itmanagement
DEZEMBER 2020

INKLUSIVE 32 SEITEN
IT SECURITY

COLLABORATION, NEW WORK UND HOMEOFFICE

SEAMLESS OFFICE

Dr. Eric Schott, Campana & Schott

REIFEGRADMODELLE

Cybersicherheit olé

ITIL 4 UND ITSM

Möglichkeiten zur Verbesserung

Drittwartung im Rechenzentrum **ab Seite 18**

www.it-daily.net


ZUHAUSE
ARBEITEN,
WIE IM BÜRO.
Mit dem HomeOffice der Telekom.
Alles aus einer Hand.
Jetzt online konfigurieren:
telekom.de/homeoffice
ERLEBEN, WAS VERBINDET.

HOME-OFFICE? HOME-OFFICE!

In Zeiten der permanenten Erreichbarkeit, wird man auch permanent mit Mitteilungen zugemüllt, die man weder haben will, noch braucht. Corona- und US-Wahl-bedingt nimmt dieser Zustand leider weiter zu. Ein solches Beispiel landete kürzlich in meiner Inbox:

„Gleichzeitig Home-Officing, Home-Schooling, Home-Haushalting und Home-Bespaßungsclowning. Ergibt Home-Nervenzusammbruching!"

Zuerst musste ich darüber schmunzeln, danach fand ich es total übertrieben und dann dachte ich, dass könnte eine gute Einleitung zum Thema New Work im neuen Editorial werden. Ich beging den Fehler und suchte diesen Satz im World Wide Web, mit der kleinen Hoffnung interessante Infos zum Thema Home-Office zu finden – das war idiotisch! Stattdessen landete ich in einer Grundsatzdiskussion darüber, dass die Mütter beziehungsweise Eltern, es früher leichter hatten (weil der Mann arbeiten musste, während sich die Mutter „nur" um Haushalt und Kinder kümmerte) oder, dass die Mütter es früher schwerer hatten (weil die Mutter nebenbei auch auf dem Hof helfen musste).

Nun, wie bekomme ich jetzt die Kurve zu New Work und Home-Office? Schwierig, aber abgesehen davon, dass die Situation so ist, wie sie ist und man das Beste draus machen sollte – auch wenn das oft leichter gesagt als getan ist – hat man heute eine unendliche Zahl an Anwendungen, Tools und Möglichkeiten, die die Arbeit zumindest im Home-Office erleichtern und unterstützen können. Sowohl unsere aktuelle Coverstory, als auch drei weitere Artikel dieser Ausgabe widmen sich diesem Thema und zeigen auf, welchen Nutzen man aus schwierigen Bedingungen ziehen kann.

Daher, Nerven behalten und positiv bleiben.

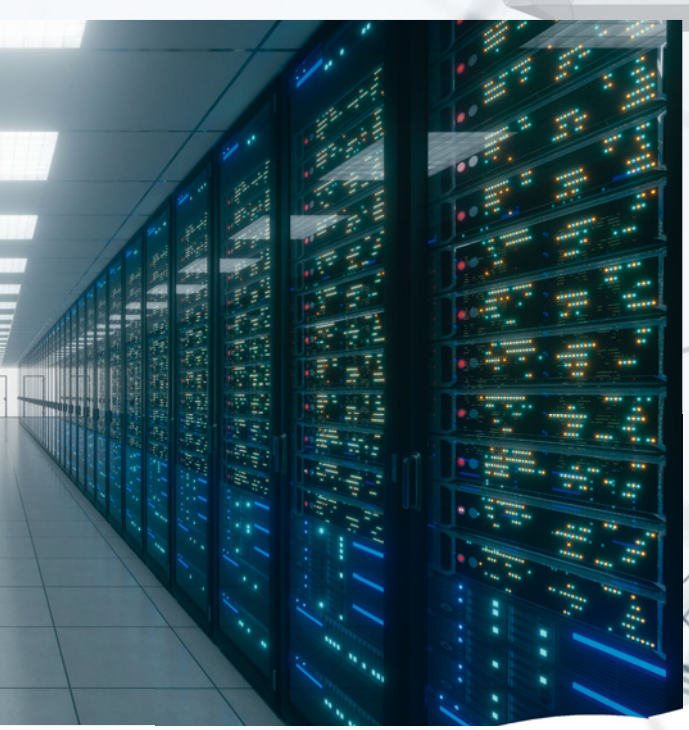
Carina Mitzschke | Redakteurin it management

24

COVERSTORY

INHALT

16



30

Inklusive 32 Seiten

IT SECURITY SPEZIAL

DATA DISCOVERY

WERTVOLLE DATEN IM BLICK

Durch die steigende Cloud-Nutzung, Remote-Arbeit und Interkonnektivität der Geschäftsprozesse werden sensible Daten heutzutage in einer Vielzahl von Systemen, Anwendungen und Datenbanken gespeichert, was ihren Schutz zu einer Herausforderung macht. Um Daten effektiv vor Verlust und Diebstahl schützen zu können, muss ein Unternehmen nicht nur wissen, welche Daten es besitzt, sondern auch, wo sie gespeichert sind, wer Zugang zu ihnen hat, wo auf sie zugegriffen wird und wie sie übertragen werden.

Als einer der größten Business-Intelligence-Trends der letzten Jahre stellt die Data Discovery deshalb eine entscheidende Komponente der Datensicherheit und Compliance dar. Data Discovery ermöglicht es, sensible und gesetzlich regulierte Daten eines Unternehmens umfassend zu identifizieren und zu lokalisieren, um sie angemessen zu sichern oder zuverlässig zu entfernen.

Data Discovery lässt sich allgemein in fünf Schritte gliedern:

1. **Daten sammeln:** Es müssen sowohl sensible als auch nicht-sensible Daten gesammelt werden und leicht einsehbar sein. Um die Einhaltung von gesetzlichen Vorschriften zu gewährleisten, sollte der Standort der gesammelten Informationen so weit wie möglich zusammengefasst und dokumentiert werden.

2. **Datenanalyse:** Sobald sich alle Daten in einer überschaubaren Umgebung befinden, werden sie analysiert. Hierbei ist es wichtig, die sensiblen Daten und die notwendigen, aber nicht-sensiblen Daten zu trennen. Unternehmen bestimmen auch, welche Daten sie aufgrund gesetzlicher Vorschriften oder für Geschäftszwecke aufbewahren müssen und welche Daten verworfen werden können.

3. **Datenbereinigung:** Alle unnötigen Daten sollten bereinigt werden. Es sollte generell eine Richtlinie für die Bereinigung von Daten festgelegt werden, sobald sie nicht mehr erforderlich sind.

4. **Daten schützen:** Alle Daten sollten daraufhin angemessen geschützt werden. Dieser Schutz sollte sowohl physisch (Aufbewahrung der Daten in einem verschlossenen Schrank oder Raum) als auch digital (mit einer Firewall, Verschlüsselung) erfolgen.

5. **Daten nutzen:** Aus den entdeckten Daten können schließlich Erkenntnisse zur Verbesserung von Geschäftsabläufen und anderen Unternehmensprozessen gewonnen werden.

Unternehmen erstellen heute Daten in noch nie dagewesener Geschwindigkeit. Data Discovery ermöglicht es Unternehmen, das vollständige Datenbild angemessen zu bewerten und die entsprechenden Sicherheitsmaßnahmen zu implementieren, um mögliche Datenverluste zu verhindern.

www.digitalguardian.com

SCHWACHSTELLEN-MANAGEMENT

ENTSCHEIDENDE RISIKOMINIMIERUNG

Schwachstellenmanagement hilft, Software-Lecks auf Endpoints zu erkennen und abzudichten. Viele Unternehmen verzichten jedoch auf den Einsatz, weil sie die Lösungen für zu teuer oder schlicht überflüssig halten – schließlich wird regelmäßig manuell gepatcht. Dies ist allerdings eine Fehleinschätzung.

Vier Mythen

1. Wer regelmäßig patcht, braucht kein Schwachstellenmanagement

Mit der wachsenden Zahl an Endpoints im Unternehmen, steigt auch der Verwaltungsaufwand. Ein Schwachstellenmanagement sorgt dafür, dass kein System übersehen wird, und verteilt automatisiert die verfügbaren Patches und Fixes.

2. Schwachstellenmanagement ist teuer und belastet die Infrastruktur

Zwar fallen für die Anschaffung und Einführung Kosten an, doch langfristig entlasten die Lösungen das IT-Budget sogar. Durch automatisierte Prüfungen der Endpoints und automatische Patch-Verteilung werden Mitarbeitern viele manuelle Tätigkeiten abgenommen.

3. Auf Remote-Arbeitsplätzen ist Schwachstellenmanagement schwer umsetzbar

Auch wenn sich Endpoints außerhalb der Unternehmensinfrastruktur befinden, hält sie ein modernes Schwachstellenmanagement auf dem aktuellen Patch-Level.

4. Ein Schwachstellentest ist ein Test, den man bestehen kann

Ein Schwachstellen-Scan liefert nur eine Momentaufnahme. IT-Verantwortliche müssen Schwachstellenmanagement daher als Prozess betrachten, der regelmäßige Scans und kontinuierliche Verbesserungen an Prüfroutinen erfordert.

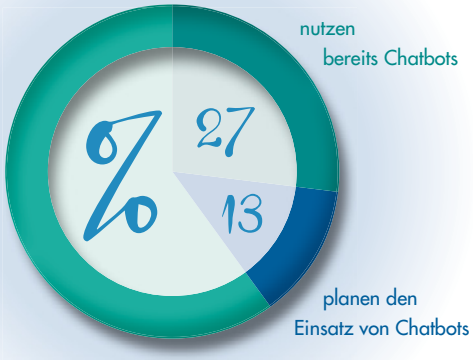
https://insights.adaptiva.com

CHATBOTS

JEDES VIERTE UNTERNEHMEN NUTZT SIE

Wie kann ich ein Produkt bestellen? Welche Fristen gelten bei einer Stornierung? Solche Anfragen von Kunden und Geschäftspartnern beantwortet mittlerweile mehr als jedes vierte Unternehmen in Deutschland (27 Prozent) per Chatbot. Weitere 13 Prozent planen den Einsatz dieser kleinen Programme, die einfache Fragen beantworten können und sogar ständig und selbständig dazulernen. Das ist das Ergebnis einer Befragung, die der Digitalverband Bitkom durchgeführt hat. Im Zuge der Digitalisierung von Prozessen wird die Nutzung von Chatbots weiter ausgebaut. Neue technische Möglichkeiten entwickeln die automatisierte Kommunikation mit dem Kunden und ermöglichen so mehr Effizienz für das Unternehmen.

www.bitkom.org



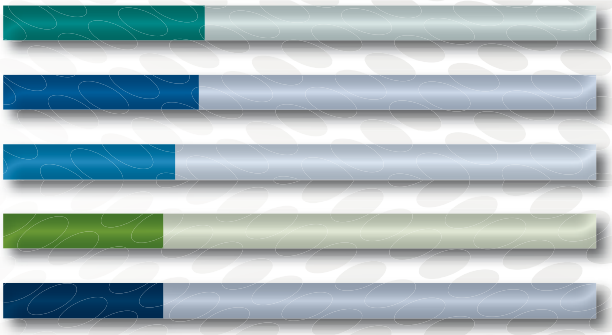
ERFOLGREICHE DEVOPS

PASSENDE RAHMENBEDINGUNG UND INTERNE UNTERSTÜTZUNG

DevOps markieren aktuell die Spitze in der Evolution der Anwendungsprogrammierung. Für die agile Entwicklung einer modernen, wettbewerbsfähigen Applikationslandschaft mit Cloud-nativen Apps hat sich die Methodik in der Branche absolut bewährt. Wie beliebt und verbreitet sie sind, zeigt eine Untersuchung von Consol: Bereits knapp 80 Prozent der befragten Unternehmen nutzen bereits DevOps. Doch die Studie zeigt auch, dass Entwickler und Unternehmen vor einer ganzen Reihe technischer und organisatorischer Herausforderungen stehen.

www.consol.de

DIE GRÖSSTEN HERAUSFORDERUNGEN BEI DER UMSETZUNG VON DEVOPS (MEHRFACHNENNUNGEN MÖGLICH)



34% IT-Kultur und Beharrungsvermögen

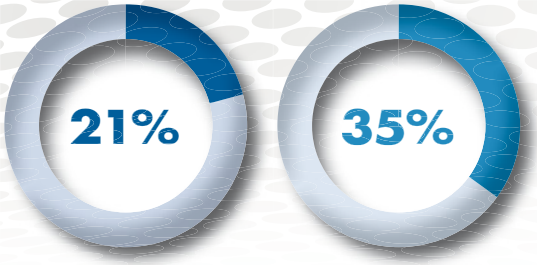
33% Integration von Anwendungsentwicklung und IT-Operations

29% Reife der Tools und der Anwendungen

27% Festlegen und Beschließen gemeinsamer KPIs

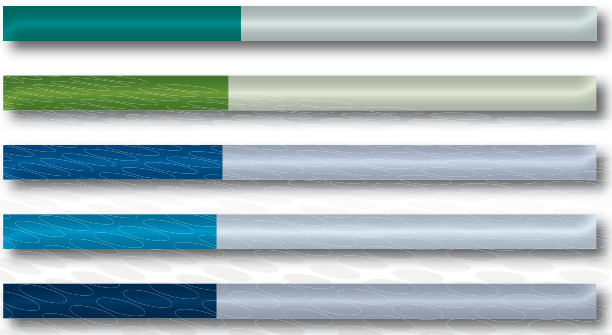
27% Fehlendes Budget

Erst 21 Prozent der Unternehmen haben DevOps-Teams inklusive Business-Stakeholdern gebildet, um die Zusammenarbeit in der Entwicklung zu fördern.



Erst in 35 Prozent der Unternehmen wird Security in DevOps-Prozessen abgebildet und Security-Teams aktiv in die App-Entwicklung einbezogen.

DIE WICHTIGSTEN TREIBER ZUR NUTZUNG VON DEVOPS (MEHRFACHNENNUNGEN MÖGLICH)



40% Gesteigerte Agilität

38% Schnellere Modernisierung der IT-Infrastruktur

37% Bessere Kundenzufriedenheit

36% Effizientere Unterstützung von Business-Innovationen

36% Höhere Entwicklungsproduktivität

AGILE TRANSFORMATION

AKTUELLE STUDIENERGEBNISSE

1.
Top-Management fordert zwar Agilität, lebt diese aber noch zu selten tatsächlich vor

2.
Wandel der Unternehmenskultur und der Umbau der Zusammenarbeitsmodelle sind die größten Herausforderungen

3.
Skalierung in Form von Agilen Frameworks ist nächster nötiger Schritt der agilen Transformation

4.
Mittleres Management passt sich immer besser an Agilität an und hat deutlich an Methodenkompetenz gewonnen

www.luenendonk.de

SEAMLESS OFFICE

IM SPANNUNGSFELD ZWISCHEN COLLABORATION, NEW WORK UND HOMEOFFICE

Dr. Eric Schott, CEO der Management- und Technologieberatung Campana & Schott im Gespräch mit Ulrich Parthier, Publisher it management über die Zukunft des Büros, der Arbeit, Projekten und Mitarbeitenden.

> SEAMLESS OFFICE IST EINE KOMBINATION AUS SOFTWARE, DER RICHTIGEN HARDWARE UND SERVICES, DIE MICH IN MEINEM INDIVIDUELLEN ARBEITSVERHALTEN BESTMÖGLICH UNTERSTÜTZEN.
>
> Dr. Eric Schott, Gründer und CEO, Campana & Schott, www.campana-schott.com

Ulrich Parthier: *Nach dem COVID19-Schock im März hieß das Gebot der Stunde für die meisten Arbeitnehmer Homeoffice. Nun kommt die zweite Welle. Hat sie dies und die Wucht persönlich überrascht oder haben Sie dies so erwartet?*

Dr. Eric Schott: Leider nicht unerwartet. Und trotzdem bin ich überrascht, mit welcher Geschwindigkeit die Welle größer wird. Bei uns waren die Mitarbeiter daher die ganze Zeit über im Homeoffice. Nur wo es wirklich erforderlich war und dazu nur auf „Anfrage + Genehmigung" sind bei uns Mitarbeiter im Büro. Aktuell ist das eine Handvoll.

Ulrich Parthier: *Das Homeoffice hat viele Veränderungen mit sich gebracht, positive wie negative. Auf der Sollseite stehen etwa eingeschränkte persönliche Kommunikation und ein sehr begrenzter direkter Kundenkontakt. Wie sehen Sie die Zukunft vor dem Hintergrund der Diskussion um einen gesetzlichen Anspruch für das Homeoffice? Viele Unternehmen haben ja bereits eine Reduktion ihrer Büroflächen ins Auge gefasst.*

Dr. Eric Schott: Wir müssen weiterdenken. Dabei geht es für mich auch weniger um Gesetzesdetails zu einem zugesicherten Homeoffice-Tag alle zwei Wochen. Es geht um die viel fundamentalere Frage: Wie wollen wir in Zukunft arbeiten? Die Arbeitsumgebung und der Wechsel zwischen verschiedenen Arbeitsorten müssen dabei so einfach wie möglich sein. Das ist für mich ein zentraler Baustein, um die Arbeitswelt besser mit Privat- und Familienleben zu vereinbaren.

Gern möchte ich Ihren Punkt der Kundenbeziehung aufgreifen. Für die Zukunft sehe ich Hybrid als das neue Normal! Darin steckt ein riesiges Potenzial für eine „nahtlose" Kundenbeziehung: Regelmäßige digitale Ansprachen und Videosessions kombiniere ich mit persönlichen Treffen vor Ort. Ich selbst praktiziere das schon an vielen Stellen so und bin damit sehr zufrieden. Unter dem Strich wird die Beziehung intensiver und zugleich effektiver, weil ich mehr Austausch habe als früher. Gleichzeitig kann ich so auch organisieren, dass ich zu Hause bin, wenn meine beiden Jungs um halb vier Uhr aus der Schule kommen. Dann haben wir gemeinsam eine Stunde Zeit für Reden, zusammen Tee trinken und nachsehen, ob die Hausaufgaben auch wirklich erledigt sind.

Ulrich Parthier: *Durch die gegenwärtige Situation ist ein neuer Begriff entstanden, das Seamless Office. Was verbirgt sich hinter diesem Begriff?*

Dr. Eric Schott: Bei Büro oder Office denken wir immer an einen Raum. Aber es geht um einen Zustand: Wie werde ich optimal für den Zustand des Arbeitens unterstützt – egal, wo ich gerade bin. Und wenn ich meine Arbeit effektiver erledigen kann, habe ich auch mehr Möglichkeiten für anderes. Seamless Office ist also eine Kombination aus Software und auch der richtigen Hardware und Services, die mich in meinem individuellen Arbeitsverhalten bestmöglich unterstützen. Mit diesem Set wird das Wechseln zwischen Arbeitssituationen deutlich vereinfacht. Mit Collaboration Tools und dem richtigen Mindset, ist es möglich dort zu arbeiten, wo man konzentriert und effizient sein kann. Ein Beispiel: Den Kickoff für ein Projekt mache ich gerne in einem Meeting mit mehreren Köpfen, die konzeptionelle Phase verschiebe ich bewusst in mein Büro zu Hause. Die Abstimmung der Präsentation mit dem Kunden läuft dann über Teams. Ich wähle den für mich passenden Arbeitsmodus – der Standort ist gleichgültig, denn Software und Services unterstützen mich im Hintergrund nahtlos.

Ulrich Parthier: *Neue Organisations- und Sicherheitskonzepte erfordern Zeit und Verständnis bei allen Beteiligten. Wer treibt einen solchen Change?*

Dr. Eric Schott: Den ersten Schritt machen die Führungskräfte. Sie müssen die neuen Arbeitsweisen vorleben, selbst ausprobieren und Freiräume in der Gestaltung des Arbeitstages zulassen. Dabei müssen sie auf die Mitarbeitenden zugehen und gemeinsam individuelle Lösungen besprechen: Wo, wie und wann kann ich selbst am besten arbeiten? Wie finde ich den richtigen Mix aus Kreativität, Effizienz und auch Auszeiten, beispielsweise für Sport?

Ulrich Parthier: *Bei allen Veränderungen hilft, wenn man diese toolbasiert durchführen kann. Sie haben das CS smart Workspace genau für solche Anforderungen entwickelt. Wie sind Sie auf die Idee gekommen?*

Dr. Eric Schott: Wir experimentieren einfach schon immer gerne mit neuen Technologien. Daraufhin entstand eine Lösung zur KI-gestützten Buchung und Optimierung von Büroräumen. Gleich zu Beginn von COVID-19 haben wir diese dann erweitert, um die Arbeitsplätze nach strengen Abstandsregelungen zu vergeben. Zugleich können wir sicherstellen, dass sich nur wenige Mitarbeiter und Besucher in den Räumlichkeiten aufhalten. Mit diesen Erfahrungen ging der CS smartWorkspace dann zu Kunden.

