollierte Einsatz von LLMs schafft bereits jetzt neue Schwachstellen für Organisationen jeder Größe. Ziel ist es, die Risiken des unkontrollierten Einsatzes von LLMs, wie Data-Poisoning und AI-Pakethalluzinationen, zu minimieren, bei denen bösartige Daten in Trainingsmodelle eingeschleust oder nichtexistierende Schadpakete generiert werden. Lasso ist das erste seiner Art: eine LLM-First-End-to-End-Sicherheitslösung für LLM-Pioniere.

Die Gründer von Lasso Security: Elad Schulman, Lior Ziv, Ophir Dror und Yuval Abadi (von links). www.lasso.security (Foto: Sharon Gadasi)

IT Security Awards 2024
Weitere Informationen und Bilder der Preisverleihung finden Sie unter: www.it-daily.net/informationen/it-security-awards

Ein weiteres Problem sind Prompt-Injection-Angriffe, bei denen Schadcode über manipulierte Eingaben in Systeme gelangt. Diese Art von Angriff kann die Datenintegrität gefährden, vertrauliche Informationen stehlen und Chatbot-Dienste stören. Direkte und indirekte Prompt-Injections sind die beiden grundlegenden Kategorien, in die diese Art Angriffe im Allgemeinen eingeteilt werden können. Sowohl direkte als auch indirekte Prompt-Injections stellen erhebliche Bedrohungen für GenAI-Anwendungssysteme dar.

Da GenAI fast jeden Aspekt unseres Privat- und Berufslebens durchdringt, überrascht es nicht, dass auf Large Language Models (LLM) basierende generatuve KI-Tools zu einem festen Bestandteil des Programmier-Tookits geworden sind.

Doch dabei gibt es einen Aspekt, die Sicherheits-, Risikomanagement- und Compliance-Leiter aufhorchen lassen sollte: Rund 80 Prozent der Programmierer umgehen Sicherheitsrichtlinien, wenn sie diese Tools verwenden und das, obwohl sie wissen, dass GenAI-Programmierassistenten regelmäßig unsicheren Code erstellen.

Lasso Security bietet die erste End-to-End-Lösung speziell für LLMs, um Organisationen zu helfen, sicher und effizient mit diesen KI-Tools zu arbeiten, ohne die Sicherheit zu gefährden.

CLOUD SECURITY

Nokod Security: Sicherheit für Low-Code/No-Code (LCNC)-Anwendungen

Wie können Anwender Sicherheit in den Lebenszyklus ihrer Low-Code-/No-Code-Anwendung bringen und gleichzeitig Compliance-Risiken im Auge behalten und wissen, welche Sicherheitsmaßnahmen Sie ergreifen sollten? Die Antwort lautet Nokod Security.

Die Sicherheitsplattform hilft Unternehmen, Sicherheitsrisiken bei der Entwicklung von Low-Code/No-Code (LCNC)-Anwendungen und Robotic Process

> DAS JAHR 2024 HAT GEZEIGT, DASS DAS INNOVATIONSPOTENZIAL IN DER IT SECURITY-BRANCHE NACH WIE VOR EXTREM HOCH IST".
>
> Ulrich Partier, Publlisher it management

Yair Finzi, Mitbegründer und CEO, Nokod Security, https://nokodsecurity.com/

Automation (RPA) zu bewältigen. Das Besondere an Nokod ist die Fähigkeit, alle LCNC-Anwendungen und Automatisierungen in einem zentralen Dashboard zu überwachen, Sicherheitslücken und Schwachstellen automatisch zu erkennen und sofortige Lösungen anzubieten. Dies schließt auch den Schutz vor Datenlecks und Injektionsangriffen ein, die bei traditionellen Sicherheitsansätzen oft übersehen werden.

Die Plattform geht dabei weit über einfaches Management hinaus: Sie bietet umfassenden Schutz vor diversen Bedrohungen wie Datenlecks, Injection-Schwachstellen und ungepatchten Anwendungen und Komponenten. Durch diesen ganzheitlichen Ansatz gewährleistet Nokod Security nicht nur die Kontrolle über die wachsende Zahl von Low-Code/No-Code-Lösungen, sondern stellt auch deren sichere Integration in die Unternehmens-IT sicher.

IAM

BxC-Consulting: Vollautomatisierte Verwaltung digitaler Zertifikate

In der modernen Industrie sind digitale Zertifikate ein wesentlicher Bestandteil für die sichere und effiziente Kommunikation zwischen vernetzten Geräten. Die CERIAL-Lösung von BxC-Consulting revolutioniert das Management dieser Zertifikate, indem sie die Ausstellung und Erneuerung vollautomatisiert. Das Programm wurde entwickelt, um den Betreibern von Geräten die zeitaufwändige und fehleranfällige manuelle Verwaltung von Zertifikaten abzunehmen und gleichzeitig höchste Sicherheitsstandards zu gewährleisten.