Ulrich Parthier: *Wie ist die Resonanz der Kunden? So sind ja beispielsweise 28 von 30 Dax-Konzernen Ihre Kunden. Soll die Software eher Großkunden oder den Mittelstand ansprechen?*

Dr. Eric Schott: Ein Beispiel: Gerade erst hat die Munich Re die Lösung eingeführt. Sie wollen damit die Nutzung ihrer Büro-Ressourcen optimieren. Im Moment setzen viele Unternehmen und wir selbst den CS smartWorkspace ein, um Infektionsketten schnell nachzuverfolgen, da man weiß, wer im Office gearbeitet hat. Dafür zeigen Großkunden und Mittelstand gleichgroßes Interesse.

Ulrich Parthier: *Es wird ja auch ein Leben nach Corona geben. Wie kann die Software da helfen?*

Dr. Eric Schott: Das CS smartWorkspace ermöglicht das nahtlose Arbeiten, über das wir eben gesprochen haben. Mitarbeitende können schnell und einfach Arbeitsplätze und Meetingräume buchen. An vollen Tagen zeigt einem die Lösung, ob man ins Office gehen sollte oder doch lieber zuhause bleibt, da zu viele Räume bereits belegt sind.

Was mich besonders freut: Viele unserer Kunden erkennen das Potenzial der Ressourcenschonung. Die Senkung von Heiz- und Energiekosten macht die CS smartWorkspace-Lösung von alleine. Die bestehenden Arbeitsplätze werden viel besser genutzt. Neue Büroflächen müssen vielleicht erst gar nicht angemietet oder gebaut werden. Das passt gut zu den Nachhaltigkeitszielen der Unternehmen. Und das passt sehr gut zu meinen Vorstellungen von nachhaltigem Wirtschaften.

Ulrich Parthier: *Dr. Schott, wir danken für das Gespräch!*

INTELLIGENT VERNETZT

DER ARBEITSPLATZ DER ZUKUNFT

Die Arbeitswelt hat sich durch Corona in den vergangenen Monaten grundlegend verändert. Homeoffice und Mobile Working sind nun in fast jedem Unternehmen angekommen und auch die Einstellung dazu hat sich zum Positiven gewandelt. Es hat sich gezeigt, dass digitale Arbeitsmodelle möglich sind und Produktionsziele oft auch ohne direkte Anwesenheit im Unternehmen erreicht werden.

Auch die Mehrzahl der Beschäftigten wünscht sich in Zukunft verstärkt in den heimischen vier Wänden tätig zu sein. Das zeigt die aktuelle Eset Studie 2020 „Quo Vadis, Unternehmen", eine Untersuchung unter Arbeitgebern und Arbeitnehmern zur aktuellen Situation in Bezug auf mobiles Arbeiten. Demnach hoffen 68 Prozent der Arbeitnehmer auch in Zukunft regelmäßig im Homeoffice arbeiten zu können. Ein Drittel möchte einen Tag pro Woche von zu Hause arbeiten oder flexibel entscheiden, ob man ins Büro geht. Die Chancen dafür stehen gut, denn 78 Prozent der deutschen Unternehmen planen auch nach dem Ende der Corona-Krise ihren Mitarbeitern mobiles Arbeiten zu ermöglichen.

Homeoffice und mobiles Arbeiten werden definitiv Teil der neuen, hybriden Arbeitswelt. Diese Entwicklungen fordern vernetzte Lösungen, die Teams standortunabhängige Zusammenarbeit ermöglichen. Dabei ist es besonders wichtig, gleiche Rahmenbedingungen wie im Büro zu schaffen - vom Zugriff auf relevante Dateien über Datensicherheit bis zu Kommunikationstools. Doch wie sehen solche Lösungen für digitale Arbeitsmodelle und den intelligent vernetzten Arbeitsplatz aus? Welche Herausforderungen gibt es dabei? Welche IT-Infrastruktur braucht es in Zukunft? Und welchen Stellenwert haben Security Lösungen und Services im IT-Bereich?

SO GELINGT DX

Erfahren Sie in der kostenlosen Webinar-Reihe „Bit für Bit" von Konica Minolta, wie die digitale Transformation (DX) Ihres Unternehmens gelingt. Entdecken Sie, wie aus den vielen einzelnen Bausteinen das große Ganze der Digitalisierung entsteht und finden Sie die richtige Session als Grundlage für Ihre Unternehmensentscheidungen.

https://bit.ly/3l3CCjD

Digitaler Transformationsprozess

Die Dringlichkeit der digitalen Transformation und des Cloud-Computings in Unternehmen ist in den vergangenen Monaten rasant gestiegen. Diese Veränderungen erfordern zuverlässige Unterstützung in Form von passenden Werkzeugen und entsprechendem Know-how. Damit Mitarbeiter im Homeoffice genauso schnell und effizient arbeiten können wie im Büro, ist eine stabile Netzwerkinfrastruktur mit passenden IT-Lösungen für einen intelligent vernetzten „Digital

Workplace" gefragt. Der Arbeitsplatz daheim muss jederzeit den vollständigen Remote-Zugriff auf geschäftskritische Arbeitsabläufe und Daten ermöglichen. Umfassende Komplettlösungen aus Hardware, Software sowie einer ganzen Bandbreite an Applikationen und Smart Managed Services sind dafür besonders geeignet. Sie vereinfachen Prozesse, automatisieren Arbeitsschritte und fördern die unternehmensweite Zusammenarbeit. Im Fokus stehen dabei die individuellen Bedürfnisse der arbeitenden Menschen. Der intelligente Arbeitsplatz muss Menschen, Arbeitswelten und Informationen einfach und bestmöglich vernetzen.

Von essenzieller Bedeutung ist daher ein zielgerichteter, digitaler Transformationsprozess. Das ist oft eine große Herausforderung für Unternehmen. Die Geschwindigkeit von Unternehmensabläufen ist ein entscheidender Faktor im Wettbewerb, weshalb das moderne Informationsmanagement einen ganz besonderen Stellenwert erhält. Strukturierte Geschäftsprozesse sowie eine sichere IT-Infrastruktur sind von grundlegender Bedeutung, um auf den heutigen Märkten wettbewerbsfähig zu bleiben.

Kompetente Partner gesucht

Für eine erfolgreiche Transformation braucht es kompetente Partner, die alles aus einer Hand anbieten: vom klassischen Drucken über diverse IT-Lösungen bis hin zu Smart Managed Services, die sich einfach und unkompliziert integrieren lassen. Ideale Wegbegleiter dafür sind Multifunktionssysteme, die auch den direkten Zugriff auf On-Demand-Plattformen in der Cloud wie bizhub Evolution ermöglichen. Solche Lösungen dienen modernen Büros nicht nur zum Digitalisieren von Dokumenten, sondern vernetzen Menschen, Orte und Systeme – egal ob beim Drucken, Scannen, Kopieren und Digitalisieren von Unterlagen. Entsprechende Services können auf der benutzerfreundlichen Plattform individuell zusammengestellt werden und vereinfachen die tägliche Büroarbeit auf allen Internet-fähigen Geräten – vom Smartphone bis zum Laptop. Oberste Priorität haben dabei ausgereifte Sicherheitskonzepte für das Netzwerk und umfassende Sicherheitsfeatures bei den MFPs. bizhub SECURE bietet genau dafür maßgeschneiderte Lösungen. Dazu gehören entsprechende Zugriffskontrollen und -rechte, Einstellungen für die MFP-Netzwerksicherheit sowie Aktivierung von Sicherheitsfunktionen für Festplatten und Hauptspeicher.

Eigene Arbeitsstrukturen erstellen und verwalten

Cloud-Services wie Cloud Printing und das Management druck- und dokumentennaher Cloud-Prozesse beschleunigen tägliche Routineaufgaben und schaffen so mehr Zeit für das Kerngeschäft. Die Dienste sind so gestaltet, dass sie Unternehmen einen einfachen Weg von papier- zu cloudbasierten Prozessen ermöglichen und ihnen damit auch den Weg in Richtung Digitalisierung aufzeigen. Weitere wesentliche Anwendungen sind cloudbasierte Collaboration Lösungen, wie zum Beispiel dokoni SYNC & SHARE von Konica Minolta, die die Synchronisation von Dokumenten und den sicheren Datenaustausch über Unternehmensgrenzen hinweg ermöglichen. Mitarbeiter können damit ihre eigenen Arbeitsstrukturen erstellen und verwalten. So hält dokoni SYNC & SHARE frühere Versionen von Dokumenten unverändert fest und speichert zuverlässig individuelle Eingaben sowie Beiträge. Die Möglichkeit, Dateien und Dokumente zu kommentieren und automatisch Benachrichtigungen an Beteiligte zu senden, erhöht die Effizienz bei der gemeinsamen Arbeit an Dokumenten. Der Service ermöglicht zudem volle Flexibilität in Bezug auf Zeit, Ort und Gerät.

Softwarelösungen wie ein innovatives Enterprise Content Management (ECM) spielen bei der Digitalisierung ebenfalls eine entscheidende Rolle. Dabei sind Best Practice Lösungen für Fachabteilungen genauso wichtig wie die unternehmensweite Einführung. Durch standardisierte, umfangreiche Integrationsmöglichkeiten in ERP- und CRM-Systeme wird die Effizienz in vielen Unternehmensbereichen gesteigert. Der notwendige Schutz persönlicher Daten ist dabei von zentraler Bedeutung. Unternehmen wird das spätestens seit Inkrafttreten der EU-DSGVO zunehmend bewusst.

DIE MÖGLICHKEIT, DATEIEN UND DOKUMENTE ZU KOMMENTIEREN UND AUTOMATISCH BENACHRICHTIGUNGEN AN BETEILIGTE ZU SENDEN, ERHÖHT DIE EFFIZIENZ BEI DER GEMEINSAMEN ARBEIT AN DOKUMENTEN.

Klaus Schulz,
Manager Product Marketing & Market Development, Konica Minolta Business Solutions Deutschland,
www.konicaminolta.de

Fazit

Die Eset Studie 2020 zeigt, dass sich die Digitalisierung in diesem Jahr enorm beschleunigt hat. Was früher nahezu undenkbar war, wie zum Beispiel das Arbeiten im Homeoffice, ist in der breiten Masse angekommen und zur Normalität geworden. In Zukunft geht es um die Gestaltung der hybriden Arbeitswelt mit einer Technologie, die den Menschen in den Mittelpunkt stellt. Das Konzept des intelligent vernetzten Arbeitsplatzes von Konica Minolta kann hier entscheidende Impulse liefern und eine einheitliche Strategie für die notwendigen Veränderungen geben.

Klaus Schulz

Weitere Informationenen zur Eset-Studie finden Sie unter
https://bit.ly/2IqEmVA

MOBILE APPS

VOM NISCHENPRODUKT ZUM ENTSCHEIDENDEN WETTBEWERBSFAKTOR

Mobile Apps haben sich zu einem wichtigen Wettbewerbsfaktor entwickelt. Getriggert durch das „New Normal" treiben Unternehmen ihre digitale Transformation konsequent voran und stellen Mitarbeitern, Kunden und Partnern immer häufiger maßgeschneiderte Anwendungen zur Verfügung, über die sie geschäftskritische Prozesse abwickeln. Um Wettbewerbsvorteile nutzen zu können, müssen diese Apps in kürzester Zeit entwickelt und bereitstellt werden. Dies stellt die am Release-Prozess beteiligten Stakeholder oft vor große Herausforderungen.

Der Freigabeprozess von Unternehmens-Apps ist häufig kompliziert, zeitintensiv und fehleranfällig. In einem typischen Szenario benötigt ein Fachbereich eine neue App und beauftragt eine externe Agentur mit der Entwicklung. Der Produktverantwortliche ergänzt das Release um weitere Daten wie etwa Screenshots und Beschreibung. Das Publishing-Team generiert dann die notwendigen Zertifikate und Profile, paketiert und signiert die App und gibt sie zur Veröffentlichung frei. Die aggregierten Daten gehen anschließend zum Enterprise Mobility Management- oder App-Store-Team, bevor die App schließlich an die Anwender ausgerollt werden kann.

Business-Apps im Spannungsfeld

Ein Release benötigt bis zur Veröffentlichung oft mehrere Tage und selbst kleinste Fehler können zu erheblichen Verzögerungen führen. Schnelle Feature-Releases, Fehlerkorrekturen und Sicherheitsupdates binden somit signifikante Ressourcen innerhalb der Organisation. Erschwerend kommen externe Einflüsse hinzu, wie regelmäßig veränderte Terms & Conditions der App-Stores oder neue Versionen von

MANAGED SERVICES

Das Unified Endpoint Management-Team von SPIRIT/21 hat mehr als 20.000 App Deployments durchgeführt. Aktuell werden Umgebungen mit über 200.000 Endgeräten betrieben und unterstützt.

iOS, Android oder spezifischen Software Development Kits. Notwendige Sicherheits-, Datenschutz- und Compliance-Audits können den Release-Prozess zusätzlich verzögern.

Spezialisierte IT-Dienstleister einbinden

Dieser komplexe und oft intransparente Prozess kann mit externer Unterstützung und den passenden Tools erheblich vereinfacht und beschleunigt werden. So hat sich SPIRIT/21 als erfahrener IT-Dienstleister im Bereich Enterprise Mobility Management auf effiziente App-Release-Prozesse spezialisiert, bietet dedizierte Beratungs- und Implementierungsleistungen an und ergänzt den gesamten App-Lifecycle-Prozess durch individuelle Lösungen.

Um die Einhaltung von Richtlinien und Verordnungen zu erleichtern, werden beispielsweise automatisierte Risiko- und Bedrohungsanalysen frühzeitig in den Entwicklungsprozess integriert. So können Risiken bereits vor dem Rollout erkannt und bewertet werden.

Automatisierung reduziert Fehlerquellen

Durch den Einsatz spezieller Softwarelösungen, wie „incapptic connect" von Mobilelron, lassen sich Abläufe signifikant beschleunigen und kosteneffizient abbilden. Eine gemeinsame Oberfläche stellt für alle Anwender Self-Services bereit, technische Abläufe sind automatisiert und die Sicherheit des gesamten App-Publishing-Prozesses wird deutlich erhöht.

SPIRIT/21 unterstützt Unternehmen auch bei der organisatorischen und technischen Planung sowie bei der Durchführung von Rollouts. Zusätzlich kann bei Bedarf auch das gesamte App-Portfolio überwacht werden.

Jens Reichardt | www.spirit21.com

DIE ARBEITSWELT VON

TECHNISCHE UNTERSTÜTZUNG FÜR DIE TEAMARBEIT REMOTE

Vieles deutet darauf hin, dass die Zukunft unserer Arbeitswelt hybrid sein wird: Ein Teil des Teams sitzt im Homeoffice, während der andere im Büro arbeitet. Dieses „New Normal" stellt ganz neue Anforderungen an eine kreative und effiziente Zusammenarbeit. Neue Technologien wie smarte Displays unterstützen dabei, kollaborative und effiziente Arbeitsprozesse über Ortsgrenzen hinweg umzusetzen.

Die Ton- und Bildqualität im Team-Call ist suboptimal, Ideen beim Brainstorming können nicht in einem Dokument gesammelt werden, und anstelle der gemeinsamen Arbeit an einer Präsentationen werden isolierte Teilkonzepte zusammengefügt – die produktive und kreative Zusammenarbeit über Ortsgrenzen hinweg hängt von vielen technischen Faktoren ab. Die Devise „so schnell wie möglich alle zurück ins Büro" stellt allerdings keine adäquate Lösung für diese Herausforderungen dar, schon allein weil es den Wünschen vieler Mitarbeiter widerspricht: 85 Prozent der Arbeitnehmer im Homeoffice bewerten ihre Situation als positiv, 69 Prozent der Befragten möchten auch in Zukunft mehr von zu Hause arbeiten. Daneben fehlt vielen Menschen die gemeinsame Mittagspause mit den Kollegen, der Plausch an der Kaffeemaschine oder der Austausch über das neue Projekt am Schreibtisch. Es zieht sie zurück an den angestammten Arbeitsplatz. Im Kampf um die besten Arbeitskräfte müssen Unternehmen flexible Arbeitsmodelle ermöglichen, die das Homeoffice, das Büro und auch neue Arbeitsumgebungen wie Co-Working Spaces miteinschließen. Wie kann dies gelingen, ohne dass darunter die kreative und produktive Zusammenarbeit im Team leidet?

Gestochen scharfe Videokonferenzen

Videokonferenzen bestimmen den Arbeitsalltag vieler Menschen – in Zukunft vermutlich noch mehr als aktuell: Einer Prognose von Global Market Insights zufolge wird sich der Umsatz im Videokonferenzmarkt in den kommenden Jahren mehr als verdreifachen – von 14 Milliarden Dollar in 2019 auf 50 Milliarden Dollar in 2026.

Für eine optimale Übertragung von Bild und Ton bietet Samsung gemeinsam mit Logitech Videokonferenzlösungen für den Schreibtisch und für Besprechungsräume jeglicher Größe an. Dafür stehen hochauflösende Business Monitore wie die der neuen TF- und TUF-Serie in 22 bis 32 Zoll, aber auch großflächige Displays zur Verfügung. In Kombination mit den USB-kompatiblen Kameras ermöglichen die Geräte kollaboratives Arbeiten in höchster Bild- und Ton-Qualität. Darüber hinaus haben Samsung und der führende Anbieter von Kollaborationssoftware, Cisco, eine branchenführende Lösung für Besprechungsräume erarbeitet. Bei dieser verbinden sich die 43- bis 75-Zoll großen Displays der QBR- und QMR-Serie automatisch mit dem Webex Room Kit von Cisco. Die Geräte schalten sich bei eingehenden Anrufen selbständig ein und wählen eigenständig die richtige Quelle. Bild und Ton werden so in bester Qualität übertragen. Diese Lösung wird stetig weiterentwickelt und erweitert. So

MORGEN

gibt es mit Webex Room Panorama seit Neuestem die Möglichkeit, Videokonferenzen über QLED 8K-Displays von Samsung zu übertragen.

Effiziente und kreative Teamarbeit dank digitaler Flipcharts

Videokonferenzen bieten eine gute Möglichkeit, trotz großer Distanzen miteinander in Kontakt zu bleiben und ein Teamgefühl herzustellen. Schwieriger wird es allerdings, wenn in einem Meeting gemeinsam an Dokumenten gearbeitet werden soll. Das trifft vor allem dann zu, wenn ein Teil des Teams im Besprechungsraum zusammensitzt und ein anderer digital zugeschaltet wird. Damit den Kollegen im Homeoffice im Vergleich zu den Mitarbeitern vor Ort keine Nachteile entstehen, haben Samsung und Cisco auch hier bestehenden Lösungen miteinander kombiniert: So wurde Webex Teams und Webex Roomkit Mini auf dem Flip 2 integriert. Skizzen und Beiträge, die auf dem digitalen Flipchart festgehalten werden, sind über Webex on Flip für alle Teilnehmer sichtbar – egal, von wo sie zugeschaltet sind. Auch können Beiträge remote auf dem smarten Display verfasst und geteilt werden. Zudem sind Dateien zentral vom PC, Laptop oder Smartphone sowie der Cloud abrufbar, um sie auf dem smarten Display übertragen und bearbeiten zu können. Die erstellten Inhalte werden auf dem Flip 2 in Echtzeit gespeichert und können im Anschluss an das Meeting per E-Mail unter den Teilnehmern geteilt werden.

Während die Kollegen im Homeoffice über ihren Laptop oder ihr Smartphone interagieren, stehen den Mitarbeitern im Besprechungsraum ein mitgelieferter Stift oder andere freiwählbare Schreibutensilien mit einer flachen Spitze zur Verfügung, um Notizen auf dem 55, 65 oder 85 Zoll großen Display zu verfassen. Der Clou dabei: Die Strichstärke auf dem Display wird automatisch an die Breite des verwendeten Stifts angepasst. Daneben gibt es einen Pinselmodus, so dass bei Bedarf wie auf einer Leinwand wahlweise mit digitalen Wasser- oder Ölfarben gemalt werden kann. Dank einer Reaktionszeit von 6 Millisekunden geschieht das ohne merkliche Verzögerung. Diese flexiblen, vielfältigen Funktionen erlauben den Einsatz des digitalen Flipcharts in unterschiedlichsten Meeting-Situationen – egal ob es sich um die technische Planung eines Projekts, die kreative Erarbeitung eines Konzepts oder die Erstellung einer Präsentation handelt.