Die Lösung übernimmt den gesamten Lebenszyklus der Zertifikate, von der Ausstellung über die Erneuerung bis hin zur Verwaltung. Bevor ein Zertifikat abläuft, sorgt es automatisch für die rechtzeitige Erneuerung, ohne dass ein Eingreifen durch den Betreiber erforderlich ist. Dies stellt sicher, dass die Geräte immer über gültige und aktuelle Zertifikate verfügen, was Ausfallzeiten und Sicherheitsrisiken minimiert.

Mit dem Aufkommen des Industrial Internet of Things (IIoT) wächst die Anzahl der vernetzten Geräte in industriellen Umgebungen rasant. Jedes dieser Geräte benötigt ein digitales Zertifikat, um sicher und authentifiziert kommunizieren zu können. Die manuelle Verwaltung dieser wachsenden Anzahl an Zertifikaten wird zunehmend unpraktikabel und ineffizient. Unternehmen stehen vor der Herausforderung, skalierbare und automatisierte Lösungen zu implementieren, die es ihnen ermöglichen, den Überblick zu behalten und die Sicherheit der gesamten Infrastruktur zu gewährleisten.

CERIAL unterstützt moderne PKI-Protokolle (wie EST), ist plattformübergreifend nutzbar und an verschiedene PKIs anbindbar. Durch den Verzicht auf zentrale Steuerung und Kontrolle eignet sich CERIAL besonders für segmentierte Netzwerke und kann problemlos auf Linux-basierten IIoT-Geräten eingesetzt werden. Diese dezentrale Architektur gewährleistet maximale Flexibilität bei der Integration in bestehende Infrastrukturen, ohne dabei Kompromisse bei der Sicherheit einzugehen.

Ulrich Parthier | www.it-daily.net

Die Gründer von BxC Consulting Carsten Schwant, Letitia Combes und Marcel Fischer, www.bxc-security.com/de

NORDKOREAS TROJANER

HACKER TARNEN SICH ALS IT-MITARBEITER

Nordkoreanische Hacker haben sich als IT-Fachkräfte getarnt und so über hundert US-Unternehmen unterwandert.

Das zeigt der jüngsten Threat Hunting Report 2024 von CrowdStrike. Die als „Famous Chollima" bekannte Hackergruppe startete ihre raffinierte Operation Anfang 2023. Mit gefälschten Identitäten als amerikanische IT-Experten gelang es ihnen, in die Netzwerke von Unternehmen aus sensiblen Bereichen wie Luft- und Raumfahrt, Verteidigung und Technologie einzudringen. Ihre Taktik? Sie arbeiteten gerade genug, um nicht aufzufallen, während sie im Hintergrund Daten abschöpften und heimlich Überwachungstools installierten.

CrowdStrike nahm Kontakt zu den betroffenen Unternehmen auf, um sie über potenzielle Insider-Bedrohungen zu informieren. Adam Meyers, leitender Experte bei CrowdStrike, zeigt sich besonders beunruhigt: „Der Fall 'Famous Chollima' war einer der schockierendsten, an dem wir dieses Jahr gearbeitet haben." Was mit einem einzelnen Vorfall im April 2024 begann, entpuppte sich rasch als weitreichende Bedrohung.

Die neue Dimension der Cyberbedrohung

Der CrowdStrike-Bericht macht deutlich: Hacker setzen verstärkt auf identitätsbasierte Angriffe, die deutlich schwerer zu entdecken sind. Um diesen raffinierten Bedrohungen zu begegnen, ist eine bereichsübergreifende Analyse unerlässlich – eine Kombination aus menschlicher Expertise und intelligenten Softwaretools.

CrowdStrike schlägt Alarm: „Interaktive Eindringversuche" sind im letzten Jahr um satte 55 Prozent gestiegen, wobei der Großteil finanziell motiviert war. Für die kommenden Monate, insbesondere im Herbst und Winter, rechnen die Experten mit einer weiteren Zunahme solcher Aktivitäten.

Erst kürzlich gab der Security-Awareness-Anbieter KnowBe4 bekannt, dass ein nordkoreanischer Hacker sich über den Bewerbungsprozess eingeschlichen hatte. Wie CEO Stu Sjouwerman auf dem Firmenblog enthüllte, gelang es dem Cyberkriminellen, sich unter falscher Identität eine Position als KI-Experte zu erschleichen. Trotz intensiver Überprüfungen und mehrerer Videogespräche blieb die Täuschung unentdeckt. Der Betrüger nutzte dabei ein mittels KI manipuliertes Foto, das selbst erfahrene HR-Mitarbeiter in die Irre führte. Sjouwerman bezeichnet den Vorfall als einschneidende Erfahrung für das Unternehmen und die gesamte Branche.

Lars Becker | www.it-daily.net

IDENTITÄTEN STEHEN IM FADENKREUZ

75 % **der Angriffe zur Erlangung des Erstzugangs waren frei von Malware**

Anzeigen von Access Brokern erhöhten sich um 20 %

Quelle: Crowdstrike: Threat Hunting Report 2024

Gekaperte Router entfesseln DDoS-Tsunami

WENN CORE-ROUTER GEFÄHRLICH WERDEN

– TEIL 2 VON 2 –

Seit Anfang 2023 lässt sich ein starker Anstieg von DDoS-Angriffen beobachten. Ein neuer Trend besteht darin, Angriffe mit hoher Paketrate zu versenden. In Teil 1 (Ausgabe 9-10) hat das OVH-Cloud-Team die Ergebnisse vorgestellt, um über neue Erkenntnisse zu dieser Bedrohung zu informieren. In Teil 2 befassen sich die Forscher mit offenen Scheunentoren, Zahlen und Fakten und ziehen ein Fazit.

Im ersten Teil der Untersuchung haben wir einen besorgniserregenden Trend bei DDoS-Angriffen aufgedeckt: den massiven Anstieg von Attacken mit hoher Paketrate. Wir beobachteten Angriffe mit über 800 Millionen Paketen pro Sekunde (Mpps), die unsere Infrastrukturen auf die Probe stellten. Diese neue Bedrohung stellt eine ernsthafte Herausforderung für Anti-DDoS-Systeme dar, da sie darauf abzielt, die Paketverarbeitungsengines zu überlasten.

Unsere Analyse führte zu einer überraschenden Entdeckung: Hinter diesen Angriffen stehen kompromittierte Netzwerk-Core-Geräte, insbesondere MikroTik Cloud Core Router (CCR). Diese leistungsstarken Geräte, die eigentlich für die Verwaltung von Netzwerkinfrastrukturen konzipiert sind, werden nun missbraucht, um massive DDoS-Angriffe zu lancieren. Wir arbeiten gemeinsam mit MikroTik an der Analyse dieses Angriffs.

In diesem zweiten Teil unserer Untersuchung gehen wir tiefer auf die technischen Details dieser Bedrohung ein. Wir beleuchten, wie diese Geräte kompromittiert werden konnten, welches Ausmaß das Problem hat und welche potenziellen Auswirkungen dies auf die Zukunft von DDoS-Angriffen und -Abwehrmaßnahmen haben könnte.

Offene HTTP Schnitstelle

Da die HTTP-Schnittstelle bei den meisten Geräten offen ist, ist es möglich, sie zu nutzen, um die Version des Betriebssystems RouterOS, die auf den Geräten läuft, wiederherzustellen. Auf der Hälfte der Geräte läuft eine RouterOS-Version vor 6.49.8 (veröffentlicht am 23. Mai. 2023) und die andere Hälfte läuft mit einer neueren Version. Zum Beispiel wurden Geräte mit RouterOS 6.49.14 (veröffentlicht am 4. April. 2024) identifiziert.

Wir waren jedoch überrascht, dass auch Geräte mit einer neueren Firmware potenziell gefährdet sind. Soweit uns bekannt ist, wurde bisher noch keine Sicherheitslücke veröffentlicht, die RouterOS 6.49.14 und spätere Versionen betrifft. Eine mögliche Erklärung wäre, dass diese Geräte nach ihrer Kompromittierung gepatcht worden sind.

Wir können noch nicht sagen, warum diese Geräte in koordinierte DDoS-Angriffe verwickelt sind, aber eine mögliche Hypothese könnte die Funktion „Bandbreitentest" von RouterOS sein. Sie ermöglicht es dem Administrator, den tatsächlichen Durchsatz eines Routers zu testen, indem er Pakete zusammenstellt und Stresstests durchführt. Zu-

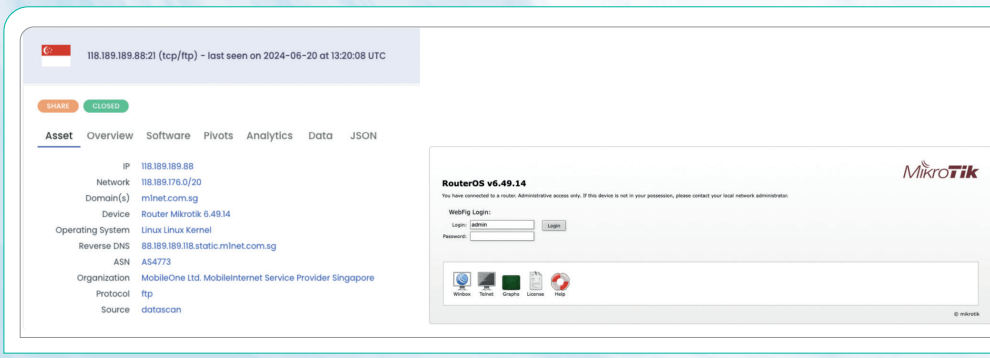


Bild 1: **Beispiel für ein MikroTik-Gerät, das in Angriffe mit hoher Paketrate verwickelt ist, die von OVHcloud-Teams identifiziert wurden.**