Unternehmen, die hybride Arbeitsmodelle ermöglichen, können von einer Win-win-Situation profitieren: Mitarbeiter, die frei über ihren Arbeitsplatz entscheiden, sind insgesamt zufriedener, wie Studien zeigen. Für diese Flexibilität braucht es allerdings die richtigen digitalen Tools, die einen kreativen und effizienten Austausch im Team auch remote erlauben. Wird die dafür notwendige technische Ausstattung zur Verfügung gestellt, erhöht das zum einen die Produktivität. Zum anderen können diese zukunftsgerichteten Unternehmen einen entscheidenden Vorteil im Ringen um die besten Mitarbeiter erhalten, da sie flexibles Arbeiten in einem modernen Umfeld ermöglichen.

www.samsung.com/de

SAMSUNG

DRITTWARTUNG IM RECHENZENTRUM

WACHSTUMS-POTENZIAL FÜR 2021

2021 verspricht für die Third-Party Maintenance-Branche und insbesondere für einen ihrer führenden Vertreter ein spannendes Jahr zu werden. Vor wenigen Monaten hat sich die Technogroup IT-Service GmbH der Evernex angeschlossen. Gemeinsam bilden sie den neuen europäischen Marktführer für Drittwartung im Rechenzentrum. Die Technogroup bietet aus einer Hand Service-, Dienstleistungs- und Consultingangebote für alle entscheidenden IT-Systeme an mit dem Ziel, Hardwareausfälle zu vermeiden, zu beheben und die Nutzungsdauer von IT-Systemen kostengünstig und nachhaltig zu verlängern. CEO Klaus Stöckert erklärt im Interview mit Ulrich Parthier, Herausgeber it management, warum er gerade im Jahr 2021 für die Drittwartungsbranche Potenzial sieht.

WIR SEHEN UNS NICHT ALS AUSTAUSCHBARER DIENSTLEISTER, SONDERN ALS PARTNER UNSERER KUNDEN UND STARKE PARTNERSCHAFTEN HELFEN ALLEN BETEILIGTEN IN DIESER HERAUSFORDERNDEN ZEIT.

Klaus Stöckert,
CEO, Technogroup IT-Service GmbH;
Managing Director, Region Central, Eastern & Northern Europe, Evernex
www.technogroup.com
www.evernex.com/de

Ulrich Parthier: *Herr Stöckert, das Jahr 2020 geht zu Ende. Wie schauen Sie auf dieses Jahr zurück?*

Klaus Stöckert: Ohne Zweifel wird das Jahr 2020 in die Lehr- und Geschichtsbücher eingehen. Covid-19 stellt Wirtschaft und Gesellschaft vor bis dato unbekannte Herausforderungen – und das weltweit. Die Pandemie wird uns auch im nächsten Jahr und deren wirtschaftliche sowie gesellschaftliche Folgen in den kommenden Jahren begleiten und beeinflussen.

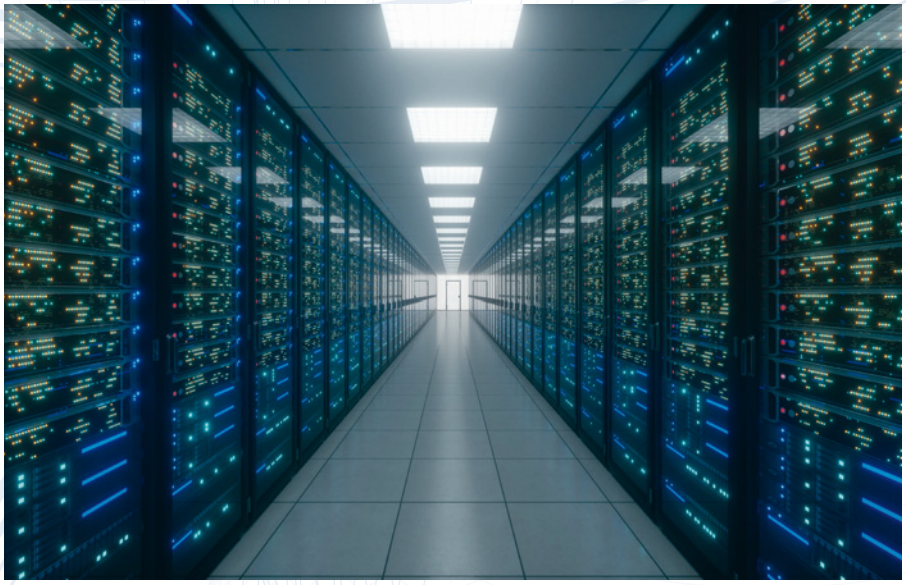
Für die Technogroup ist das Jahr 2020 aber gleichzeitig in positiver Hinsicht etwas Besonderes. Wir haben unser 30-jähriges Firmenjubiläum gefeiert und dabei auf eine sehr erfolgreiche Firmengeschichte zurückgeblickt. Gleichzeitig haben wir einen entscheidenden Schritt in die Zukunft gemacht, indem wir uns mit Evernex zusammengeschlossen haben.

Ulrich Parthier: *Die Technogroup war Marktführer im D/A/CH-Raum für Drittwartung in Rechenzentren. Jetzt ist sie mit Evernex der neue Marktführer in ganz Europa. Was bedeutet diese neue Rolle für die Technogroup?*

Klaus Stöckert: Durch den Zusammenschluss mit Evernex als global tätiges Unternehmen stärken wir als Technogroup unsere internationale Präsenz und eröffnen neue Wachstumschancen. Wir bündeln unsere Kräfte und können unsere Expertise und unseren Service nun noch mehr Unternehmen zur Verfügung stellen und unser Angebot erweitern. Als Mitglied der Evernex bieten wir unseren Kunden ein weltweites Netzwerk mit echter globaler Abdeckung. Evernex ist in über 160 Ländern tätig. Gemeinsam haben wir rund 850.000 Ersatzteile in über 350 Logistikstützpunkten weltweit. Trotz dieser globalen Ausrichtung bewahrt sich die Technogroup die Vorteile eines Mittelständlers. Wir sind nah an unseren Kunden und kennen die Bedürfnisse des Mittelstandes genauso gut wie die großer Konzerne.

Ulrich Parthier: *Der Markt für Drittwartung oder Third-Party Maintenance (TPM) ist noch relativ unbekannt. Wie wird sich das 2021 entwickeln?*

Klaus Stöckert: Nicht jedem ist Drittwartung ein Begriff, aber der Bekanntheitsgrad ist gestiegen. Das zeigen unsere Studien. 2019 war 43 Prozent der Studienteilnehmer das Konzept Drittwartung bekannt, 2020 waren es fast 63 Prozent. Wir sind davon überzeugt, dass die Bekanntheit 2021 weiter steigen wird. Das hat drei Gründe: Erstens, die Digitalisierung nimmt an Bedeutung zu, das sehen wir gerade jetzt in Zeiten der Pandemie. Und in diesem Prozess spielt das Rechenzentrum und dessen Hochverfügbarkeit eine entscheidende Rolle. Zweitens, die IT-Landschaften der Unternehmen werden aufgrund der fortschreitenden Digitalisierung immer komplexer. Und drittens, die wirtschaftliche Lage vieler Unternehmen ist momentan aufgrund der Wirtschaftskrise herausfordernd und wird dies auch 2021 sein.



Ulrich Parthier: *Welche Konsequenzen haben die Unternehmen aufgrund der wirtschaftlichen Herausforderungen gezogen?*

Klaus Stöckert: Diese Frage haben wir uns in unserer diesjährigen Studie mit über 350 Teilnehmern auch gestellt. Diese ist noch nicht veröffentlicht, aber einige signifikante Zahlen kann ich hier schon einmal nennen. Demnach haben die Pandemie und die damit einhergehende Wirtschaftskrise auf fast drei Viertel der befragten Unternehmen negative Auswirkungen. Um den wirtschaftlichen Auswirkungen der Krise zu begegnen, verschieben 60 Prozent der Unternehmen Investitionen, die Hälfte kürzt die Budgets und zwei Drittel versuchen, ihre Prozesse zu optimieren. Gerade jetzt ist es für Unternehmen wichtig, sich auf ihr Kerngeschäft zu konzentrieren und ihre Kapazitäten strategisch zu nutzen. Daher gehen wir davon aus, dass sich der Trend Managed Services zu nutzen im nächsten Jahr fortsetzen wird.

Ulrich Parthier: *Und diese Wege der wirtschaftlichen Herausforderung zu begegnen, schlagen sich auch auf die Strategien und Maßnahmen in der IT und im Rechenzentrum nieder?*

Klaus Stöckert: Richtig. Laut unserer Umfrage suchen drei Viertel der Befragten nach Möglichkeiten, die Kosten für den Betrieb ihres Rechenzentrums zu reduzieren und gleichzeitig die Qualität des IT-Betriebs aufrechtzuerhalten. Hierbei kann die Umorientierung von der Wartung durch den Hersteller hin zur Drittwartung eine Möglichkeit bieten. Das Analystenhaus Gartner nennt in einem Bericht ein Einsparpotential in der IT-Wartung von bis zu 70 Prozent durch den Einsatz herstellerunabhängiger Drittwartung.

Ulrich Parthier: *Laut Ihren Zahlen wollen Unternehmen Investitionen nicht nur streichen, sondern verschieben. Was hat das mit Drittwartung zu tun?*

Klaus Stöckert: Eine ganze Menge. Hersteller bieten ihren Hardware-Support oft nur für wenige Jahre an. Unsere Studie von 2019 hat aber gezeigt, dass 31 Prozent der befragten Unternehmen ihre Server und Data-Center-Hardware zwischen sieben und zehn Jahren im Einsatz haben, weitere 28 Prozent sogar mehr als zehn Jahre. Drittwartung ermöglicht die Nutzung von Hardware über den End-of-Service-Life hinaus. Das schafft Unternehmen den nötigen Spielraum, kostenintensive Neuanschaffungen zu verschieben, ohne Sicherheits- oder Performanceverluste befürchten zu müssen.

Ein weiteres unterschätztes Einsparpotenzial ist refurbished Hardware. Durch den Einsatz technisch einwandfreier, geprüfter Geräte aus zweiter Hand können Unternehmen bis zu 50 Prozent der Kosten gegenüber Neuware sparen, ohne bei der Qualität Abstriche zu machen. Auch diese Hardware kann ein TPM-Anbieter warten.

Ulrich Parthier: *Sie sagen, ein Grund für das Wachsen des TPM-Marktes sei die zunehmende Komplexität der IT-Landschaften. Können Sie das erläutern?*

Klaus Stöckert: In unserer Studie aus dem vergangenen Jahr haben 47 Prozent der Befragten angegeben, Geräte von fünf oder mehr Herstellern im Einsatz zu haben. Bei der Wartung durch den OEM heißt das, dass man fünf oder mehr unterschiedliche Vertragskonditionen und Ansprechpartner hat. Macht man die Wartung nach dem EOSL inhouse, bedeutet es, dass die IT-Abteilung über breites Fachwissen zu sämtlichen Geräten aller vertretenen Hersteller parat haben und up to date halten muss. Angesichts der oft fehlenden Ressourcen ein schwieriges Unterfangen. Übernimmt ein TPM-Dienstleister die Wartung, hat das Unternehmen nur einen Ansprechpartner, der 24/7 bereitsteht, über die entsprechende Fachkompetenz verfügt und Störungen sehr schnell beheben kann.

Hinzu kommt, dass der Hersteller bei der Wartung nur die eigenen Produkte im Blick hat. Bei Technogroup handhaben wir es so, dass Techniker-Teams die IT-Landschaft unserer Kunden ganzheitlich betrachten. Das erleichtert nicht nur die Wartung, sondern schafft die Grundlage für eine fundierte Beratung. Wir sehen uns nicht als austauschbarer Dienstleister, sondern als Partner unserer Kunden und starke Partnerschaften helfen allen Beteiligten in dieser herausfordernden Zeit.

Ulrich Parthier: *Herr Stöckert, wir danken für dieses Gespräch.*

A4Q
Selenium Tester
Foundation

Get Selenium Certified – Now

Perfekt für alle, die das Selenium WebDriver Toolset nutzen wollen.
Ideal für die Karriere mit international anerkanntem Nachweis von Skills durch einen unabhängigen Zertifizierer.

iSQI
International Software Quality Institute

A4Q Alliance for Qualification

isqi.org/de/54-a4q-certified-selenium-tester-foundation.html

VOM LADENHÜTER ZUM VERKAUFSSCHLAGER

ORDER MANAGEMENT MIT AROMA® VON ARVATO SYSTEMS

Die Auswirkungen der Corona-Pandemie treffen auch Handelsunternehmen mit Filialnetz: Sie müssen ihre Läden zeitweise schließen, Kunden weichen auf Online-Angebote aus, Abstands- und Hygieneregeln schrecken die Kundschaft ab. Die Folgen: Umsatzeinbußen, hohe Bestände vor Ort und der daraus resultierende Zwang, Produkte zu teils ruinösen Preisen zu verkaufen. Ein Omni-Channel Order-Management-System (OMS) wie aroma® von Arvato Systems entspannt die heikle Situation. Es verbindet stationären sowie Online-Handel und bildet die Voraussetzung für Ship-from-Store-Konzepte: Händler verkaufen Ware aus den Lagern der Filialen mit Gewinn ab.

Alles muss raus!

Das Sortiment in den Läden wechselt regelmäßig. Doch was tun, wenn das Lager bereits überquillt? Auf Neuware zu verzichten, ist keine Option. Viele Filial- und Kaufhaus-Manager senken die Preise radikal – mit der Folge immer geringerer Margen. Doch trotz niedriger Preise bleibt der große Run in die Läden aus. Auch die anhaltend hohen Online-Bestellvolumina können die Verluste im Filialgeschäft nicht kompensieren. Zudem stoßen die Abwicklungs-Systeme im E-Commerce durch die Vervielfachung der Online-Bestellungen an ihre Grenzen, und es kommt zu Backlogs: Aufträge werden nicht pünktlich ausgeliefert, die Bearbeitung von Retouren und Reklamationen verzögert sich.

aroma®: Kundenservice und Margen verbessern

Für Händler, die ein performantes OMS wie aroma® einsetzen, bietet sich ein Ausweg: Online-Kunden erhalten ihre Bestellung aus der nächstgelegenen Filiale. Der Händler muss die Ware nicht zu Dumpingpreisen verramschen, während der Kunde von schnellen Lieferzeiten profitiert. Hierfür fließen im zentralen OMS alle relevanten Informationen kanalübergreifend zusammen. aroma® optimiert den Auslieferungsweg nach Kriterien wie den Transportkosten oder der Priorität einer Bestellung. Das sorgt für eine optimale Balance zwischen Kundenservice, Kapazität und Wirtschaftlichkeit.

Mehr Service und Komfort

Mit einem OMS können Mitarbeiter vor Ort und auch im Call-Center Kunden nicht nur sofort Auskunft geben, sondern auch Bestellungen ändern: von Teilstornierungen über die Auslieferung von Ersatzartikeln bis hin zu Gutschriften. Zugleich erfüllen Händler die Wünsche ihrer Kunden: Kunden kaufen online und bekommen das Produkt aus einem Lager oder einer Filiale zugeschickt oder holen es in der Wunsch-Filiale ab bzw. retournieren es dort; oder sie lassen sich die Kosten für retournierte Produkte in einer Filiale erstatten.

Prozesse integrieren und automatisieren

Neben der Kernfunktion, der optimierten Auslieferung von Waren, verfügt ein OMS über weitere Module, welche die Arbeit des Händlers erleichtern: ein Call-Center-Modul, ein Filial-Modul, ein Lieferanten-Modul, ein Preis- und Promotionen-Modul, ein Dokumentenmanagement-Tool und eine Administrationskonsole. Schließlich sind Omni-Channel-Prozesse nur dann wirtschaftlich, wenn sie integriert und automatisiert sind.

Win-Win-Situation für Händler und Verbraucher

Der Einsatz eines OMS wie aroma® verbessert den Service über alle Kanäle hinweg. Es bildet die technologische Grundlage, um die Lieferzeiten zu verkürzen, die Kosten zu senken, die Flexibilität von Verkaufsprozessen zu erhöhen, stets aktuelle Einblicke zu erhalten und die Marge zu vergrößern. Mit automatisierten Prozessen und optimierten Warenbeständen müssen Retailer ihre Produkte nicht länger zu Kampfpreisen verramschen. Mehr im kostenfreien White Paper unter https://arva.to/wp-aroma.

Dr. Martin Anduschus
www.arvato-systems.de

ASSET- UND LIZENZMANAGEMENT IN DER PRAXIS

VERSTECKTE KOSTEN UND EINSPARPOTENZIALE AUFDECKEN

Ein stets verfügbarer und aktueller Überblick über die vorhandene Hard- und Software? In vielen Unternehmen ist diese Anforderung noch immer nicht realisiert. Dabei spart ein umfassendes Asset- und Lizenzmanagement wie es etwa die ACMP-Suite von Aagon bereitstellt, spürbar Zeit und Geld. Denn häufig schlummern im Controlling versteckte Kosten in Form von Überlizenzierung oder nicht mehr benötigter Hardware.

Planungs- und Entscheidungssicherheit sind für Systemadministratoren essenziell für eine optimale Steuerung der IT-Landschaft. Ein umfassendes Asset-Management sorgt für einen Überblick über alle Sach- und Anlagegüter der IT-Umgebung, und das Lizenzmanagement kennt jedes eingesetzte Programm inklusive der individuellen Lizenzmodelle. Dies schützt nicht nur vor unnötigen Investitionen, sondern auch vor Problemen bei Software-Audits.

Optimaler Einsatz der Lizenzen

Besonders einfach gelingt die Erfassung aller Inventardaten, wenn die eingesetzte Software die relevanten Daten weitgehend automatisiert aufnimmt. Wichtig ist insbesondere die komplette Registrierung aller Geräte, Benutzer und deren Lizenzen – und zwar für PCs, Server, Thin Clients, virtuelle Server und Clients, Voice-over-IP-Telefonanlagen, Drucker, Zeiterfassungsterminals, Terminalserver, SNMP-Geräte und vieles mehr. Wesentlich zudem ist auch das Erfassen der einzelnen Abhängigkeiten jedes Benutzers zu den Geräten und Lizenzen, die Administratoren normalerweise nur halbautomatisch erledigen können. Diese Informationen eröffnen IT-Teams detaillierte Einblicke in die Lizenznutzung und den optimalen Einsatz der Lizenzen.

Dadurch erschließen sich vielfältige Optimierungsmöglichkeiten. Etwa indem unnötige Anschaffungen beim Softwareeinkauf vermieden werden. Zudem senkt ein effektives Lizenzmanagement Investitions- und Pflegekosten. Weitere Kosten lassen sich einsparen durch aktives Application Usage Tracking. Ein weiterer Vorteil des Lizenzmanagements ist die gezielte Wiederverwendung bereits angeschaffter Software, etwa indem – anstelle eines Neuerwerbs – die vorhandene Lizenz auf einen anderen Arbeitsplatz übertragen wird. Und: Unternehmen, die ihre Lizenzzahlen exakt analysieren, können häufig mit dem Hersteller ein kostengünstigeres Lizenzierungsmodell aushandeln.

Asset Management

Sobald alle Software-Assets erfasst sind, eröffnet sich weiteres Einsparungspotenzial. So zeigt sich unter anderem, ob sich die Software standardisieren oder die Anzahl der eingesetzten Produkte gezielt reduzieren lässt. Ferner, ob Update-Varianten eine Alternative zu den wesentlich teureren Vollversionen darstellen. Mit Lösungen wie ACMP lassen sich Programme und Bundles automatisiert erfassen und direkt den bestehenden Lizenzen zuordnen. So kann der IT-Administrator unerwünschte Software erkennen und in einer Datenbank auf einen Blick sehen, welche Software überhaupt lizenzpflichtig ist.

Das Asset Management liefert einen stets verfügbaren Überblick über alle Sach- und Anlagegüter. ACMP etwa berücksichtigt dabei den gesamten Lebenszyklus der Soft- und Hardware-Assets und ermöglicht es dem IT Verantwortlichen, alle Unternehmens-Assets komfortabel von einem Ort aus zu verwalten und zu automatisieren. Als großer Vorteil erweist sich dabei auch, dass jederzeit alle Fragen zu den einzelnen Assets beantwortet werden können: Etwa wo befindet sich ein bestimmtes Smartphone, wer benutzt es, welcher Kostenstelle ist es zugeordnet, welche Software ist installiert und in welcher Version. Ein optimales Asset- und Lizenzmanagement unterstützt sowohl mittlere als auch große Unternehmen dabei, ihre IT-Performance zu optimieren und dabei spürbar die Kosten zu senken.

Sebastian Weber | www.aagon.com

DIGITAL EMPLOYEE EXPERIENCE

SECHS-PUNKTE PLAN FÜR PROAKTIVEN IT-SERVICE

Viele Innovationen führen nicht zum erwarteten Erfolg, weil sie von den Anwendern nicht angenommen werden oder zu mehr technischen Problemen am Arbeitsplatz führen als zunächst angenommen.