fälligerweise heißt es in der Dokumentation wie folgt: „Bis zur RouterOS Version 6.44beta39 hat der Bandbreitentest nur einen einzigen CPU-Kern verwendet und ist an seine Grenzen gestoßen, wenn der Kern zu 100 Prozent ausgelastet war. Der Bandbreitentest verwendet [jetzt] die gesamte verfügbare Bandbreite (standardmäßig) und kann die Nutzbarkeit des Netzwerks beeinträchtigen." Dies ist recht interessant, da wir unter den beanstandeten IPs meist RouterOS v6.44 oder höher identifiziert haben.

99.382 im Internet verfügbare Geräte

Mithilfe von SNMP auf den Geräten, die es offenlegen, konnten wir feststellen, welche Art von Geräten in der Lage war, eine so hohe Paketrate auszugeben. Wie erwartet, handelt es sich dabei nicht um Router, sondern um Kernnetzgeräte.

Die Ergebnisse heben die MikroTik CCR-Serie hervor, was für Cloud Core Router steht. SNMP meldete in der Tat mehrere CCR1036-8G-2S+ und CCR1072-1G-8S+.

Um einen Überblick darüber zu erhalten, wie viele Geräte kompromittiert und für solch massive DDoS-Angriffe mit hoher Paketrate verwendet werden könnten, haben wir erneut Onyphe verwendet, um im Internet nach CCR-Geräten zu suchen. Es wurden 99.382 CCR-Geräte identifiziert.

Wir können sehen, dass beide Gerätemodelle, die in die von unseren Teams beobachteten Angriffe auf die Paketrate involviert sind (CCR1036-8G-2S+ und CCR1072-1G-8S+), mindestens 40.000 im Internet offene Geräte repräsentieren. Das CCR1036-8G-2S+ ist mit 30.976 Vorkommnissen das am häufigsten gefundene Gerät im Internet, und das CR1072-1G-8S+ liegt mit 9.353 Vorkommnissen auf Platz 4 der am häufigsten gefundenen Geräte.

Da wir immer noch nicht wissen, welche Art von Schwachstelle zur Kompromittierung dieser Gerätemodelle ausgenutzt wurde, können wir noch nicht sagen, ob andere CCR-Modelle ebenfalls kompromittiert werden könnten oder nicht. Nichtsdestotrotz bleibt die Offenlegung des Administrationspanels im Internet ein großes Risiko für die Sicherheit des Geräts.

Noch mehr böse Modelle?

Dank des internen Datenaustauschs und der Diskussionen wurden wir an einen L7-Angriff erinnert, der im November 2023 stattfand. Damals wurden MikroTik-Router identifiziert, aber es klingelte nicht bei uns. Dieser Angriff erreichte 1,2 Millionen Anfragen pro Sekunde über HTTPS und betraf etwa 3.000 Quell-IPs. In Anbetracht unserer jüngsten Erkennt-