Die ganzheitliche Sicht auf IT-Arbeitsplätze – also das Konzept von Digital Employee Experience (DEX) Management – im IT Support kann entscheidende Beiträge in der Steuerung der unternehmensweiten IT-Strategie leisten. Der einfache Grundgedanke dabei: Raus aus der Warteposition als Annahmestelle für Störungen und Beschwerden, hin zu einer proaktiven, anwenderzentrierten Rolle. Proaktiver Support verbessert das Verhältnis zwischen IT und den Fachabteilungen und trägt dazu bei, die IT wirklich als Business Enabler zu verstehen.

IT-Support und Help-Desk brauchen einen Perspektivenwechsel. Welche Kriterien hier wesentlich sind, dafür hat Nexthink aus seiner Projekterfahrung eine Guideline zu den Fähigkeiten entwickelt.

1. Kosten-Nutzen-Rechnung für DEX

Zunächst geht es darum, sich die Anforderungen von DEX Management bewusst zu machen: Digitale Arbeitsplätze sind immer stärker geprägt von hybriden Konzepten und dynamischen Veränderungen. Es gilt eine Balance zwischen Benutzerfreundlichkeit und IT-Sicherheit herzustellen, um Mitarbeiterzufriedenheit und Produktivität zu gewährleisten.

2. IT-Control Center mit Detailwissen

Ob bei IT-Arbeitsplätzen alles störungsfrei läuft und beispielsweise Software-Upgrades oder Roll-outs tatsächlich Verbesserungen bringen, lässt sich nicht allein an niedrigen Ticketzahlen und kurzen Bearbeitungszeiten ablesen – zumal, wie eine Nexthink-Studie zeigt, im Schnitt nur etwa 50 Prozent der Störungen an IT-Arbeitsplätzen im Help Desk gemeldet werden. Wer als IT-Control Center ein produktives Arbeitsumfeld sicherstellen will, braucht technische Performance-Daten vom Endgerät.

3. Blick in die Zukunft

Welche Maßnahmen oder Faktoren führen zu einer verbesserten DEX? Aus dem Big-Data-Ansatz mit den Messdaten aus den IT-Infrastrukturen gilt es, proaktiv Maßnahmen für optimale IT-Arbeitsplätze zu treffen und vorausschauend zu agieren.

4. Priorisierung und optimierter Ressourceneinsatz

Was hat Vorrang: die Störung mit den meisten Betroffenen, das, was am einfachsten zu lösen ist oder doch zuerst die unternehmenskritischen Bereiche? Nur technische Parameter genügen hier nicht. Bei der Priorisierung von Störungsbehebungen bietet KI-basiertes Clustering mit Drill-Down-Optionen Vorteile, die an Business Intelligence angelehnt sind.

5. Automatisierte Arbeitsanweisungen zur Entstörung

Hinterlegte Skripte und Playbooks beschleunigen die Prozesse im IT-Support, Störungsdetails zu verstehen und nötige Maßnahmen in der richtigen Reihenfolge umzusetzen, möglichst automatisiert, ohne den Anwender zu stören.

6. Kooperation mit Anwendern

Bloße Performance-Messungen sind aber nur ein Teil der Wahrheit. Es braucht eine enge Kommunikation zwischen IT-Support und Anwendern durch kontextbezogene Umfragen und Informationen an ausgewählte Zielgruppen.

Fazit

Der IT-Support muss Teil einer Digitalisierungsstrategie werden. Proaktiver Support und die Sicherstellung, dass alle Services auch reibungslos genutzt werden können, erfordern einen Perspektivenwechsel, der den Anwendern stärker in den Mittelpunkt rückt.

Holger Dörnemann

www.nexthink.de

nexthink

DIE AUSWIRKUNGEN VON ITL 4 AUF ITSM-TOOLS

MÖGLICHKEITEN ZUR VERBESSERUNG

In ITIL 4 werden im Vergleich zur Vorgängerversion ITIL v3/2011 einige neuartige, übergreifende Konzepte vorgestellt und auch etliche Möglichkeiten zur Verbesserung des strategischen und operativen IT Service Managements. Daraus können einige funktionale Anforderungen für IT Service Management Tools abgeleitet werden. Dieser Artikel erläutert, welche Tool-Funktionen Sie für die Einführung von ITIL 4 Practices benötigen. Er ist ein Auszug aus einem umfangreichen Whitepaper, das die USU zusammen mit dem ITIL Experten Stephen Mann verfasst hat.

Allgemeine Tool-Anforderungen

Die Nutzung der ITIL 4 Value Streams anstelle der ITIL v3/2011-Prozesse kann durch grafische Workflow-Engines unterstützt werden, die in vielen ITSM-Tools bereits enthalten sind. Anstelle der volumen- und aktivitätsbasierten Kennzahlen wie „wie viele" und „wie lange" sollten jedoch eher business-orientierte Metriken eingesetzt werden, die den geschäftlichen Nutzen besser vermitteln. Das können zum Beispiel die durch IT-Unterstützung erhöhten Stückzahlen in einem Produktionsunternehmen sein.

Für die breiteren Einsatzszenarien von ITIL 4 im Enterprise Service Management sollten die Tools ein sehr gutes Benutzererlebnis für Endanwender bieten, die Einführung neuer, IT-fremder Datenobjekte erlauben (etwa Gebäude oder Mobiliar) und die Trennung spezifischer Funktionen, Daten und Wissensmanagementartikeln für die einzelnen Servicebereiche ermöglichen.

Ein wesentliches ITIL 4-Prinzip ist die Automatisierung. Hierzu werden KI-gestützte ITSM-Funktionen benötigt wie zum Beispiel ChatBots, intelligentes Ticketrouting, automatische Trenderkennung und Problemanalyse und die KI-basierte Identifizierung relevanter Events im Monitoring.

Spezifische Tool-Anforderungen

Neben den konzeptbasierten, allgemeineren Auswirkungen erfordern auch die einzelnen Practices (siehe Bild) jeweils spezifische ITSM-Tool-Funktionen.

Die folgenden ITSM-Tool-Funktionen unterstützen die gängigsten Prozesse/Practices und werden demzufolge von der Mehrzahl der IT-Organisationen benötigt, die ITIL 4 einführen möchten:

Erforderliche ITSM-Tool-Funktionen für:

1. Change Enablement, Deployment Management und Release Management:
- Integration von DevOps-Tools
- Automatisierung von Changes und Releases
- Automatisierung von Continuous Integration,Continuous Delivery und Continuous Deployment
- Abbildung von Blue/Green-Releases, Feature-Flag-Releases

2. Incident Management:
- Unterstützung von "Swarming"

3. Problem Management:
- KI-basierte Funktionen für die Problem-Erkennung und proaktive Störfallvermeidung

4. Service Catalog Management:
- Erstellen neuer Service-Angebote durch Aggregation bestehender Servicekomponenten

5. Service Configuration Managment:
- Integration von Tools wie Vagrant, Ansible, Puppet und Docker zur Unterstützung des „Infrastructure-as-Code"-Ansatzes

6. Service Desk
- Abbildung eines „Query-Tickets" für noch nicht kategorisierte Endanwender-Tickets
- Funktionen für den Omnichannel-Support

„ETLICHE DER VON ITIL 4 GEFORDERTEN TOOLFUNKTIONEN SIND BEREITS IN EINIGEN ITSM-TOOLS VORHANDEN. ES GIBT ABER AUCH FUNKTIONEN, DIE NOCH NICHT IN ABSEHBARER ZEIT ZUR VERFÜGUNG STEHEN WERDEN."

Martin Landis, Business Unit Manager, USU GmbH.

DIE 34 ITIL 4 MANAGEMENT PRACTICES

GENERAL MANAGEMENT PRACTICES

- Architecture management
- Continual improvement (ITIL v3/2011: continual service improvement)
- Information security management
- Knowledge management
- Measurement and reporting
- Organizational change management
- Portfolio management (service portfolio management)
- Project management
- Relationship management (ITIL v3/2011: business relationship management)
- Risk management
- Service financial management (ITIL v3/2011: financial management for IT services)
- Strategy management (ITIL v3/2011: strategy management for IT services)
- Supplier management
- Workforce and talent management

SERVICE MANAGEMENT PRACTICES

- Availability management
- Business analysis
- Capacity and performance management (ITIL v3/2011: capacity management)
- Change enablement (ITIL v3/2011: change management)
- Incident management
- IT asset management (service asset and configuration management)
- Monitoring and event management (ITIL v3/2011: event management)
- Problem management
- Release management (ITIL v3/2011: release and deployment management)
- Service catalog management
- Service configuration management (ITIL v3/2011: service asset and configuration management)
- Service continuity management (IT service continuity management)
- Service design (ITIL v3/2011: design coordination)
- Service desk (was an ITIL v3/2011 function)
- Service level management
- Service request management (ITIL v3/2011: request fulfilment)
- Service validation and testing

TECHNICAL MANAGEMENT PRACTICES

- Deployment management (ITIL v3/2011: release and deployment management)
- Infrastructure and platform management
- Software development and management

- Neu
- Name geändert oder auf-geteilt
- unveränderter Name
- unveränderter Name, aber geänderter Inhalt

7. Service Level Management:
- Einführung sogenannter eXperience Level Agreements (XLAs)

Weniger gebräuchliche Prozesse/ Practices

Tool-Funktionen zur Unterstützung weniger gebräuchlicher ITIL-Prozesse/Practices dürften von der Mehrzahl der IT-Organisationen nicht nachgefragt werden, obwohl sie einen Mehrwert bieten können. Die folgenden ITSM-Tool-Funktionen werden in den Produktentwicklungsplänen der Tool-Anbieter deshalb wahrscheinlich nicht berücksichtigt.

Potenzielle neue ITSM-Tool-Funktionen:

1. Information Security Management
- Automatisierte Workflows für das Security Incident Handling

2. Portfolio Management
- Funktionen für das Project-Portfolio-Management (PPM)

3. Relationship Management
- Dokumentation der Kommunikation mit Servicekunden
- gewichtete Matrix zur Bewertung von Beziehungen mit Verlinkungen in den kontinuierlichen Verbesserungsprozess

4. Service Continuity Management
- Automatisierte Management-Workflows für das Erstellen, Überprüfen, regelmäßige Testen und Verbessern von Service Continuity-Plänen (und anderen Business Continuity-Plänen)

5. Service Financial Management
- Cloud Cost Management & Optimization für Infrastruktur- und Software-Lizenzkosten in Multi Cloud- und Hybrid Cloud-Umgebungen
- Integration mit den gängigsten Cloud-Service-Providern

6. Supplier Management
- Funktionen für das Multi Supplier Management (Service Integration and Management/SIAM)
- Austausch von Incidents zwischen Kundenorganisation und mehreren Lieferanten
- Unterstützung von Service-Level-Zielen für komplexere Service Delivery-Vereinbarungen mit mehreren Suppliern
- Abbildung von non-IT-Assets (Gebäude, Fahrzeuge, …)

3. Project Management
- Planung von Aufgaben, Terminen, Meilensteinen, Ressourcenzuordnung für Projekte
- Statusüberwachung

4. Risk Management
- Auflistung und Bewertung von Risiken
- Maßnahmen zur Risikovermeidung

5. Workforce und Talent Management
- People Management-Funktionen, wie Resource Planning, Recruitment, Onboarding, Performance Management, Learning und Development sowie Succession Planning.

Neue Prozesse/Practices

Bei den folgenden neuen ITIL 4 Prozessen/Practices wird sich erst im Laufe der Zeit zeigen, wie sie jeweils von den Organisationen angenommen und welche Änderungen der ITSM-Tools ihnen folgen und ihre Einführung vorantreiben werden.

Potenzielle neue ITSM-Tool-Funktionen:

1. Organizational Change Management
- Workflow-Funktionen für sämtliche Schritte bei organisatorischen Veränderungen, wie zum Beispiel Planung, Managen von Risiken und Problemen, Erstellen von Fortschrittsberichten, Dokumentieren von Entscheidungen, Verfolgen von Schulungen und anderen Maßnahmen

2. IT Asset Management (ITAM)
- Funktionen für das Asset Lifecycle Management

Stephen Mann, Martin Landis
www.usu.de

WHITEPAPER DOWNLOAD

Dieser Artikel ist ein Auszug aus einem umfangreichen Whitepaper, das hier heruntergeladen werden kann:
http://bit.ly/wp-itil4-tools-itm

AGILE ORGANISATIONS-ENTWICKLUNG

ITERATIVE, INKREMENTELLE UND LERNENDE BEWEGUNG ERMÖGLICHEN

Klassische wie systemische Organisationsentwickler und -entwicklerinnen beschreiben Veränderungen mit der Veränderungskurve nach Kübler-Ross und/oder Kotter. Diese beschreiben Veränderungen als unabänderliche Impulse, die mittels geeigneter Kommunikationsmaßnahmen besser „verdaubar" sind.

Erfolgreiche agile Transitionen verändern Werte, Verhalten und Arbeitsumfelder (=Hardware) der Beteiligten. Im Sinne Everett Rogers nehmen die Beteiligten also eine Innovation an – oder sie verwerfen diese.

Die Autorin beschreibt in dem Buch „Agile Organisationsentwicklung" erfolgreiche Verfahren/Vorgehensweisen, die es den Beteiligten erleichtert, die Innovation „Agilität" auf allen Ebenen anzunehmen.

Agile Organisationsentwicklung – Iterative, inkrementelle und lernende Bewegung ermöglichen; Judith Andresen, Carl Hanser Verlag, 03/2021

DIE KUNST DER ONLINE-MODERATION

TOOLS, IDEEN UND TIPPS FÜR DIE ERFOLGREICHE UMSETZUNG

Alles, was wir bis dato über die Art unserer Zusammenarbeit zu wissen glaubten, ändert sich gerade: Es ändert sich, wer wo und wie zusammenarbeitet. Bis zuletzt wurden die meisten Workshops von Angesicht zu Angesicht geführt. Mit zunehmender Verteilung der Teams verbringen alle mehr Zeit in Online-Workshops. Nun braucht es mutige Menschen, die die Kommunikation zwischen Teams, die teilweise weltweit verstreut zur gleichen Zeit am selben Projekt arbeiten wollen, fördern, aktivieren und begleiten. Die eigentliche Herausforderung liegt darin, Bedingungen zu ermöglichen, unter denen wichtige Diskussionen entstehen und Dialoge sich entwickeln können.

Dieses Buch ist eine umfassende Ressource für Moderatoren, Trainer und Berater. Es beschreibt die Rolle eines Moderators und umreißt dessen Schlüsselelemente in der digitalen Welt. Es untersucht auch die häufigsten Herausforderungen, denen sich Moderatoren in der virtuellen Umgebung gegenüberstehen.

Die Kunst der Online-Moderation – Tools, Ideen und Tipps für die erfolgreiche Umsetzung; Ingrid Gerstbach; Carl Hanser Verlag, 10/2020

BIG DATA UND ANALYTICS

KI UND ML AUF DEM VORMARSCH

Das eBook „Big Data und Analytics" ist deutschsprachig, 44 Seiten lang und das PDF ca. 7 MB groß. Es steht unter diesem Link kostenlos zum Download bereit:
www.it-daily.net/download

Die Datenmenge schwillt rasant an und Prognosen werden immer schwieriger. Hinzu kommen immer mehr unstrukturierte Daten, die auch irgendeine Form der Integration in den Unternehmenskontext bedürfen.

Dieses eBook weist den Weg in die Zukunft von Big Data und Analytics. Deep Data Analytics, Künstliche Intelligenz, Machine Learning und Natural Language Processing heißen die Gefährten.

Highlights aus dem eBook

• BI & Analytics in der Cloud
Wir zeigen Möglichkeiten analytischer Lösungen in der Cloud. Darüber hinaus werden Vorteile als auch Nachteile der Cloud Services kritisch gegenübergestellt. Es werden die drei wichtigen Architekturkomponenten vorgestellt, auf denen Cloud Services in der Regel basieren und konkrete Services sowie deren Anbieter beispielhaft vorgestellt, um Vergleiche zu ermöglichen.

• Datenstrategien für Big Data
Die Verarbeitung von Metadaten wird immer wichtiger, um Daten anhand relevanter Kriterien zu finden. Mit ihnen lassen sich beispielsweise verschiedene Daten zusammenführen, ungleiche Daten unterscheiden oder Ortsangaben machen. Saubere Daten inklusive der passenden Metadaten machen es Organisationen einfacher, einen Wert aus den Daten zu ziehen.

• Next Dimension Big Data
Es geht hier um die Synchronizität von Information und Aktion. Durch performante und frei skalierbare In-Memory-Lösungen wird auf die teuren Multi-Core-Server verzichtet. Stattdessen werden über eine neuartige Technologie leistungsfähige Cluster geschaffen. Viele Standard-Computer werden über nur einen speziell dafür entwickelten Hypervisor zu einem System zusammengefasst.

SOFTWARE QUALITY & TESTING

NEUE ARBEITSGEBIETE FÜR FEHLERFREIEN CODE

Das eBook „Software Quality & Testing" ist deutschsprachig, 52 Seiten lang und das PDF ca. 8 MB groß. Es steht unter diesem Link kostenlos zum Download bereit:
www.it-daily.net/download

Automatisiertes Testen ist heutzutage kein Hexenwerk mehr. Jedes gute Unternehmen entwickelt Software mit automatisierten Unit-Tests und Integrationstests. Es ist klar, dass neue Programmiersprachen und Verfahren die tägliche Arbeit erleichtern. Egal ob DevOps, Low-Code, das Stichwort heißt Evolution.

Highlights aus dem eBook

• Potential- & Prozessanalyse
Wenn Effizienz, Effektivität und Qualität in den Prozessen verbessert oder Methoden, Tools oder Techniken auf den neuesten Stand gebracht werden sollen, dann nur mit Hilfe einer Potenzialanalyse mit Umsetzungs-Roadmap.

• Open Source Risikoanalyse
Veralteter Code, überholte Versionen, fehlende Patches, das ist bei Open Source Normalität. Es gibt einen besorgniserregenden Rückstand bei der Nutzung der neuesten Version von Open-Source-Komponenten.

• Schlüsselwortbasiertes Testen
Wir zeigen, wie ein automatisiertes Umfeld aufgebaut werden kann, so dass manuell arbeitende Tester schon nach einer kurzen Einarbeitung automatisierte Testfälle schreiben und auch verwalten können.

DIE ZUKUNFT DES IT-MITTELSTANDS

MIT IT2MATCH DEN BESTEN PARTNER FÜRS EIGENE UNTERNEHMEN FINDEN

Die Entwicklungen in der IT-Branche schreiten unaufhörlich voran. Um aber auch auf Dauer konkurrenzfähig zu bleiben, fordern disruptive Strukturveränderungen und eine steigende Wettbewerbsintensität neue Strategien von Software-Unternehmen. Die App „IT2match" findet für IT-Unternehmen passende Kooperationspartner, mit denen das eigene Produktportfolio erweitert und die Wertschöpfung gesteigert werden kann.

Besonders in Anbetracht der aktuellen Krise, ist es für die IT-Branche enorm wichtig, kreativ an neuen Services zu arbeiten und Prozesse zu optimieren, um den gesteigerten Bedarf an digitalen Lösungen decken zu können.

Mittelständische Software-Lösungen zählen häufig zu den sogenannten „Best of Breed"-Angeboten, die sich durch eine besonders hohe Funktionalität der abgebildeten Kundenprozesse auszeichnen. Dies ist gerade jetzt wichtig, da sich im Zuge der Digitalisierung die Anforderungen der Anwender an Software verändern und der Bedarf an Interoperabilität steigt.

Kompetenz in allen Bereichen

Viele KMUs sind durch das reguläre Alltagsgeschäft und den steigenden Fachkräftemangel nicht in der Lage, notwendige Schritte hin zur Digitalisierung aus eigener Kraft voran zutreiben. Der Bundesverband IT-Mittelstand e.V. (BITMi) hat hier Handlungsbedarf gesehen und das Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft (KIW), finanziert durch das Bundesministerium für Wirtschaft und Energie, gegründet. Dieses wird ab sofort, gemeinsam mit Partnern, kleine und mittlere IT-Unternehmen bei technischen und unternehmerischen Fragen unterstützen und ihnen bei der notwendigen Vernetzung zur Seite stehen. Hilfestellung werden beispielsweise bei der Suche nach passenden Partnern, bei rechtlichen Fragestellungen, bei der Entwicklung neuer Geschäftsmodelle und bei IT-Schnittstellen gewährt.

Einfaches Matching

Hierfür bietet das KIW die B2B-Matching-Plattform „IT2match" an. Die kostenfreie App ist eine geschlossene Plattform für die vertrauensvolle Vernetzung von Software-Anbietern innerhalb der gesamten IT-Branche. Nach der Registrierung und Beschreibung der eigenen Lösung, erhält das kooperationswillige Unternehmen automatisiert Matching-Vorschläge. Als Orientierung dient die Beschreibung der angebotenen Lösung. Bedeutet: Je präziser das Lösungsprofil erstellt wurde, desto erfolgsversprechender erfolgen die Matching-Vorschläge. Eine aktive Suche und das Anlegen von realisierten Projekten unterstützen das Finden des richtigen Kooperationspartners.

Erste Schritte Richtung Zukunft

IT-Kooperationen helfen, Größennachteile auszugleichen, Kapazitäten, Spezialisierungen und Marktzugänge zu bündeln und sich im Wettbewerb mit anderen Anbietern besser zu behaupten. Erfolgreiche Beispiele, wie CombiPlus, sind die Antwort von KMUs auf die sich ständig verändernden Märkte und den globalen Wettbewerb.

CombiPlus, ein Software-Anbieter für KfZ-Sachverständige, ist es gelungen, mit seinem Kooperationspartner eine integrierte Software-Lösung zu entwickeln, mit der Schadensgutachten unkomplizierter und sicherer abzuwickeln sind. „IT-2match hat uns auf einfache Weise Kooperationsmöglichkeiten geboten, auf die wir sonst nicht aufmerksam geworden wären", betont Stefan Grimm, Geschäftsführer bei CombiPlus, die Bedeutung von kooperativen Geschäfmodellen.

www.itwirtschaft.de

Mittelstand 4.0
Kompetenzzentrum
IT-Wirtschaft

REIFEGRADMODELLE FÜR DIE CYBERSICHERHEIT

UNTERNEHMEN BENÖTIGEN FASSBARE INSTRUMENTE ZUR EVALUATION UND PLANUNG VON CYBERSICHERHEIT

Laut der Allianz-Studie „Risikobarometer" aus dem Jahr 2019 gehörte die Cybersicherheit bereits vor der Corona-Krise zu den wichtigsten Herausforderungen für Unternehmen. Cyberattacken lagen in der Risikobewertung des Versicherers auf Platz eins der möglichen Bedrohungen, dicht gefolgt von Gefahren durch Betriebsunterbrechungen wegen rechtlicher Veränderungen wie Handelskonflikten, Zöllen, Sanktionen oder des BREXITs.

Publikationen zur Cybersicherheit gehen oft nicht differenziert auf die Verortung eines Unternehmens in Bezug auf verfügbare Ressourcen oder Maßnahmen zur schrittweisen Steigerung von Cybersicherheit ein. Unternehmen benötigen fassbare Instrumente und Methoden der langfristigen Planung, die iterativ und berechenbar umgesetzt werden können.

Cyber-Resilienz

Ein Ansatz, unter dem solche Methodiken strukturiert zusammengefasst werden, ist der der Cyber-Resilienz. Mit der Umsetzung dieses ganzheitlichen Konzepts steigert das Unternehmen langfristig die für die Umsetzung nachhaltiger Cybersicherheit relevanten Fähigkeiten:

- **Anpassungsfähigkeit** des IT-Managements und der betrieblichen Infrastruktur, um zukünftigen Bedrohungsszenarien wie Pandemien, Naturkatastrophen oder politischen Konflikten so zu begegnen, dass der Geschäftsbetrieb aufrechterhalten werden kann;
- **Widerstandsfähigkeit** durch Entwicklung eines Maßnahmenplans, um schnell und angemessen zu reagieren, wenn Bedrohungssituationen eintreten;
- **Handlungsfähigkeit** des IT-Managements und der IT-Infrastruktur, um komplexen Bedrohungsszenarien proaktiv zu begegnen und Risiken zu minimieren;
- **Wiederherstellungsfähigkeit** des Geschäftsbetriebs mithilfe von Notfallplänen und eines wirksamen Disaster Recovery Managements;
- **Lernfähigkeit,** um die Erfahrungsbasis des Managements im Umgang mit Krisen sowie die Prozesse zur Abwehr von Bedrohungsszenarien und Wiederherstellung des Geschäftsbetriebs kontinuierlich auszubauen.

Reifegradmodelle

Die so genannte „Maturity" oder der Reifegrad ist ein Maß, mit dem die Fähigkeit einer Organisation zur kontinuierlichen Verbesserung in einer Disziplin wie der Cybersicherheit bestimmt wird. Reifegradmodelle oder „Cybersecurity Maturity Models" (CMM) sind für Unternehmen, die mit der Umsetzung von Cyber-Resilienz beginnen, von besonderem Wert. Sie unterstützen bei der Evaluation gegenwärtiger Fähigkeiten, Ressourcen und vorhandener Infrastruktur. So kann der aktuelle Reifegrad ermittelt und auf dieser Grundlage ein Maßnahmenplan entwickelt werden, um gegebenenfalls die nächste Stufe des Reifegradmodells zu erreichen. Damit ist eine Reihe von Vorteilen verbunden: Das Unternehmen weiß, welche Aufgaben als nächstes anstehen und kann seine Ressourcen und die Investitionsbedarfe entsprechend planen. Ein „Cybersecurity Maturity Model" hilft bei der Sicherstellung der Produktivität und Qualität des Unternehmens sowie der Einhaltung der Budget- und Zeitplanungen.

REIFEGRADMODELLE SIND FÜR UNTERNEHMEN, DIE MIT DER UMSETZUNG VON CYBER-RESILIENZ BEGINNEN, VON BESONDEREM WERT. SIE UNTERSTÜTZEN BEI DER EVALUATION GEGENWÄRTIGER FÄHIGKEITEN, RESSOURCEN UND VORHANDENER INFRASTRUKTUR.

Carsten Marmulla, Managing Partner & Senior Trusted Advisor, carmasec GmbH & Co.KG, www.carmasec.com

Cybersecurity Maturity Model Certification (CMMC)

Reifegradmodelle zum Management der Cybersicherheit sind zuerst im amerikanischen Verteidigungsministerium angewandt worden: Das Pentagon kündigte im Mai 2019 an, dass Lieferantenbetriebe und Dienstleister des „Department of Defense" (DoD) für die Beteiligung an Ausschreibungen die Qualifizierung ihrer Cybersicherheit dokumentieren und nachweisen müssen. Hierfür setzte das Ministerium das Zertifizierungs- und Auditierungsprogramm „Cybersecurity Maturity Model Certification" auf. Damit wurde das Ziel verbunden, diese Unternehmen einer Risikoqualifizierung zu unterziehen und sie gleichzeitig in der Weiterentwicklung ihrer Cybersicherheit zu fördern. Je höher der Reifegrad der Cybersicherheit, den ein Unternehmen erreicht, umso höher die Chance, an Ausschreibungen teilzunehmen.

Das Verteidigungsministerium hat insgesamt fünf Reifegradstufen unterschieden:

– **Level 1:** Basic Cyber Hygiene

– **Level 2:** Intermediate Cyber Hygiene

– **Level 3:** Good Cyber Hygiene

– **Level 4:** Proactive

– **Level 5:** Advanced/Progressive

Das CMMC des amerikanischen Verteidigungsministeriums stellt allerdings in erster Linie eigene Interessen sicher. Die schrittweise Verbesserung der Cybersicherheit der Unternehmen hat nur eine nachgelagerte Priorität.

Cybersecurity Capability Maturity Model (C2M2)

Das amerikanische Energieministerium hat mit dem "Cybersecurity Capability Maturity Model" einen mittlerweile etablierten Ansatz entwickelt. Dieser baut auf dem „Cybersecurity Framework des National Institute of Standard and Technology" (NIST CSF) auf. NIST selbst legt großen Wert darauf, dass das entwickelte Framework in unterschiedlichen Bereichen zum Einsatz kommt.

Beide Modelle unterscheiden folgende fünf Reifegradstufen:

– **Level 1:** Identifizieren

– **Level 2:** Schützen

– **Level 3:** Erkennen

– **Level 4:** Reagieren

– **Level 5:** Genesen

Community Cyber Security Maturity Modell (CCSMM)

Im Mittelpunkt des CCSMM, eines dritten Ansatzes, steht die lokale Wirtschaft (Community). Diese besteht neben Einzelpersonen aus einer Verwaltung, Zivilgesellschaft und Wirtschaftsbetrieben. Das Modell rückt den Menschen stärker in den Mittelpunkt und bietet für die Messbarkeit zur qualitativen und quantitativen Standortbestimmung eines Unternehmens eine Vielzahl an Messgrößen. Diese Metriken beziehen sich allerdings auf die Gesamtheit einer Gemeinschaft. Unternehmen sind davon nur eine Teilmenge.

Dieses Reifegradmodell unterscheidet folgende fünf Stufen:

- **Level 1:** „Security Awareness" (Sicherheitsbewusstsein): In dieser Stufe gilt es, ein hohes Maß an Bewusstsein für Cybersicherheit zu fördern.

- **Level 2:** „Process Development" (Prozessentwicklung): In dieser Stufe stehen die Prozesse und Richtlinien im Vordergrund.

- **Level 3:** „Information Enabled" (Informationspolitik): Voraussetzung für diese Stufe ist, dass die Organisationsmitglieder das erforderliche Sicherheitsbewusstsein besitzen und in der Organisation entsprechende Prozesse existieren, damit Informationen wirksam fließen können, um Bedrohungen zügig zu erkennen und beseitigen.

- **Level 4:** „Tactics Development" (Taktikentwicklung): In dieser Stufe verfügt das Unternehmen bereits über die Fähigkeit (und die dazugehörigen Pläne), um Bedrohungsszenarien proaktiv zu erkennen und zu beseitigen. Prävention spielt an diesem Punkt eine wichtige Rolle.

- **Level 5:** „Full Security Operational Capability" (Volle Betriebsfähigkeit in Cybersicherheit): In dieser Reifegradstufe erfüllt das Unternehmen nicht nur alle zuvor genannten Voraussetzungen. Zusätzlich wirken die Prozesse und Mechanismen durchgehend im gesamten Unternehmen. Darüber hinaus kann es sich mit anderen relevanten Unternehmen und Institutionen vernetzen, um auf ein komplexes Bedrohungsszenario zu reagieren.

Das Reifegradmodell unterscheidet hierbei zwischen verschiedenen Bedrohungssituationen:

➤ **Unstrukturierte Bedrohungen:** Kriminelle verfolgen kurzfristige Effekte, ohne die gesamte Betriebsfähigkeit gefährden zu wollen. Ein typischer Angriff ist „CEO-Fraud", um die schnelle Überweisung von Geldern zu erwirken.

➤ **Strukturierte Bedrohungen:** Hinter den Angriffen steckt oft eine organisierte Gruppe. Die Attacken sind geplant und die Verantwortlichen gehen methodisch vor. Ihr Ziel ist nicht, sich zu bereichern, sondern an sensible Informationen zu gelangen oder die Betriebsfähigkeit zu beeinträchtigen. Neben Kriminellen gehören zur Tätergruppe auch (politische) Aktivisten, so genannte „Hacktivisten".

➤ **Hochgradig organisierte Bedrohungen:** Angriffe auf diesem Niveau haben das Ziel, die Betriebsfähigkeit zu beeinträchtigen. Zu den Zielen der Angreifer zählt nicht nur die Informationsgewinnung, sondern auch die Vernichtung von Informationen. Die Gruppe ist in der Regel hochgradig organisiert, verfügt über ein großzügiges Budget und greift auf multidisziplinäre Kompetenzen zurück. Die Angriffe finden oft in Kombination mit physischen und psychischen Bedrohungen statt.

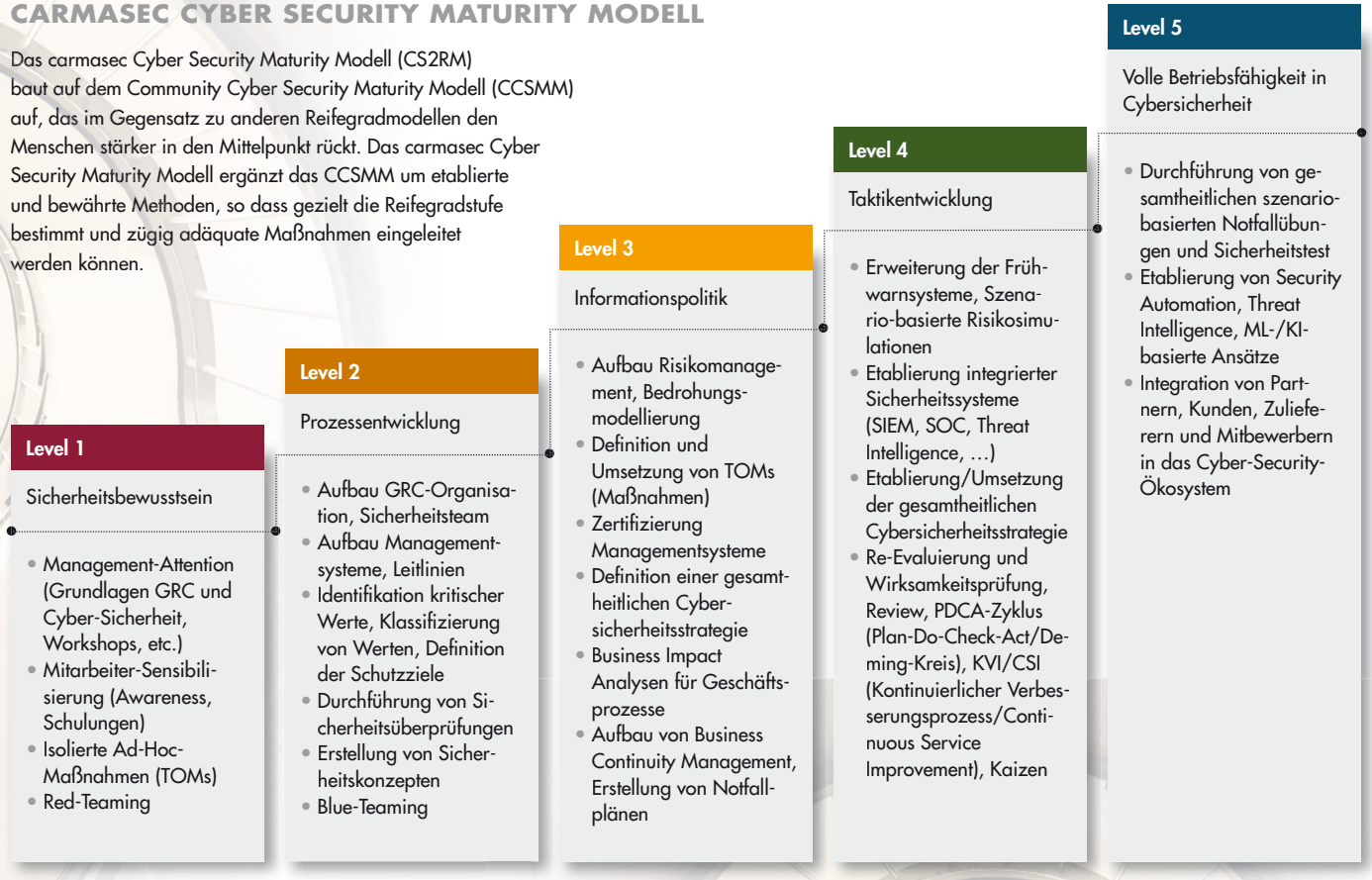
Bei der Betrachtung der verschiedenen Bedrohungssituationen wird deutlich,

AUSGEWÄHLTE REIFEGRADMODELLE ZUR CYBERSICHERHEIT IM VERGLEICH

Bedrohungslage	**unstrukturiert**		**strukturiert**		**hochgradig strukturiert**
Reifegradstufe	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
CMMC	Basic Cyber Hygiene	Intermediate Cyber Hygiene	Good Cyber Hygiene	Proactive	Advanced/Progressive
C2M2	Identifizieren	Schützen	Erkennen	Reagieren	Genesen
CCSMM	**Sicherheitsbewusstsein** *(Security Awareness)*	**Prozessentwicklung** *(Process Development)*	**Informationspolitik** *(Information Enabled)*	**Taktikentwicklung** *(Tactics Development)*	**Volle Betriebsfähigkeit in Cybersicherheit** *(Full Security Operational Capability)*
Beschreibung	In dieser Stufe gilt es insbesondere bei Organisationsmitgliedern ein hohes Maß an Bewusstsein für Anliegen der Cybersicherheit zu fördern.	In dieser Stufe stehen die Prozesse und Richtlinien im Vordergrund. Diese gewährleisten, dass Cybersicherheit im Betrieb funktioniert.	Voraussetzung für diese Stufe ist, dass die Organisationsmitglieder über das erforderliche Sicherheitsbewusstsein verfügen und in der Organisation entsprechende Prozesse existieren, damit Informationen wirksam fließen können, um zügig Bedrohungen zu erkennen und zu beseitigen.	In dieser Stufe verfügt das Unternehmen bereits über die Fähigkeit (und Pläne), um Bedrohungsszenarien proaktiv zu erkennen und zu beseitigen. Prävention spielt an diesem Punkt eine wichtige Rolle.	In dieser Reifegradstufe erfüllt das Unternehmen nicht nur alle zuvor genannten Voraussetzungen. Die Prozesse und Mechanismen wirken im gesamten Unternehmen durchgehend. Darüber hinaus kann es sich mit relevanten Unternehmen und Institutionen vernetzen, um auf ein komplexes Bedrohungsszenario zu reagieren.

CARMASEC CYBER SECURITY MATURITY MODELL

Das carmasec Cyber Security Maturity Modell (CS2RM) baut auf dem Community Cyber Security Maturity Modell (CCSMM) auf, das im Gegensatz zu anderen Reifegradmodellen den Menschen stärker in den Mittelpunkt rückt. Das carmasec Cyber Security Maturity Modell ergänzt das CCSMM um etablierte und bewährte Methoden, so dass gezielt die Reifegradstufe bestimmt und zügig adäquate Maßnahmen eingeleitet werden können.



dass nicht jedes Unternehmen die höchste Reifegradstufe erreichen muss. Strebt ein Unternehmen allerdings Wachstum an, geht dies mit Änderungen in der Wertschöpfungskette, des Geschäftsmodells und der Märkte einher. Hierdurch kann sich die Bedrohungslage ändern.

Das carmasec Cybersecurity Reifegradmodell (CS2RM)

In der Cybersicherheit stellen Reifegradmodelle einen sehr jungen Ansatz dar. Existente Modelle aus dem angelsächsischen Raum können nicht vollständig auf die Anforderungen deutschen Unternehmen übertragen werden. Daher hat die Beratungsboutique für Cybersicherheit carmasec auf Basis des „Community Cyber Security Maturity Model" (CCSMM) einen auf die Anforderungen deutscher Unternehmen angepassten Ansatz entwickelt. Für seine Anwendbarkeit sieht das „carmasec Cybersecurity Reifegradmodell" einen Assessment-Prozess vor, in dem ein Unternehmen zu Beginn hinsichtlich der gegenwärtigen Cybersicherheit (Architektur, Richtlinien, Kultur, Technologien) auditiert wird. Es erfolgt eine Standortbestimmung im Reifegradmodell. Sie stellt dabei eine Art Blaupause dar, mit der der Handlungs- und Optimierungsbedarf des Unternehmens sichtbar gemacht wird. Auf dieser Grundlage werden ein Maßnahmenkatalog und ein Fahrplan entworfen, welche durch eine Investitions- und Budgetplanung ergänzt werden. Durch Monitoring und Evaluation der Maßnahmen wird der Fortschritt kontinuierlich bewertet und geprüft. Sind die Anforderungen der Reifegradstufe erfüllt, wird entschieden, ob die nächste Reifegradstufe abhängig von der Geschäftsstrategie angestrebt werden soll.

So kann ein Unternehmen zielgerichtete Handlungsmaßnahmen definieren, Budgets zuweisen, den Fortschritt kontinuierlich überwachen und entsprechend der Geschäftsstrategie einen sinnvollen Zeitplan festlegen, um dann die nächste Reifegradstufe anzustreben.