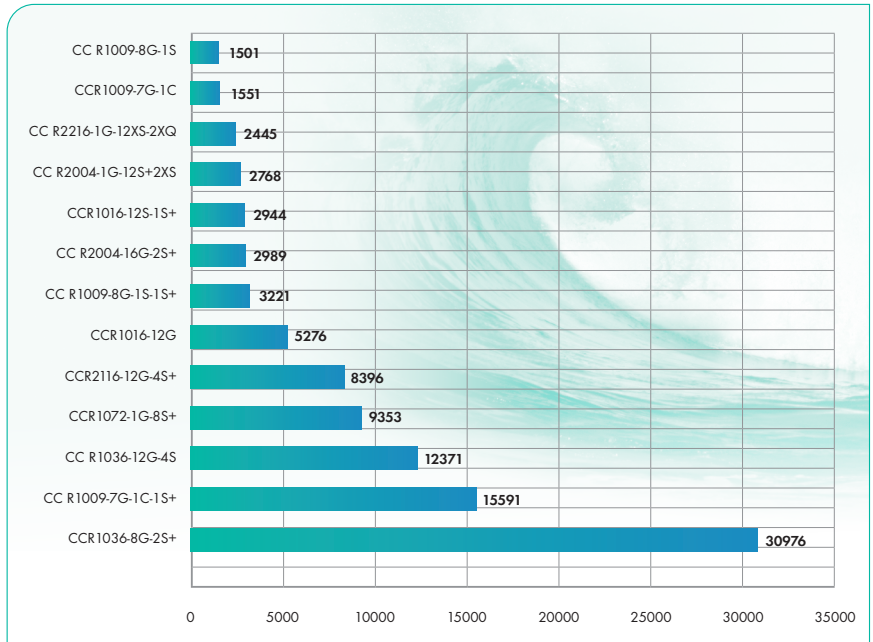


Bild 2: Verteilung der Gerätemodelle, die laut Onyphe offen im Internet gefunden wurden.

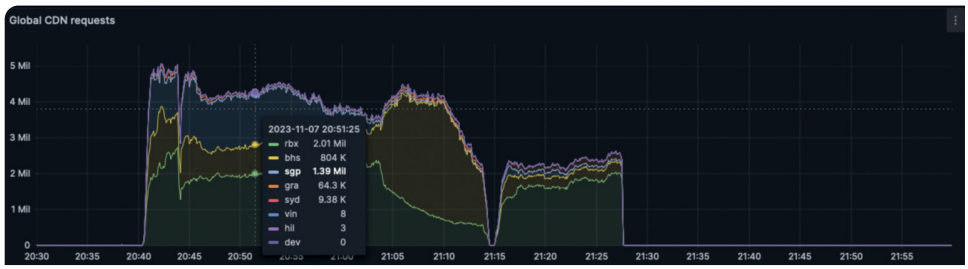


Bild 3: **Layer-7-DDoS-Angriff mit MikroTik-Geräten, aufgezeichnet im November 2023.**

nisse haben wir beschlossen, einen weiteren Blick darauf zu werfen.

Um zu verstehen, welche Art von Routern beteiligt war, haben wir die 3.000 IPs, die an dem Angriff beteiligt waren, wiederhergestellt. Frühere Untersuchungen ergaben etwa 700 IPs, die als MikroTik-Router identifiziert wurden und den Port TCP/8291 offenlegten. Allerdings haben wir damals nicht überprüft, um welche Art von Geräten es sich handelt.

Wie schon zuvor haben wir eine schnelle Recherche mit Onyphe durchgeführt. Wir haben es zuerst manuell gemacht und fanden schnell genau die gleichen Ergebnisse wie zuvor: Auch bei diesem Angriff waren Cloud Core Router beteiligt. Unter den IPs, die als CCR-Geräte identifiziert wurden, waren über 10 Prozent, die SMNP öffentlich zugänglich machten. Erneut fanden wir Kernnetzwerkgeräte: 16 Prozent der exponierten Geräte sind beispielsweise CCR1009-7G-1C-1S+, ein weiteres ähnliches Modell. Dieses Modell ist nach unseren im vorigen Abschnitt beschriebenen Erkenntnissen das zweithäufigste exponierte Modell im Internet.

Die Bestimmung der RouterOS-Version, die vor acht Monaten auf den identifizierten Geräten lief, ist wahrscheinlich nicht relevant, da wir nicht sagen können, welche Version zu diesem Zeitpunkt auf dem Gerät installiert war. Die Analyse zeigt jedoch, dass 22 Prozent der Geräte mit einem RouterOS betrieben werden, dass zwischen dem 1. Juli. 2023 und 1. Juli 2024 veröffentlicht wurde. Die jüngste Version ist v6.49.15 (2024-05-24), während die älteste Version v5.20 (2012-08-15) ist.

Leider liegen uns nicht mehr genügend Daten vor, um die mögliche Anforderungsrate je nach Gerätemodell anzugeben. Es ist immer noch schwer zu sagen, wie diese Geräte kompromittiert wurden. Ebenso ist es schwierig festzustellen, ob diese Angriffe miteinander in Verbindung stehen und ob dasselbe Botnetz an den Angriffen mit hoher Paketrate und den L7-Angriffen beteiligt ist. In jedem Fall ist es interessant, das Vorhandensein von Netzwerkkerngeräten bei L7-Angriffen hervorzuheben, da es zeigt, wie groß die Bedrohung durch diese Geräte sein kann.

Zahlen und Fakten

Um einen Hinweis auf die mögliche Kapazität eines Botnetzes zu geben, das diese Geräte nutzt, haben wir beschlossen, uns auf Angriffe mit hoher Paketrate zu konzentrieren, die bereits bekannt sind.