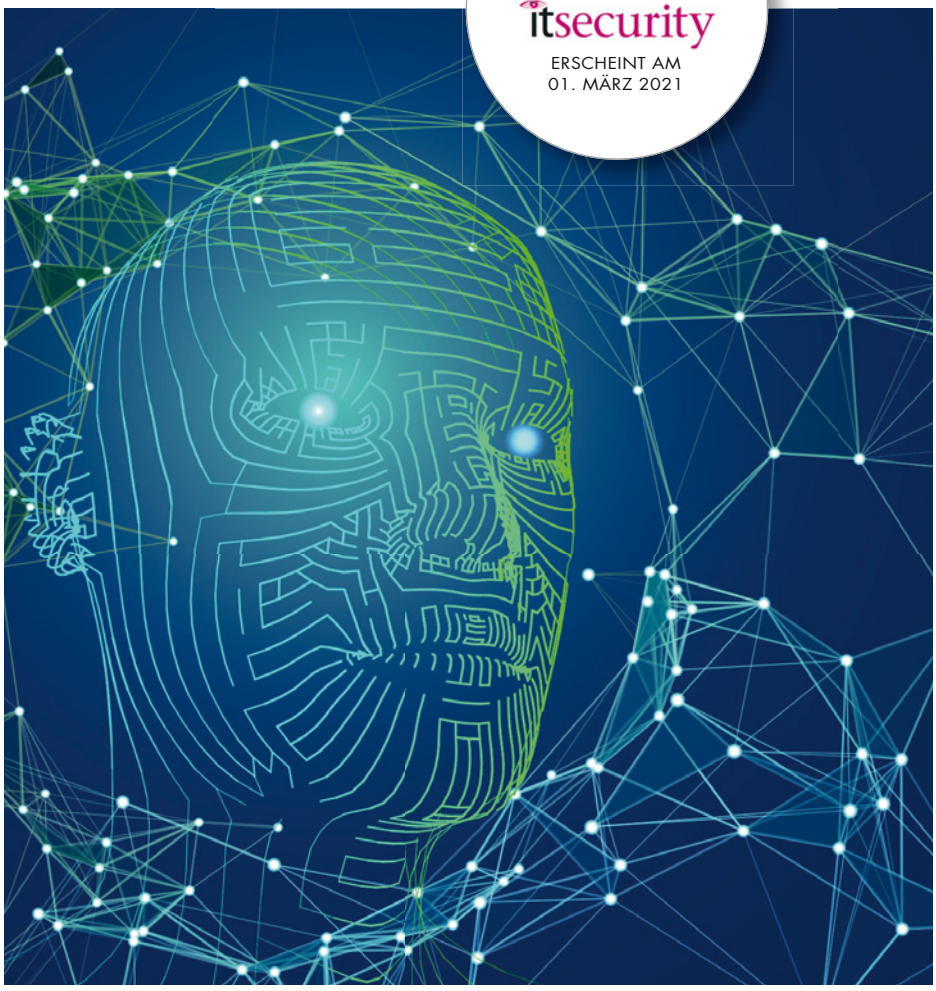
Carsten Marmulla

SIND REIFEGRADMODELLE WIRKSAM?

In einer fundierten Studie „Value of maturity models in performance measurement", fassen die Wissenschaftlerinnen und Wissenschaftler S. Bititcia, Patrizia Garengob, Aylin Atescand und Sai S. Nudurupat ihre Untersuchung zur Wirksamkeit in zwölf Fertigungsbetrieben zusammen. Sie gelangen zu der Erkenntnis, dass organisatorisches Lernen und die Managementfähigkeiten durch Planung, Einführung und Evaluation mithilfe von Reifegradmodellen verbessert werden.

Quelle: Umit S. Bititci, Patrizia Garengo, Aylin Ates & Sai S. Nudurupati (2015) Value of maturity models in performance measurement, International

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
01. MÄRZ 2021



KÜNSTLICHE INTELLIGENZ

Struktur im Servicedesk

FLEXIBLE ERP-LÖSUNG

Transparente Prozesse

CLOUD COMPUTING

In Zukunft Multi-Cloud?

DIE AUSGABE 01/02 VON IT MANAGEMENT ERSCHEINT AM 31. JANUAR 2021.

INSERENTENVERZEICHNIS

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Carina Mitzschke, Silvia Parthier (-26)

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Dr. Martin Anduschus, Holger Dörnemann, Martin Landis, Stephen Mann, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Jens Reichardt, Klaus Schulz, Sebastian Weber

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 veröff entlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenver arbeitungsanlagen 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 Veröff entlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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. 28.
Preisliste gültig ab 1. Oktober 2020.

Mediaberatung & Content Marketing-Lösungen it management | it security | it daily.net:
Kerstin Fraenzke
Telefon: 08104-6494-19
E-Mail: berthmann@it-verlag.de

Karen Reetz-Resch
Home Office: 08121-9775-94,
Mobil: 0172-5994 391
E-Mail: reetz@it-verlag.de

Online Campaign Manager:
Vicky Miridakis
Telefon: 08104-6494-21
miridakis@it-verlag.de

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

Erscheinungsweise:
10x pro Jahr

Verkaufspreis:
Einzelheft 10 Euro (Inland),
Jahresabonnement, 100 Euro (Inland),
110 Euro (Ausland), Probe-Abonnement
für drei Ausgaben 15 Euro.

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 Bezugs zeitraumes 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

Folge uns auf Social Media:

Suchen: IT-Profis.
Bieten: Deutschland.

Jetzt beim ITZBund bewerben und unsere Zukunft digital gestalten.
Digital-für-Deutschland.de

Informations
Technik
Zentrum Bund

itsecurity
DEZEMBER 2020

DAS SPEZIAL

WatchGuard
Synergieeffekte und Innovationen
ab Seite 6

proofpoint.
Aktuelle CISO-Studie
ab Seite 8

CYBERVERSICHERUNG

WAS IST HEUTE MÖGLICH?

Sabine Träumer, AXA

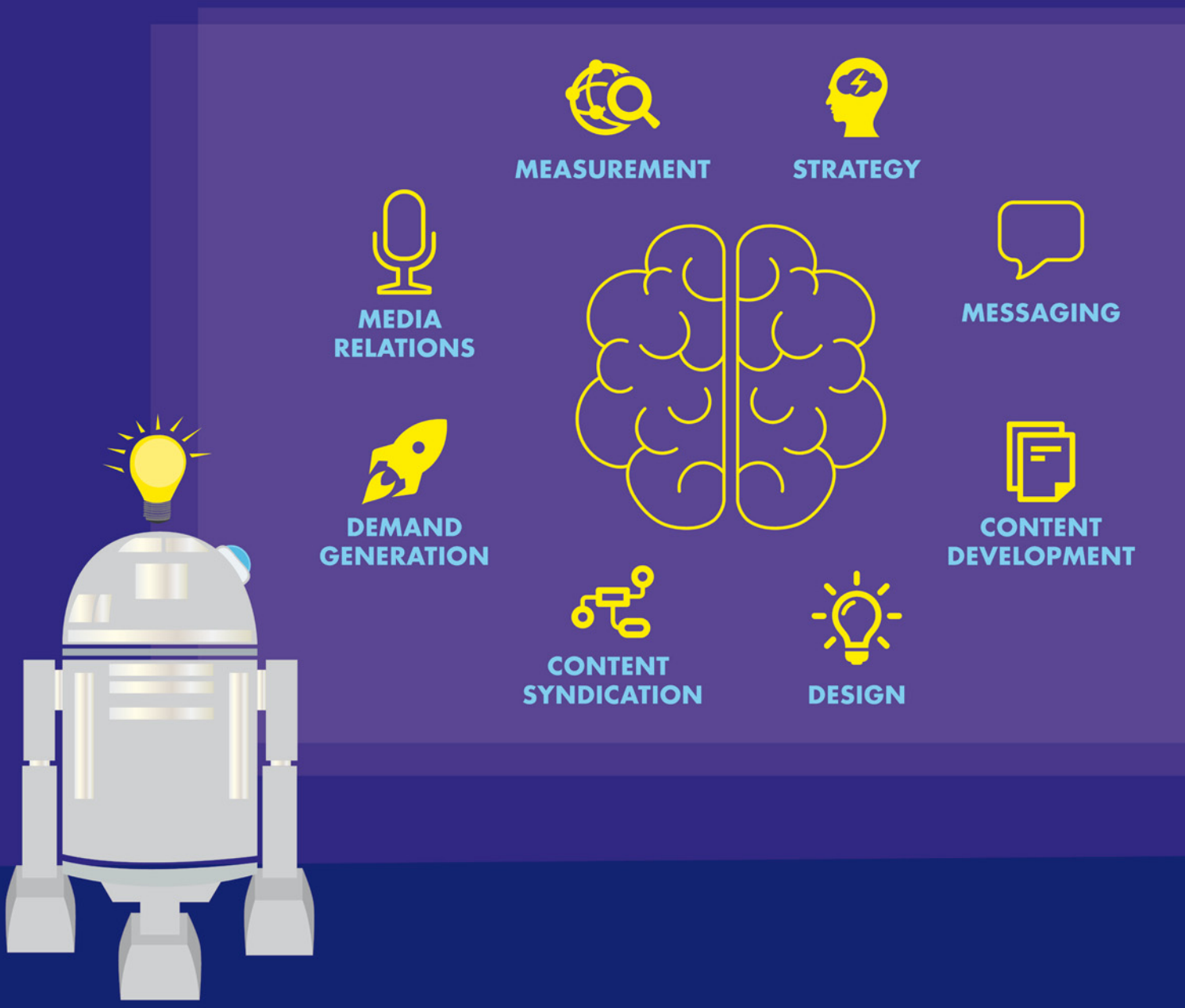
MANAGED DETECTION
Das schwächste Glied

SOC AS A SERVICE
Helfer in der Cyber-Not

CYBER-SICHERHEIT
Frühe Risikoerkennung

www.it-daily.net

Thought Leadership



KÜNSTLICHE INTELLIGENZ
THOUGHT LEADERSHIP

4 COVERSTORY

10

16

INHALT

VERSICHERUNGSSCHUTZ BEI CYBERSECURITY-ANGRIFFEN

WAS IST HEUTE MÖGLICH?

Cyberangriffe an sich sind schon eines der großen IT-Probleme. Was, wenn kein Versicherungsschutz vorliegt? Sabine Träumer, Leiterin Cyberversicherung im Industriekundengeschäft bei AXA in Deutschland im Interview mit it management-Herausgeber Ulrich Parthier.

Ulrich Parthier: *Mittlerweile gibt es unzählige Berichte über Cyberangriffe. Eindeutig ist vor allem eins: die steigende Tendenz. Es geht nur in eine Richtung, nach oben. Sind die deutschen Unternehmen darauf vorbereitet?*

Sabine Träumer: Nein, eher nicht. Insbesondere weil Angriffe nicht zeitig genug erkannt werden und dementsprechend nicht schnell genug reagiert wird. Durchschnittlich „verweilt" Malware sechs Monate unerkannt im Unternehmens-Netzwerk bevor der Schaden entsteht.

Neben häufigeren Angriffen beobachten wir aber auch mehr und mehr gravierende finanzielle Folgen von Cyber-Attacken. Wir sehen daher noch starken Verbesserungsbedarf.

Ulrich Parthier: *Wie verändern sich Quantität und Qualität der Angriffe und welcher Art sind sie?*

Sabine Träumer: Durch die zunehmende Digitalisierung gibt es auch fast zwangsläufig eine immer größer werdende Menge von zum Beispiel Hacker-Angriffen. Man kann fast von einer Kommerzialisierung der Cyber-Kriminalität reden, mit all ihren Begleiterscheinungen: Spezialisierung auf bestimmte Hacks oder „Gesamt-Angriffe" mit Arbeitsteilung gegen Provision, also wenn beispielsweise ein Angreifer darauf spezialisiert ist, im Netzwerk eines Unternehmens eine Hintertür für das Eindringen von Schadsoftware einzubauen und diese „Dienstleistung" im Darknet dem Höchstbietenden anbietet, damit andere einen Angriff durchführen können. Häufigkeit, Struktur und Professionalität haben dabei zugenommen – fast schon wie „Cyber Crime as a Service".

Ulrich Parthier: *Aktiver Schutz bedeutet für die Unternehmen Investitionen in die IT-Infrastruktur. Gibt es mehrheitlich ein mehrstufiges Schutzkonzept?*

Sabine Träumer: Das stellt man sich am besten wie ein Zwiebel-Konzept vor, wobei jede einzelne Schicht dafür sorgen soll, dass kein Eindringen erfolgt. Am Beispiel Phishing-Mails kann man das anschaulich verdeutlichen. Der erste technische Schutz sind Mailfilter und eine Netzwerk-Firewall. Danach kommt es auf die Aufmerksamkeit der MitarbeiterInnen des Unternehmens an, die leider immer noch das häufigste Einfallstor für Hacker darstellen. Bei manipulierten Texten sprechen wir von extrem genauen, oftmals

bis auf winzige Details identisch wirkende Firmen-Korrespondenzen, die es durch das Ausführen bestimmter Dateien Angreifern ermöglicht, ins Unternehmensnetzwerk einzudringen.

In der nächsten Schicht ist es absolut notwendig, weitere gezielte und zum Unternehmen passende Maßnahmen zu ergreifen, schnell zu reagieren – das geht dann vom Notfall-Konzept bis hin zu einem Backup, das im Fall der Fälle die Datenrekonstruktion erleichtert oder ermöglicht.

Dabei gilt die Faustregel: Je größer ein Unternehmen, desto mehr Professionalität ist bei der IT-Sicherheit notwendig.

? **Ulrich Parthier:** *Professionelle Hilfe?*

Sabine Träumer: Ja, auch wenn IT-Fachkräfte hart umkämpft und teuer sind, gibt es alternativ auch IT-Dienstleister, die optimaler Weise schon im Vorfeld mit Versicherungsunternehmen kooperieren. So ist man gut aufgestellt.

Der beste Schaden ist immer noch der, der erst gar nicht passiert und wenn doch, dann gilt es, die Belastungen für Kunden und Partner der betroffenen Unternehmen so gering wie möglich zu halten. Vor diesem Hintergrund haben wir in Kooperation mit dhpg ein sogenanntes Security Operations Center (SOC) in unser Service-Portfolio integriert. Damit sollen unerwünschte Besucher schon beim Versuch des Eindringens ins Unternehmensnetzwerks abgewehrt werden.

Das SOC von AXA und dhpg übernimmt die aktive Überwachung und Analyse aller integrierten Systeme, erkennt IT-Schwachstellen, alarmiert bei Bedrohungen und berichtet unverzüglich an die IT-Verantwortlichen – und das zu einem bezahlbaren Preis.

Ein auffälliger Zugriff kann so bestenfalls in Echtzeit eliminiert, seine Auswirkungen auf jeden Fall minimiert werden. Auf Wunsch kann das SOC aktiv einschreiten und kritische Systeme aus der Gefahrenzone nehmen und somit Sicherheitslücken schließen.

Es kommt immer darauf an schnell zu reagieren – in einer Situation, in der man schon mal leicht den Kopf verlieren und in Panik geraten kann, wird man durch das SOC an die Hand genommen. Mit dieser Lösung vereinfachen wir die mittlerweile sehr komplexe Risikosituation und entlasten die Unternehmen bei ihrer IT-Governance.

? **Ulrich Parthier:** *Wie können sich KMUs am besten informieren?*

Sabine Träumer: Allgemein lohnt sich immer ein Blick auf die Informationen des Bundesamts für Sicherheit in der Informationstechnik (BSI). Bei AXA haben wir dazu ein ganzes Ökosystem im Kontext Cyber aufgebaut. Neben dem SOC können damit MitarbeiterInnen unserer Kunden zielgerichtet informiert und geschult werden. Mit unserem Partner 8com bieten wir in diesem Zusammenhang ein sogenanntes Awareness Portal an. Damit packen wir das Problem bei der Wurzel und arbeiten präventiv. Denn auch wenn die Mitarbeitenden häufig das Einfallstor für schadhafte Malware im Unternehmen sind, so können sie auch ein funktionierendes Bollwerk dagegen werden.

? **Ulrich Parthier:** *Werden Cyberversicherungen heute schon als Präventivmaßnahme gesehen oder erst nach dem ersten Schadensfall abgeschlossen?*

Sabine Träumer: Sowohl als auch – denn trotz bester Präventivmaßnahmen kann niemand hundertprozentig vor Angriffen sicher sein und eine Cyberversicherung hilft nicht nur den monetären Schaden zu begrenzen. Wir bieten unseren Kunden einen individuellen Schutz, je nach Bedarf, Unternehmensgröße und Absicherungswunsch. Dazu haben wir ein modulares Bausteinsystem entwickelt, das inhaltliche und preisliche Anpassungen ermöglicht. Unser Angebot umfasst alle notwendigen Inhalte, um finanzielle Folgen einer erfolgreichen Cyber-Attacke auszumerzen. Von der Datenwiederherstellung oder -rettung, Forensik-/Sachverständigenkosten über Kosten, die entstehen, weil ein Unternehmen aufgrund des Cyber-Schadens nicht wie gewohnt arbeiten kann, bis hin zum Krisen- und Reputationsmanagement oder Schutz vor Ansprüchen Dritter.

? **Ulrich Parthier:** *Die verschiedenen Branchen haben doch sehr unterschiedliche Anforderungen. Wie können Sie diese abdecken?*

Sabine Träumer: Der Angriff mit Malware bleibt ein Angriff mit Malware, aber natürlich gibt es unterschiedliche Erwartungen an die IT-Sicherheit je nach Branche. Die Cyberversicherung ist kein „Produkt von der Stange", sondern sollte für jeden Kunden individuell zusammengesetzt werden. Nehmen wir zum Beispiel Krankenhäuser, die sehr viele personenbezogene Daten verwalten. Hier gilt es mit spezifischen Maßnahmen diese zu schützen. Bei Fertigungsbetrieben geht es hingegen verstärkt darum, das Risiko einer Betriebsunterbrechung zu minimieren.

Wir beraten hier durch unseren hauseigenen Risikoingenieur in Zusammenarbeit mit unseren technisch geschulten Underwritern, um den optimalen Schutz zu ermitteln. Für uns ist es wichtig, ein begleitender Partner unserer Kunden zu sein und nicht erst im Schadenfall zu reagieren.

! **Ulrich Parthier:** *Frau Träumer, wir danken für das Gespräch!*

WATCHGUARD UND PANDA

SYNERGIEEFFEKTE UND INNOVATIONSGEDANKE ALS TREIBENDE KRÄFTE

Durch den Zusammenschluss der beiden Unternehmen ist ein schlagkräftiges Portfolio in puncto IT-Sicherheit entstanden. Ulrich Parthier, Publisher it security, sprach darüber mit Michael Haas, Vice President Central Europe bei WatchGuard Technologies.

Ulrich Parthier: *Was war die Intention der Übernahme von Panda Security?*

Michael Haas: Für uns spielten vor allem zwei Punkte eine wichtige Rolle: Zum einen ist der technologische Ansatz von Panda natürlich extrem spannend. Cloudbasierte Endpoint Security unter Einbeziehung von KI und Machine Learning stellt die logische Ergänzung unseres eigenen Portfolios dar. Hier gehört Panda mit seinen Produkten – allen voran Panda Adaptive Defense 360 – ganz sicher zu den fortschrittlichsten Anbietern im Markt. Zum anderen ist die Übernahme für uns mit einem signifikanten Ausbau des Vertriebsnetzwerks verbunden. Da es hinsichtlich der Partnerlandschaften von WatchGuard und Panda bisher kaum Überschneidungen gab, können wir unsere Schlagkraft im Channel hierzulande nahezu verdoppeln. Die kombinierte Lösungspalette wird von der Mehrzahl der Vertriebspartner auf beiden Seiten sehr gut angenommen. Schließlich sind diese nun in der Lage, ihren Kunden ein noch umfangreicheres Leistungsspektrum anzubieten – und das alles aus einer Hand. Dass sich die DNAs von WatchGuard und Panda so ähneln, sehen wir dabei als entscheidenden Vorteil. Beide Unternehmen fühlen sich seit jeher dem Mittelstand verpflichtet und haben frühzeitig das Potenzial der Cloud erkannt. Aus unserer Sicht kommt also zusammen, was zusammengehört.

Ulrich Parthier: *Es gibt jetzt vier Säulen im Portfolio: Netzwerksicherheit, Multifaktor-Authentifizierung, sicheres cloudbasiertes WLAN und Endpoint Security. Wie ist diese Ausrichtung strategisch zu verstehen?*

Michael Haas: Wir vereinen auf diese Weise hochentwickelte Technologien, die konsequenten Schutz vom Perimeter bis zum Endpunkt gewährleisten – wobei insbesondere die Zusammenführung all dieser Funktionen in der Cloud den Anforderungen mittelständischer Unternehmen nachhaltig Rechnung trägt. Ziel ist die nahtlose Verbindung zwischen Netzwerk- und Endpunktschutz bei gleichzeitig zentralisierter Verwaltung. Alle Module des Leistungsspektrums bleiben aber nach wie vor auch einzeln erhältlich beziehungsweise können je nach Bedarf beliebig kombiniert werden.

Ulrich Parthier: *Die Sicherheit im Homeoffice ist derzeit das beherrschende Thema. Welche Lösungen bieten Sie hier den Unternehmen?*

SECURITY IM TANDEM

Michael Haas: Gerade im Homeoffice ist der Schutz der Endpunkte von entscheidender Bedeutung. Arbeitgeber müssen Lösungen finden, mit denen sich Mobilität und der Schutz der Unternehmensressourcen bestmöglich in Einklang bringen lassen. In dem Zusammenhang haben wir mit WatchGuard Passport ein Rundumsorglos-Paket geschnürt, welches neben der Multifaktor-Authentifizierungslösung AuthPoint und DNS-Filtern am Endpunkt mittlerweile auch Panda Adaptive Defense mit seinem umfangreichen Leistungsspektrum umfasst. Dieses reicht von fortschrittlichem Virenschutz über Endpoint Detection and Response (EDR), Patch-Management, Inhaltsfiltern und E-Mail-Sicherheit bis hin zur Datenträgerverschlüsselung. Neben der ausgefeilten Methodik zur Gefahrenerkennung und -abwehr besticht die neue Kernkomponente des WatchGuard-Produktspektrums für Endpoint Security vor allem durch die Einfachheit und Benutzerfreundlichkeit der Management-Konsole. Auf Basis spezieller Machine-Learning-Algorithmen werden ausnahmslos alle Prozesse und Ereignisse am Endpunkt durchleuchtet, um jede einzelne ausführbare Datei zu klassifizieren. Es gibt nur dann eine Warnung, wenn tatsächlich Gefahr besteht, wobei entsprechende Endgeräte automatisch isoliert werden. Das Ergebnis: maximale Kontrolle der laufenden Prozesse bei gleichzeitiger Verringerung der Angriffsfläche.

Ulrich Parthier: *Stichwort „Verringerung der Angriffsfläche": Ist das der Grund, warum sie das Dark Web beobachten?*

Michael Haas: Exakt. Im Dark Web finden Hacker seit Jahren eine ideale Plattform, um sensible Informationen wie Zugangsdaten, die im Zuge von Sicherheitslecks erbeutet wurden, illegal zum Verkauf anzupreisen. Das Fatale: Unternehmen wissen meist nicht einmal, dass „ihre" Daten hier bereits gehandelt werden. Daher bieten wir über unsere Webseite seit einiger Zeit jedem Interessierten die kostenlose Möglichkeit für einen individuellen Dark Web Scan. Dazu muss einfach nur die Firmen-Domain angegeben werden und in Sekundenschnelle ist klar, ob es konkreten Anlass zur Sorge gibt. Zusätzlich kann eine detaillierte Analyse angefordert werden, die dabei unterstützt, die potenzielle Gefahr genauer zu spezifizieren.

WATCHGUARD UND PANDA FÜHLEN SICH SEIT JEHER DEM MITTELSTAND VERPFLICHTET UND HABEN FRÜHZEITIG DAS POTENZIAL DER CLOUD ERKANNT. AUS UNSERER SICHT KOMMT ALSO ZUSAMMEN, WAS ZUSAMMENGEHÖRT.

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

Ulrich Parthier: *Was gibt es darüber hinaus produktseitig Neues auf der klassischen WatchGuard-Schiene?*

Michael Haas: Trotz der aktuellen Erweiterung unseres Gesamtportfolios ist das Thema Netzwerksicherheit für uns natürlich nach wie vor ein strategischer Grundpfeiler. Hier laufen die Entwicklungstätigkeiten auf Hochtouren. So haben wir im Sommer mit unseren neuen Tabletop-Appliances zur Absicherung kleiner und mittelgroßer Netzwerkumgebungen und auch Homeoffices in Sachen Leistungsstärke eine ganze Schippe draufgelegt. Dies gilt auch für unsere jüngsten High-End-Appliances Firebox M4800 und M5800. Mit einem Firewall-Datendurchsatz von bis zu 87 Gbit/s und einem UTM-Datendurchsatz von bis zu 11,3 Gbit/s, vielschichtiger Sicherheitsfunktionalität sowie bedarfsgerechter hoher Portdichte eignen sie sich insbesondere als Knotenpunkt in der Unternehmenszentrale – mit optimalem Preis-Leistungs-Verhältnis.

Ulrich Parthier: *Was plant Ihr Unternehmen als nächstes?*

Michael Haas: Im Moment steht für uns im Fokus, den Mehrwert des erweiterten Portfolios noch greifbarer zu machen. Über die produktseitige Integration der Panda-Lösungen sollen die operativen Potenziale im Hinblick auf zentralisierte Verwaltungsoptionen konsequent erschlossen werden – damit es unseren Kunden künftig noch leichter fällt, kompromisslosen Schutz vom Netzwerk bis zum Endpunkt sicherzustellen.

Ulrich Parthier: *Herr Haas, wir danken für das Gespräch!*

AKTUELLE CISO-STUDIE

ZWEI VON DREI UNTERNEHMEN BEREITS OPFER VON CYBERKRIMINELLEN

Proofpoint, der US-amerikanische Cybersecurity-Spezialist, hat im Juli und August eine Vielzahl von CISOs und CSOs in Deutschland, Österreich und der Schweiz zum Thema Cybersecurity befragt – und dabei erstaunliche Widersprüche zwischen der aktuellen Bedrohungslage und dem Verhalten vieler Cybersecurity-Verantwortlichen entdeckt. Darüber sprach Ulrich Parthier, Herausgeber it security, mit Irene Marx, Country Manager Österreich und Schweiz bei Proofpoint.

Ulrich Parthier: *Frau Marx, wo stehen wir denn in Europa, genauer gesagt in Deutschland, Österreich und der Schweiz beim Thema Cybersecurity?*

Irene Marx: So pauschal lässt sich das natürlich nicht beantworten. Allerdings ist die Situation zurückhaltend ausgedrückt bedenklich. Schon heute sind zwei Drittel aller Unternehmen mit mehr als 250 Mitarbeitern nicht nur mit Angriffsversuchen konfrontiert gewesen, sondern sie sind bereits kriminellen Hackern zum Opfer gefallen, ein aus meiner Sicht höchst alarmierender Wert.

Ulrich Parthier: *Woran liegt das? Haben diese Unternehmen mangelhafte IT-Sicherheitslösungen im Einsatz?*

Irene Marx: Das glaube ich kaum. Wir treffen heute bei unseren Kunden eigentlich kein Unternehmen mehr an, dass nicht erhebliche Mittel für die IT-Security aufwendet. Allerdings gibt es hier eine deutliche Diskrepanz zwischen den Ausgaben für die IT-Sicherheit und der Bedrohungslage. Denn Hacker greifen heutzutage nur in den seltensten Fällen die technischen Schwachstellen von Systemen an oder nutzen Sicherheitslücken aus. Sie fokussieren sich vielmehr auf ein deutlich leichter zu knackendes Einfallstor: den Menschen. Dafür ist oft nicht viel mehr nötig als eine gut gemachte E-Mail, mit oder ohne Anhang, die den Mitarbeiter zu einer unbedachten Aktion verleitet.

Ulrich Parthier: *Wie funktioniert das? Und was sind die Folgen?*

Irene Marx: Das ist gar nicht schwierig. Die Kriminellen senden eine E-Mail unmittelbar an einzelne Mitarbeiter, oft mit gefälschtem Absender und frei erfundenen, aber auf die potenziellen Opfer maßgeschneidert zugeschnittenen Inhalten. Auf diese Weise sollen die Angestellten dazu verleitet werden, sensible Daten preiszugeben oder direkt Geld auf die Konten der Kriminellen zu überweisen. Fallen Mitarbeiter auf die Tricks der Betrüger herein, sind die Schäden oft noch sehr lange spürbar. So hatten vier von zehn der befragten Unternehmen in unserer Umfrage den Verlust sensibler Daten zu beklagen. Etwa genauso viele verzeichneten Störungen in den Betriebsabläufen.

Ulrich Parthier: *Sind denn die Unternehmen auf die Angriffe nicht vorbereitet?*

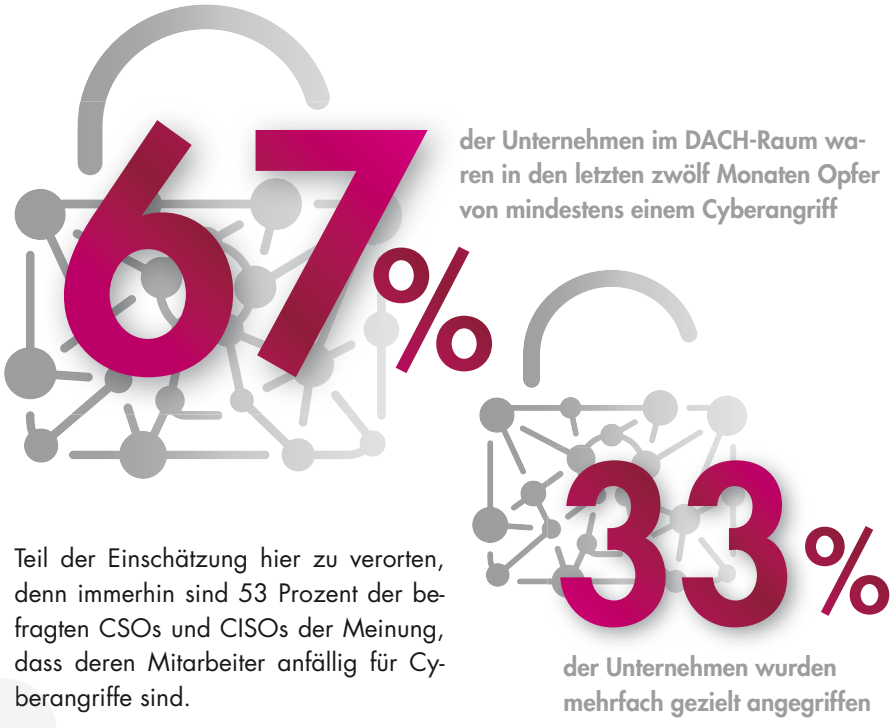
Irene Marx: Sagen wir so: Die einen mehr, die anderen weniger. Und es betrifft nicht nur Unternehmen, sondern auch die öffentliche Hand. So haben wir in unserer Studie herausgefunden, dass drei von vier Unternehmen nach eigenen Angaben nicht optimal auf digitale Angriffe vorbereitet sind. Lediglich 24 Prozent aller Befragten konnten die Frage, ob sie auf eine Cyberattacke vorbereitet seien, vorbehaltlos bejahen.

Aber besonders beunruhigt haben mich die Angaben aus der öffentlichen Verwaltung, denn während etwa dreiviertel der Unternehmen zumindest teilweise auf digitale Attacken vorbereitet sind, liegt dieser Wert im Public Sector bei nur 46 Prozent. Das heißt, nicht einmal jede zweite Behörde, jedes zweite Amt ist auf Hackerangriffe vorbereitet.

Ulrich Parthier: *Sie sagten, dass Mitarbeiter das bei weitem beliebteste Angriffsziel sind, um dem Unternehmen Schaden zuzufügen. Ist das der Grund, dass die Unternehmen sich nicht als ausreichend vorbereitet erachten?*

Irene Marx: Es erscheint durchaus naheliegend, wenigstens einen bedeutenden

> HACKER GREIFEN HEUTZUTAGE NUR IN DEN SELTENSTEN FÄLLEN DIE TECHNISCHEN SCHWACHSTELLEN VON SYSTEMEN AN ODER NUTZEN SICHERHEITSLÜCKEN AUS. SIE FOKUSSIEREN SICH VIELMEHR AUF EIN DEUTLICH LEICHTER ZU KNACKENDES EINFALLSTOR: DEN MENSCHEN.
>
> Irene Marx, Country Manager Österreich und Schweiz, Proofpoint, www.proofpoint.com



Teil der Einschätzung hier zu verorten, denn immerhin sind 53 Prozent der befragten CSOs und CISOs der Meinung, dass deren Mitarbeiter anfällig für Cyberangriffe sind.

Was ich allerdings nicht wirklich verstehe, ist umgekehrt die Haltung der Verantwortlichen: Sie erkennen, dass Mitarbeiter durchaus auf gut gemachte Fälschungen legitimer E-Mails hereinfallen können, sparen jedoch gleichzeitig daran, die Angestellten genau davor durch regelmäßige Trainings besser zu schützen. Mehr als dreiviertel – genauer 77 Prozent – der Unternehmen schulen höchstens zwei Mal pro Jahr in Sachen Cybersicherheit. Aus unserer Sicht liegt hier sehr viel Potenzial zur Verbesserung der Sicherheit brach. Wir haben beispielsweise in unseren interaktiven Security Awareness Trainings festgestellt, dass sich die Klickraten, also das Anklicken von Links auf mit Malware infizierte Webseiten oder das Öffnen von Dateien mit Schadsoftware um bis zu 90 Prozent reduzieren lassen.

? **Ulrich Parthier:** *Auf welche Bedrohungen sollten die Unternehmen die Mitarbeiten denn gegenwärtig besonders vorbereiten?*

Irene Marx: Phishing ist aus unserer Sicht gegenwärtig eine der größten Bedrohungen. Das sieht jeder zweite der Befragten unserer Studie übrigens genauso. Dabei kann natürlich durch die Übernahme eines Accounts, wie eines Office-365-Kontos, durch erfolgreiches Phishing sehr großer Schaden entstehen, denn versendet ein Krimineller dann im Namen des eigentlichen Kontoinhabers Mails, zum Beispiel um eine Überweisung zu veranlassen oder geschäftskritische Daten zu erhalten, kann der Empfänger zumindest anhand des Absenders die Legitimität nicht überprüfen.

Aber auch ein weiteres Thema bereitet den CISO und CSOs zunehmend Sorgen: Insider Threats. Jeder dritte – immerhin 35 Prozent – der Sicherheitsverantwortlichen sieht hier mittlerweile eine große Gefahr für sein Unternehmen. Dieses Risiko rangiert damit auf Platz zwei der Bedrohungen, noch vor Ransomware mit 32 Prozent.

? **Ulrich Parthier:** *Dazu noch eine Frage zum Einfluss der Pandemie auf die IT-Sicherheit: Hat sich die Bedrohungslage dadurch verbessert oder verschlechtert?*

Irene Marx: Ich wäre davon ausgegangen, dass die Kriminellen die Unsicherheit überall ausnützen würden. Aber man muss hier deutlich unterscheiden: Mit 34 Prozent sieht ein Drittel der von uns befragten Experten durchaus eine Zunahme, aber gleichzeitig können 29 Prozent diese Erfahrung nicht bestätigen.

Zudem bestehen große Unterschiede zwischen den verschiedenen Branchen: So waren es im öffentlichen Sektor gerade einmal 15 Prozent der CSOs und CISO, die eine Zunahme der Attacken beobachtet haben, wohingegen es in der Fertigungsindustrie und dem Einzelhandel mit 45 Prozent drei Mal so viele waren. Spitzenreiter im negativen Sinne war die Logistik-Branche. Mehr als 56 Prozent der Unternehmen hatten einen Zuwachs an Phishing-Attacken zu verzeichnen.

? **Ulrich Parthier:** *Frau Marx, noch eine Frage zum Schluss: In den meisten Fällen haben wir im Bereich der digitalen Sicherheit mit Männern zu tun, Frauen sind da eher die Ausnahme. Allerdings leiten Sie das Geschäft von Proofpoint in Österreich und der Schweiz. Gibt es eigentlich viele Frauen, die im Bereich der Cybersecurity tätig sind?*

Irene Marx: Nein, sehr viele Expertinnen sind es gegenwärtig noch nicht. Allerdings sehen wir durchaus eine stetige Zunahme in diesem Markt. Bei Proofpoint selbst habe ich mit Adenike Cosgrove und Sherrod DeGrippo zwei Kolleginnen, die auf ihren Gebieten mittlerweile einen ausgezeichneten Ruf als Expertinnen in Sachen digitaler Sicherheit genießen. Ich denke, unsere Vorbildfunktion und Kompetenz in Sachen Technologie und Unternehmensleitung sollten weitere Frauen motivieren sich für Cybersecurity zu interessieren und zu engagieren.

! **Ulrich Parthier:** *Wir danken für dieses Gespräch!*

Die CISO-Studie können Sie unter folgendem Link kostenlos herunterladen: ***https://bit.ly/3lqS2ym***

FRÜHZEITIGE RISIKOERKENNUNG

CYBERSICHERHEIT IM INTELLIGENTEN GEBÄUDE

Benutzerfreundlichkeit und Energieeffizienz sind die Versprechen vernetzter intelligenter Gebäude. Unter den immer zahlreicher werdenden Komponenten für die Gebäudeautomation erfolgt kontinuierlich ein Datenaustausch jeglicher Art – manchmal zulasten jeglicher Sicherheit. Ob für Datennetzwerke (IT) oder operationelle Netze (OT), die Gewährleistung der Cybersicherheit eines intelligenten Gebäudes stellt eine große Herausforderung dar. Doch keine unüberwindbare.

In den ersten intelligenten Gebäuden (Dienstleistungsgebäude zur gewerblichen Nutzung oder Mehrfamilienhäuser) erfolgte der Datenaustausch für lange Zeit unter wenigen Gerätearten, die maßgeblich für das zentralisierte technische Management (ZTM), beispielsweise Beleuchtung, Heizung oder Klimatisierung, eingesetzt wurden. Das modernere technische Gebäudemanagement (TGM) wiederum erstellt eine vielfältigere Verbindung zwischen Systemen und Netzwerken und fügt dem ZTM eine Automatisierungs- und Überwachungsebene hinzu. Gebäudeautomationssysteme werden derzeit immer globaler und intelligenter: Beleuchtung, HLK (Heizung, Lüftung, Klimatisierung), Brandschutz (Rauchmelder), Aufzüge, Parksensoren, Überwachungskameras, automatische Türen und Zutrittskontrollen sind einige Bereiche davon. Die dadurch erhobenen Daten dienen der Überwachung des Anlagenzustands, der Erstellung von Funktionsstatistiken sowie der Einleitung von Maßnahmen zur Präventivwartung und prädiktiven Instandhaltung.

Diese zusätzliche Automatisierungs- und Überwachungsebene ist allerdings mit nicht zu unterschätzenden Cyberrisiken verbunden. Das exponentiell zunehmende Datenvolumen aus einer steigenden Anzahl von Systemen verschiedenster Anbieter macht die Gewährleistung der Datenintegrität für das reibungslose Funktionieren intelligenter Gebäude zu einer schwierigen Aufgabe: Die zugrunde liegenden Protokolle und Betriebssysteme sind genauso unterschiedlich wie der Reifegrad der Anbieter in Bezug auf IT- und OT-Cybersicherheitsrisiken. Ein Paradebeispiel dafür war bereits 2014 der Fall von der US-amerikanischen Einzelhandelskette Target: Hacker konnten die Daten von Millionen Bankkarten der Target-Kunden stehlen, indem sie sich Zugang über das Netz eines Subunternehmens verschafften, der für die Klimaanlagen verantwortlich war.

Kenne deinen Feind

Das intelligente Gebäude kann durch mehrere Arten von Cyberangriffen geschädigt werden: vom Hacken der Netze und Server der Gebäudeverwaltung oder der jeweiligen Subunternehmer über Datenmanipulation bis hin zur ganzheitlichen Blockierung eines vernetzten Gebäudes durch eine Ransomware. Diverse Studien aus dem Jahr 2019 belegen,

dass fast jeder vierte für die Kontrolle der Automatisierungssysteme eingesetzte Rechner Cyberangriffen zum Opfer fiel.

> DAS EXPONENTIELL ZUNEHMENDE DATENVOLUMEN AUS EINER STEIGENDEN ANZAHL VON SYSTEMEN VERSCHIEDENSTER ANBIETER MACHT DIE GEWÄHRLEISTUNG DER DATENINTEGRITÄT FÜR DAS REIBUNGSLOSE FUNKTIONIEREN INTELLIGENTER GEBÄUDE ZU EINER SCHWIERIGEN AUFGABE.
>
> Uwe Gries, Countr-Manager DACH, Stormshield, www.stormshield.com

Hinzu kommen IoT-Komponenten, die nach wie vor Fragen bezüglich der Sicherheit aufwerfen und hauptsächlich über kabellose Netze (wie WLAN oder Bluetooth) kommunizieren: Sie fördern Angriffe aus der Nähe. So konnten zum Beispiel zwei Forscher die Fernsteuerung von intelligenten Glühbirnen übernehmen und über ein falsches Update eine Malware in das gesamte Netz eines smarten Gebäudes einschleusen. Angriffe vom Gebäudeinneren sind ebenfalls möglich, dazu reicht ein USB-Stick.

Die Folge davon sind Zwischenfälle beim Funktionieren des intelligenten Gebäudes und sogar physische Schäden, wenn man beispielsweise an einen Angriff auf Aufzüge, Feueralarme, Torverriegelungen oder auch Lüftungssysteme denkt. Szenarien, die jeden erschaudern lassen, vor allem in Bezug auf Einkaufszentren und Krankenhäuser oder Bank- und Regierungsgebäude.

Die Bedeutung der frühzeitigen Risikoerkennung

Die Cyberrisiken im ZGM- und TGM-Bereich sind vielen bekannt, doch die fehlende frühzeitige Risikoerkennung ist offensichtlich: „Man bereitet sich auf die Zukunft vor, indem man auf bereits erfolgte Cyberangriffe Bezug nimmt. Doch das Cyberrisiko muss bereits ab der Entwurfs- und Umsetzungsphase eines intelligenten Gebäudes erfasst werden", erklärt Uwe Gries, Country-Manager DACH bei Stormshield.

Die mittlerweile oft genutzten digitalen 3D-Zwillingsmodelle („BIM" – „Building Information Modeling") sind ebenfalls für mögliche Datenmanipulation und -missbrauch anfällig. Im Rahmen einer Gebäuderenovierung ist es üblich, mehrere Anbieter um die Anfertigung von 3D-Modellen zu bitten. Kritische Daten zur Erstellung solcher Modelle werden oft von den Auftragnehmern unverschlüsselt mit Subunternehmen geteilt. Könnten sich Cyberkriminelle Zugriff darauf verschaffen, würden sie genau erfahren, wie die Heizung auf Höchststufe gedreht, die Sauerstoffzufuhr unterbrochen oder ein Feueralarmsystem deaktiviert werden kann.