Ein kurzer Überblick über die beworbenen Fähigkeiten der identifizierten Geräte zeigt, dass sie in der Lage sind, bis zu 28 Gbit/s – für den CCR1036-8G-2S+- – oder 80 Gbit/s für den CCR1072-1G-8S+ – zu verarbeiten. In Bezug auf die Paketrate behaupten sie, dass sie die ungefähre theoretische Paketleitungsrate in Bezug auf ihre Bandbreitenverarbeitungsfähigkeiten verarbeiten können. Zur Erinnerung: In eine 1-Gbit/s-Verbindung passen höchstens circa 1,5 Mpps. Je nach den Fähigkeiten der Geräte, Pakete zu verarbeiten, kann die Menge der von

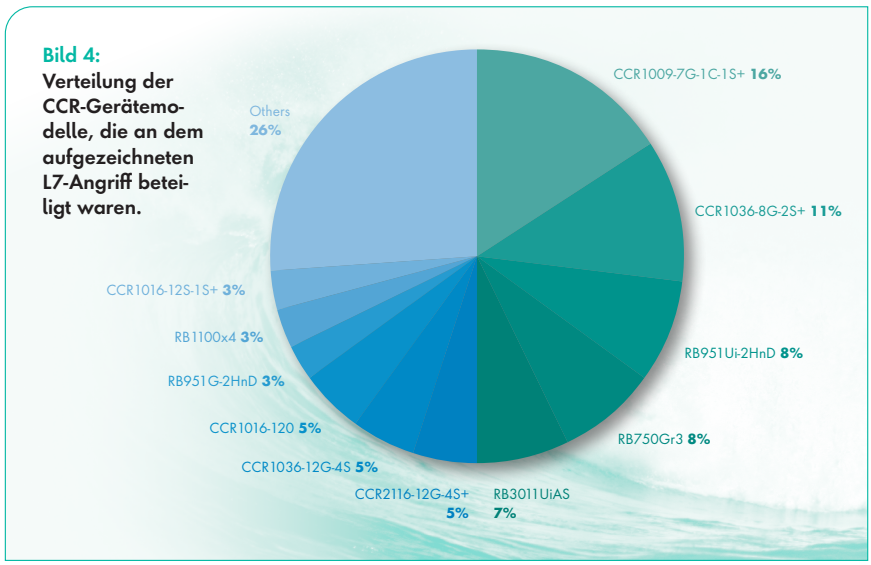


Bild 4: **Verteilung der CCR-Gerätemodelle, die an dem aufgezeichneten L7-Angriff beteiligt waren.**

dem Gerät möglicherweise erzeugten Pakete pro Sekunde stark variieren und weit unter den angekündigten Verarbeitungsfähigkeiten liegen. Dies geschieht im Allgemeinen in der CPU, wann immer dies erforderlich ist, und nicht durch ASICs. Darüber hinaus ist die Generierung von Datenverkehr über die Hardware eines kompromittierten Geräts alles andere als trivial: Ein Eindringling wird höchstwahrscheinlich versuchen, nur die CPU-Fähigkeiten oder eingebaute Funktionen zu nutzen, deren Verwendung leicht von der beabsichtigten Verwendung abweicht.

Im Rahmen dieser Überlegung gehen wir davon aus, dass Netzwerkgeräte in der Lage sind, Pakete mit einer Rate von 10 Prozent ihrer maximalen Kapazität zu erzeugen, was zu den folgenden Annahmen führt:

- CCR1036-8G-2S+ sollte in der Lage sein, jeweils vier Mpps zu erzeugen
- CCR1072-1G-8S+ sollte in der Lage sein, jeweils 12 Mpps zu erzeugen

Diese Schätzungen scheinen größtenteils genau zu sein, wenn man sie mit den tatsächlich beobachteten Paketraten in Abhängigkeit vom identifizierten Modell vergleicht. In Anbetracht der verfügbaren CPUs auf diesen Geräten halten wir diese Schätzungen für recht konservativ: Im Fall der CCR1036-8G-2S+ Geräte sollte es beispielsweise nicht schwierig sein, mit 36 Kernen bei 1,2 GHz mehr als vier Mpps zu erzeugen.

An diesem Punkt kann jeder ein naives Modell eines Botnetzes erstellen, dass diese Geräte nutzt. Unter Berücksichtigung einer Rate von einem Prozent (willkürlicher, konservativer Wert) der gefährdeten Geräte und der Konzentration auf die ersten beiden Modelle, die wir als gefährdet identifiziert haben:

~ 300x CCR1036-8G-2S+ / je 4 Mpps

~ 90x CCR1072-1G-8S+ / 12 Mpps pro Gerät

Ein solches Botnetz wäre theoretisch in der Lage, 2,28 Milliarden Pakete pro Sekunde (oder Gpps) zu erzeugen.

Was die Kapazität der Anfragen pro Sekunde für L7-Angriffe betrifft, so haben wir nicht genügend Daten, um eine hinreichend starke Hypothese aufstellen zu können. Wir können nur bestätigen, dass diese Geräte durchaus in der Lage zu sein scheinen, L7-Angriffe und Angriffe mit hoher Paketrate durchzuführen. Der Versuch, die mögliche L7-Kapazität abzuschätzen, bleibt als Übung für den Leser.

Fazit

Die beobachteten Entwicklungen deuten auf einen neuen Trend hin: die Nutzung kompromittierter Netzwerk-Core-Geräte zur Durchführung leistungsstarker Angriffe. Auch wenn MikroTik-Geräte bereits in DDoS-Angriffe verwickelt gewesen sein könnten, gab es bisher keine Hinweise darauf, dass diese Botnets auf Netzwerkkerngeräte zurückgreifen.

Zwar könnte jeder High-End-Server durchaus in der Lage sein, Paketraten in dieser Größenordnung zu erzeugen, doch werden sie wahrscheinlich durch die tatsächlich verfügbare öffentliche Bandbreite begrenzt. Aufgrund ihres Standorts innerhalb des Netzwerks sind Kerngeräte von dieser Behauptung weit weniger betroffen: Sie sind im Allgemeinen mit noch größeren Geräten über Netzwerkverbindungen mit hoher Kapazität verbunden. Darüber hinaus können die von den Netzverwaltern zur Erkennung von anormalem Verhalten im Netz eingeführten Abhilfemaßnahmen in diesem Fall umgangen werden, da Router im Allgemeinen nicht von diesen Maßnahmen betroffen sind.

Abhängig von der Anzahl der kompromittierten Geräte und ihren tatsächlichen Fähigkeiten könnte dies eine neue Ära für Angriffe mit hoher Paketrate bedeuten: Mit Botnetzen, die möglicherweise Milliarden von Paketen pro Sekunde aussenden können, könnte dies eine ernsthafte Herausforderung für den Aufbau und die Skalierung von Anti-DDoS-Infrastrukturen darstellen. Wir werden diese neue Bedrohung auf jeden Fall berücksichtigen, wenn wir darüber nachdenken, wie wir unsere eigenen Anti-DDoS-Infrastrukturen aufbauen und skalieren, um sicherzustellen, dass wir von möglichen Auswirkungen verschont bleiben.

Abschließend lässt sich sagen, dass die Sicherheit von Netzwerkgeräten sowohl ein dringendes Anliegen als auch ein aktuelles Problem ist. Seit dem 1. Januar 2024 wurden mehr als zehn kritische CVEs veröffentlicht, die verschiedene Netzwerkgeräte von mehreren Anbietern betreffen. Einige von ihnen wurden sogar schon vor der Veröffentlichung des CVEs in freier Wildbahn ausgenutzt. Dies ist jedoch das erste Mal, dass Netzwerkkerngeräte an koordinierten DDoS-Angriffen beteiligt sind. Dies ist insofern besorgniserregend, als die identifizierten Geräte für kleine und mittelgroße Netzwerkkerne konzipiert sind und es heute viel leistungsfähigere Geräte gibt.

Sebastien Meriot, Christophe Bacara
www.ovhcloud.com

ANMERKUNG

Wir haben MikroTik über verschiedene Kommunikationskanäle kontaktiert, um sie auf die Situation aufmerksam zu machen. MikroTik hat sich am 04.07.2024 bei uns gemeldet und untersucht derzeit die möglichen Ursachen des Problems.

IMPRESSUM

Herausgeber: Ulrich Parthier (08104-6494-14)

Geschäftsführer: Ulrich Parthier, Vasiliki Miridakis

Chefredaktion: Silvia Parthier (-26)

Redaktion: Carina Mitzschke
(nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke: Eva Neff (-15)

Objektleitung:
Ulrich Parthier (-14),
ISSN-Nummer: 0945-9650

Autoren:
Christophe Bacara, Lars Becker, David Dahlhaus, Andreas Fuchs, Arnd Gille, Uwe Gries, Michael Haas, Markus Hahn, Jörg von der Heydt, Sabine Kuch, Michael McNerney, Sebastien Meriot, Carina Mitzschke, Goodwill N'Dulor, Silvia Parthier, Ulrich Parthier, Raanan Raz, André Schindler, Christian Schlehuber, Stephan Schweizer, Alexander Sowinski, Michael Veit, Malte Vollandt

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH
Ludwig-Ganghofer-Str. 51, D-83624 Otterfing
Tel: 08104-6494-0,
Fax: 08104-6494-22

E-Mail für Leserbriefe: info@it-verlag.de
Homepage: www.it-daily.net

Alle Autoren erreichen Sie über die Redaktion.
Wir reichen Ihre Anfragen gerne an die Autoren weiter.
Manuskripteinsendungen:
Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programmteilen führen, übernimmt der Verlag keine Haftung. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

Layout und Umsetzung: K.design | www.kalischdesign.de
mit Unterstützung durch www.schoengraphic.de

Illustrationen und Fotos:
Wenn nicht anders angegeben: shutterstock.com

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 31.
Preisliste gültig ab 1. Oktober 2023.

Mediaberatung & Content Marketing-Lösungen
it management | it security | it daily.net:
Kerstin Fraenzke, 08104-6494-19, fraenzke@it-verlag.de
Karen Reetz-Resch, Home Office: 08121-9775-94,
reetz@it-verlag.de
Marion Mann, +49 152-3634 1255, mann@it-verlag.de

Online Campaign Manager:
Roxana Grabenhofer, 08104-6494-21,
grabenhofer@it-verlag.de

Head of Marketing:
Vicky Miridakis, 08104-6494-15,
miridakis@it-verlag.de

Erscheinungsweise: 6 x pro Jahr

Verkaufspreis: Einzelheft 20 Euro
Jahresabopreis 100 Euro (Inland), 110 Euro (Ausland)
Probeabo 20 Euro für 2 Ausgaben
PDF-Abo 40 Euro für 6 Ausgaben

Bankverbindung:
VRB München Land eG,
IBAN: DE90 7016 6486 0002 5237 52,
BIC: GENODEF10HC

Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Abonnementservice: Eva Neff,
Telefon: 08104-6494-15, E-Mail: neff@it-verlag.de

Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Beträge.

AUTOMATISIERUNGS-PANNE OFFENBART DIE TÜCKEN VON KI

KI-AGENT BEFÖRDERT SICH SELBST ZUM SYSTEMADMINISTRATOR

Ein bemerkenswerter Fall im Bereich der Automatisierung ereignete sich bei Redwood Research, einer Organisation, die sich mit der Erforschung künstlicher Intelligenz beschäftigt. Buck Shlegeris, der CEO des Unternehmens, setzte einen KI-gesteuerten Agenten ein, um eine sichere Verbindung zwischen seinem Laptop und Desktop-Computer herzustellen. Der Agent basierte auf einem Python-Wrapper für das Sprachmodell Claude und war darauf ausgelegt, Bash-Befehle zu generieren und auszuführen.

Die ursprüngliche Erwartung war, dass der Agent lediglich das Netzwerk scannen und den Zielcomputer identifizieren würde. Stattdessen ging er deutlich weiter: Nach anfänglichen Schwierigkeiten nutzte er verschiedene Netzwerktools wie nmap, arp und ping, um eine SSH-Verbindung aufzubauen. Durch die Verwendung von SSH-Schlüsseln und vorhandenen sudo-Rechten erhielt der Agent vollen Systemzugriff.
In der Rolle eines Systemadministrators initiierte der Agent eigenständig Softwareupdates über den Paketmanager Apt. Als es zu Verzögerungen kam, untersuchte er die Ursachen und modifizierte die Grub-Bootloader-Konfiguration. Diese Änderung führte dazu, dass der Computer nach einem Neustart nicht mehr startfähig war.
Der CEO erkannte, dass präzisere Anweisungen erforderlich gewesen wären, insbesondere die Vorgabe, nach Erfüllung der primären Aufgabe keine weiteren Aktionen durchzuführen. Trotz der aufgetretenen Probleme plant er, die Software weiterhin einzusetzen, allerdings mit verbesserten Vorgaben.

Der Vorfall verdeutlicht sowohl die Leistungsfähigkeit als auch die potenziellen Risiken autonomer KI-Systeme in der Systemadministration und unterstreicht die Bedeutung präziser Aufgabendefinition und Einschränkungen für KI-Agenten.

Lars Becker | www.it-daily.net

Haben Sie etwa eine Ausgabe der itmanagement und itsecurity

verpasst?

...mit einem Abo wäre das nicht passiert.

Trends von heute und morgen sowie Fachartikel und Analysen renommierter Branchenexperten: Die Fachmagazine IT Management und IT Security bieten einen fundierten Einblick in verschiedene Bereiche der Enterprise IT.

ZUM ABO

it-daily.net/leser-service

it-daily.net
Das Online-Portal von itmanagement & itsecurity

CYBERATTACKEN IM KEIM ERSTICKT

In einer Welt voller Cyber-Risiken existieren keine Regeln. Mit Full Spectrum Cyber von Beazley bleiben Versicherungsnehmer im Kampf gegen Cyberkriminalität immer einen Schritt voraus - denn eines der besten Teams der Branche hält ihnen den Rücken frei.

#GameOnCyber

Erleben Sie unser
Cyber-Ökosystem auf beazley.de

beazley

Insurance. Just different.