Aufgrund der hohen Anzahl an Beteiligten an solchen Projekten sind Sicherheitslücken vorprogrammiert. Ein BIM-Manager, der das Kritikalitätsniveau der Daten und daraufhin die erforderlichen Zugangsberechtigungen und Verschlüsselungsmaßnahmen festlegt, ist in dieser Phase entscheidend, damit das produzierte Modell nicht als Generalschlüssel für Hacker dient.

Das intelligente Gebäude in gänzlicher (Cyber-)Sicherheit

Zur Sicherung der eingesetzten digitalen Technik und für einen maximalen Schutz der vom intelligenten Gebäude produzierten Daten wird empfohlen, starke Authentifizierungsverfahren aller Beteiligten einzuführen. Die Absicherung des Informationssystems durch eine Netzwerksegmentierung und die Installation einer in Echtzeit agierenden Firewall sind ebenfalls zu empfehlen. Und zu guter Letzt ist es ebenso wichtig, die erstellten Daten mit einer robusten Ende-zu-Ende-Verschlüsselung zu versehen.

„Wir sagen immer, dass die Technik nur 30 Prozent der Sicherheit ausmacht, die restlichen 70 Prozent sind hauptsächlich eine Organisationsfrage", beteuert Gries. Die getroffenen Schutzmaßnahmen sollten von allen getragen werden. „Wir haben alle das Bild des Feuerlöschers im Kopf, der zwischen Tür und Türrahmen gestellt wird, um Korridore und dahinter liegende Räume zu lüften oder gar um dem Personal „schneller" Ein- und Ausgang zu gewähren." Das hört sich zwar wie eine einfache Anekdote an, ist aber ein schwerwiegender Fehler. Missgeschicke wie dieses unterminieren die Verlässlichkeit der eingerichteten technischen Maßnahmen und gefährden die allgemeine Sicherheit des Gebäudes oder der Daten. Aus diesem Grund sollten die Sensibilisierung und die Ausbildung des Personals, vor allen in Bezug auf Cybersicherheit, oberste Priorität haben.

Das sind Maßnahmen, die gleichermaßen für die „Smart Industry" und in größerem Maßstab auch für die „Smart City" gelten. Letztere weist ähnliche Probleme wie das intelligente Gebäude auf, nur auf höherer Ebene. Die Anzahl der involvierten Anbieter nimmt immer weiter zu, was Fragen in Bezug auf Vorschrifteneinhaltung, Vertraulichkeit oder Datensicherheit mit sich bringt – umso mehr, da die Entwicklung neuer Sensortechnologien (LoRa, SigFox oder auch 5G) die Entwicklung der Stadt von morgen vorantreibt. Es handelt sich um einen Übergang in Richtung digitaler Stadt, der nicht ohne einen bestimmten Grad an Cybersicherheit stattfinden dürfte.

Uwe Gries

STANDARDS SCHAFFEN SICHERHEIT

… AUCH IM INTERNET DER DINGE

Ob in der industriellen Produktion, im Consumerbereich oder im Gesundheitswesen: Die Zahl der über das Internet of Things (IoT) vernetzten Geräte wächst dynamisch. Prognosen zufolge könnte es bis 2025 weltweit über 75 Milliarden IoT-Geräte geben. Höchste Zeit also, dass diese Geräte einheitliche Sicherheitsstandards erfüllen. Dafür plädiert Stefan Vollmer, CTO der TÜV SÜD Sec-IT.

Krankenhäuser stehen derzeit mehr denn je im Blick der Öffentlichkeit: Einerseits wegen der Corona-Krise, andererseits wegen vermehrter virtueller Angriffe gegen diese Einrichtungen, darunter Lösgeldforderungen mittels Ransomware. Ein mögliches und beliebtes Einfallstor in die Netzwerke der Krankenhäuser stellen deren IoT-Geräte dar, oft das schwache Glied in der Kette: Diese sind mit dem Internet verbunden und verfügen meist über unterschiedliche und verschieden starke Absicherungen. Hinzu kommt das sogenannte Schatten-IoT: unbekannte, oft unbemerkte IoT-Geräte im Netzwerk, die daher weder überprüft noch aktualisiert werden.

IOT-GERÄTE MÜSSEN BEREITS BEI DER PRODUKTION DURCH DEN HERSTELLER NACH KLAR FORMULIERTEN RICHTLINIEN ABGESICHERT WERDEN.

Stefan Vollmer, CTO, TÜV SÜD Sec-IT, www.tuev-sued.de

Trotz des Risikos sind IoT-Geräte unumstößlicher Bestandteil des Gesundheitssystems: Informationen über Patienten können von verschiedenen Geräten kumuliert, automatisch ausgewertet und an die Ärzte verteilt werden; intelligentere Geräte können sogar Abläufe, wie die Dokumentation, übernehmen.

Einheitliche IoT-Zertifizierung überfällig

Die größte Wirkung zur Steigerung der Sicherheit von IoT-Geräten hätte die längst überfällige Einführung von Standards und entsprechender Zertifizierung durch unabhängige Experten. Geräte würden dann während ihrer Konzeption und Produktion bereits einheitliche Sicherheitsanforderungen erfüllen müssen, deren Einhaltung sich im Anschluss objektiv überprüfen ließe. Es genügt, wenigstens die Hälfte der aktiven IoT-Geräte auf diese Weise zu verbessern, um die anderen indirekt positiv zu beeinflussen, weil die Angriffsoberfläche im Verbund schrumpfen würde. Als Richtschnur für solche Standards sollte die Relevanz des jeweiligen Gerätes dienen. Zudem erlangen die Hersteller der IoT-Geräte durch die Standards und ihre Überprüfung eine gesetzliche Absicherung im Schadensfall.

Europäische Union macht ersten Schritt

Den Weg zu einem Standard innerhalb der europäischen Gemeinschaft (EU) bereitet der EU-Cybersecurity Act, der im Juni 2019 in Kraft trat. Dieses Rahmenwerk soll die Zertifizierung von Produkten, Dienstleistungen und Prozessen der Informationstechnologie einheitlich regeln und Standards etablieren. Zudem wurde die Gründung der europäischen Stakeholder Cybersecurity Certification Group (SCCG) beschlossen. Dieses Gremium soll sich derweil darum kümmern, die Rahmenbedingungen für jene Zertifizierungen im EU-Raum zu definieren. Solche supranationalen Bemühungen zeigen, wie wichtig einheitliche Sicherheitsstandards eingestuft werden – endlich.

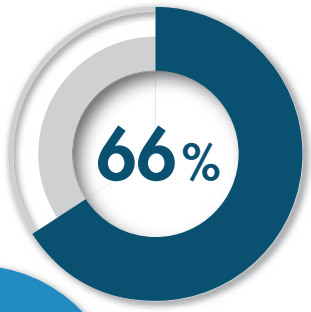
Gemeinsam mehr IT-Sicherheit schaffen

IoT-Geräte sind in der Lage, beispielsweise das medizinische Personal entscheidend zu unterstützen, doch müssen die Geräte bereits bei der Produktion durch den Hersteller nach klar formulierten Richtlinien abgesichert werden. Im Anschluss muss deren regelmäßige Überprüfung durch unabhängige Experten verpflichtend sein. Andernfalls lässt sich eine hohe Absicherung nicht zuverlässig gewährleisten. Diese Routine aber lässt sich nur durch einheitliche Standards und Zertifikate erreichen, die innerhalb einer Nation, oder sogar einer Staatengemeinschaft, definiert wurden und anerkannt werden.

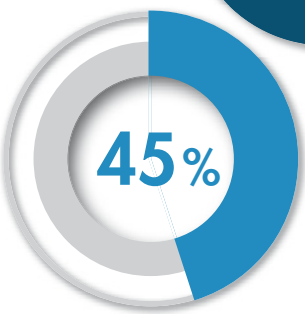
Stefan Vollmer

CYBERRISIKEN MINIMIEREN

MANGELNDE ABSTIMMUNG ZWISCHEN GESCHÄFTS- UND SICHERHEITSVERANTWORTLICHEN SCHADET DEN UNTERNEHMEN



der deutschen Sicherheitsverantwortlichen arbeiten nicht mit geschäftlichen Interessenvertretern zusammen, um Kosten-, Leistungs- und Risikominderungsziele abzustimmen



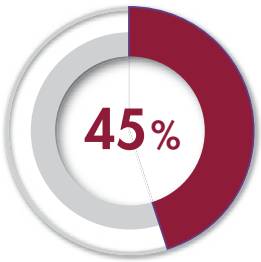
der geschäftlichen Führungskräfte konsultieren bei der Ausarbeitung von Geschäftsstrategien nur selten die Sicherheitsverantwortlichen.

Eine der größten Herausforderungen für Sicherheitsteams ist der Mangel an Transparenz:

können das Risiko, das von Remote-Mitarbeitern ausgeht, nicht vollständig überblicken

haben unzureichenden Einblick in OT und Mobilgeräte

der Unternehmen verzeichneten fünf oder mehr Geschäftsschädigende Cyberangriffe



der Angriffe beeinträchtigten die Handlungsfähigkeit

www.de.tenable.com

HELFER IN DER CYBER-NOT

SECURITY OPERATIONS CENTER AS A SERVICE

Cyber-Angriffe werden immer häufiger, komplexer und langfristiger. Mit klassischen, isolierten Gegenmaßnahmen auf reaktiver Basis ist diesen Gefahren nicht mehr beizukommen. Schnell entstehen kritische Risiken für das eigene Geschäft, materielle Verluste oder Reputationsschäden.

Nicht von allen Betroffenen wird diese Gefahr als solche erkannt und ernst genommen. Bei Security Awareness bietet sich allzu oft eine Analogie zum Straßenverkehr an: Mir wird schon nichts passieren, ich bin doch ein guter Fahrer – sagt beinah jeder von sich. Die Unfallstatistiken sprechen eine andere Sprache. Und so spricht auch beispielsweise der BITKOM in aktuellen Studien davon, dass 75 Prozent der befragten mittelständischen Unternehmer bereits von erfolgreichen Cyber-Attacken gegen die eigene Organisation wissen und weitere 13 Prozent vermuten, dass es entsprechende Angriffe bereits unbemerkt gab.

Der Angriffstrend: Advanced Persistent Threats

Auch hier liegt eine Krux der aktuellen Bedrohungslage: Gefährdungen verlagern sich immer weiter weg von akuten Angriffen mit roher Gewalt hin zu langfristig angelegten so genannten Advanced Persistent Threats (ATP).

Spätestens hier sind die herkömmlichen Schutz-Layer und Firewalls weitgehend machtlos, wenn etwa über Phishing ein Zugang ins Unternehmensnetzwerk erfolgt ist und nun schrittweise von Innen über laterale Bewegungen erweiterte Rechte und Privilegien erschlichen und damit weitere Schutzmechanismen ausgehebelt werden. Über Tage, Wochen oder sogar Monate vorbereitet und mit Geduld und Vorsicht durchgeführt, bleiben diese Manöver oft lange unbemerkt.

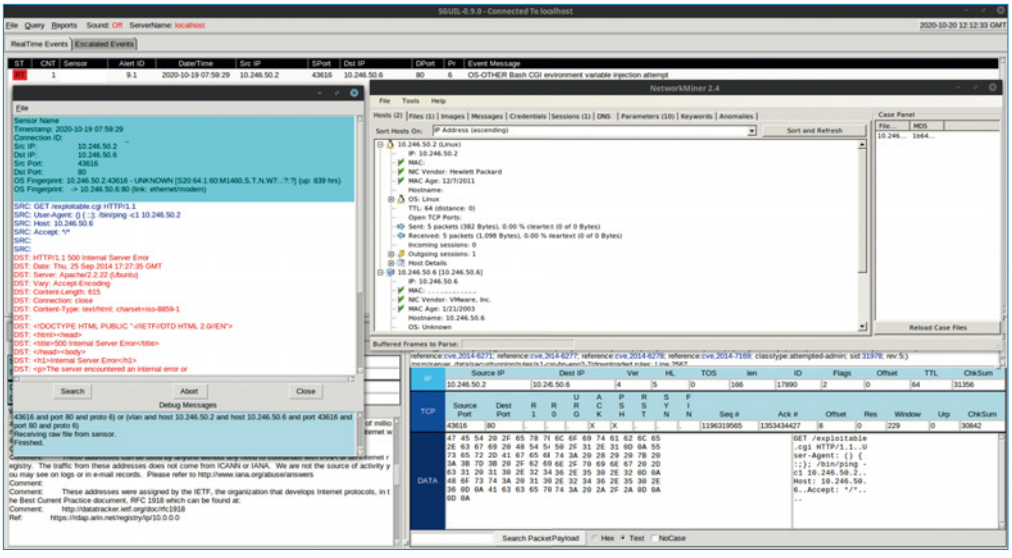
Gebündelte Gegenmaßnahmen

Um Gefährdungen und tatsächliche Angriffe zuverlässig zu erkennen und geeignete Gegenmaßnahmen einleiten und steuern zu können, benötigen Unternehmen und Organisationen aller Art und Größe daher heutzutage eine zentrale Stelle, an der Beobachtung, Detektion, Analyse, Reaktion und Steuerung gebündelt werden.

Der zunehmend verbreitete Ansatz um eine solche „Sicherheitszentrale" zu etablieren ist ein Security Operations Center (SOC). In dessen Zentrum arbeitet ein Security Information and Event Management, kurz SIEM, daran, über die Aggregation und Korrelation von Ereignissen Auffälligkeiten automatisiert zu entdecken und auszuwerten.

Logfiles versus Netflow

Die meisten SIEM setzen dabei auf eine Logfile-Analyse mit hohem Automatisierungsgrad, um sehr große Datenmengen verarbeiten und auffällige Vorgänge als Events ermitteln zu können. Hierbei kommen bestimmte Regeln zum Einsatz, die Sicherheitsspezialisten zuvor definiert und im System eingepflegt haben. Dieses Vorgehen sammelt Ereignisse mit Metadaten und versucht diese anhand von bekannten Mustern und Use Cases automatisiert in eine Korrelation zu setzen und damit zu bewerten. Aufgrund der beste-



Analyse eines Events mittels der Netflow-Analyse

henden Grenzen der Automatisierung nach dem aktuellen Stand der Technik, enthalten die so identifizierten Incidents für sich aber noch wenig Aussagekraft und oftmals auch einen sehr hohen Anteil an False Positives.

Die Netflow-Analyse setzt hingegen die Packages in Datenströmen mit den Metadaten aus den Inhalten in Beziehung und ermöglicht es erfahrenen Sicherheitsfachleuten so, auf einen Blick typische Angriffsmuster zu erkennen und tatsächlich kritische Vorfälle zu identifizieren. Dazu bietet die Netflow-Analyse noch weitere Vorteile: Die außerhalb der Datenflüsse implementierten Sensoren sind anders als Logfiles nicht manipulierbar, zudem sind die Ergebnisse der Netflow-Analyse endgeräteunabhängig, verifizierbar, mitigierbar und referenzierbar.

IN EINEM SOC AS A SERVICE AUF DIENSTLEISTUNGSBASIS ERHALTEN UNTERNEHMEN PROFESSIONELLE SICHERHEIT ZU ÜBERSCHAUBAREN UND VOR ALLEM TRANSPARENT KALKULIERBAREN KOSTEN.

Manfred Müller,
Business Development Manager Cyber Security, CONET Solutions GmbH,
www.conet.de

Der Faktor Mensch

Beide Herangehensweisen haben also spezielle Stärken und bevorzugte Einsatzbereiche, können aber auch in Kombination eingesetzt werden. Beiden gemeinsam ist allerdings eine Tatsache, die bei Überlegungen zur Nutzung eines Logfile-basierten SIEM oftmals aus dem Blickfeld gerät: dass es sich hierbei nicht um ein vollautomatisches Sicherungssystem handelt.

Sowohl im Vorfeld bei der Definition der Use Cases als auch im Nachgang bei der Bewertung von Events sind erfahrene Sicherheitsspezialisten im Security Operations Center nötig. Zwar sind entsprechende Systeme mehr und mehr in der Lage, auf Basis von Konfigurationen und Erfahrungswerten nach dem Prinzip künstlicher Intelligenz zu lernen, aber von einer wirklichen Zuverlässigkeit sind diese Automatismen noch weit entfernt. Sie würden in Ihrer Logistik Ihre wertvollen Frachtgüter heut wohl noch lange nicht einem autonom fahrenden LKW anvertrauen – Ihre Sicherheit aber schon? Es geht also auch weiterhin nicht ohne menschliches Fachpersonal, um ein SOC wirkungsvoll aufzubauen und mit den angeschafften Systemen zielgerichtet umzugehen.

Managed Security & SOCaaS

Für jedes Unternehmen, gerade aber den Mittelstand, entsteht hier ein schwer zu entschärfendes Spannungsfeld. Ist überhaupt erst einmal die Awareness für Sicherheitsbedrohungen und eine mangelhafte Sicherheitslage geweckt, stellt sich die Frage, wie mit den Gefahren umzugehen ist: Oftmals sind Security-Prozesse nicht ausreichend verankert. Komplexe SIEM-Systeme sind in Art und Arbeitsweise auf Konzerngrößen ausgerichtet und sind damit für den Mittelstand weder sinnvoll, erschwinglich noch gewollt. Zudem fehlen ohnehin die Fachleute für Systemkonfiguration, Auswertung und Reaktion auf entsprechende Vorfälle, denn ausreichend erfahren und bezahlbar stehen diese bei Weitem nicht für alle Interessenten zur Verfügung. Überspitzt gesagt, fehlt für komplexe und damit teure Lösungen das Geld, für clevere und damit günstigere Lösungen aber das Know-how.

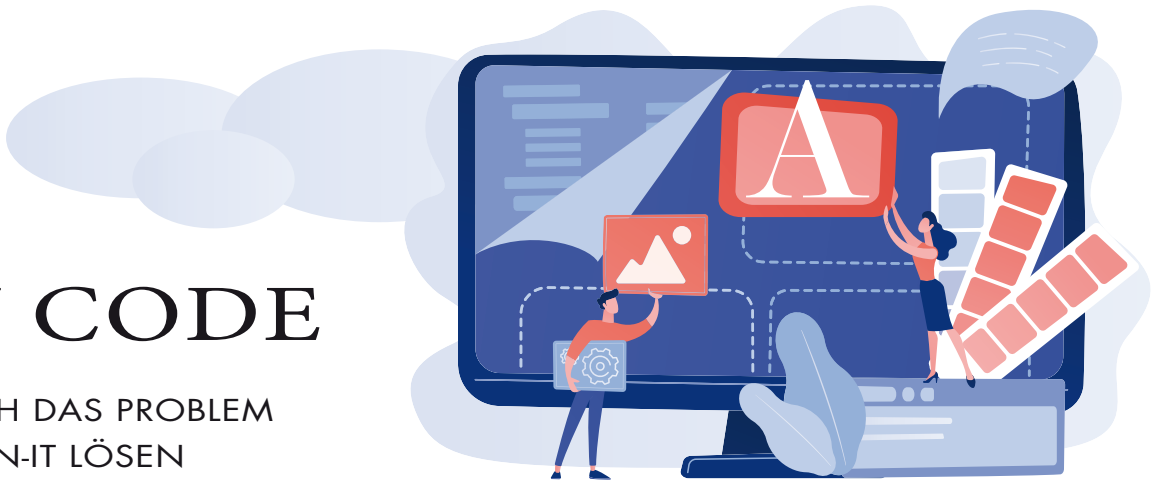
Den Ausweg aus diesem Dilemma bieten Modelle wie Managed Security oder Security as a Service. Anstatt selbst Unmengen an Ressourcen auszugeben und zu binden, werden sicherheitsrelevante Dienstleistungen bedarfsgerecht von einem darauf spezialisierten und mit den nötigen technischen und personellen Mitteln ausgestatteten Anbieter bezogen. In einem SOC as a Service auf Dienstleistungsbasis erhalten Unternehmen professionelle Sicherheit zu überschaubaren und vor allem transparent kalkulierbaren Kosten.

So ist das CONET SOC beispielsweise von Beginn an auf die Bedürfnisse und Möglichkeiten des Mittelstands entwickelt und ausgerichtet worden. Ist die für die Netflow-Analyse notwendige Sensor-Phalanx einmal eingerichtet und über ein Site2Site-VPN an das SOC angeschlossen, arbeitet das Security Operations Center weitgehend ohne Eingriffe auf die Kunden-IT. Sämtliche Daten und Prozesse bleiben beim Kunden und damit EU-DSGVO- und Compliance-konform gesichert.

Im komplett an deutschen Standorten beheimateten SOC werden die Datenströme je nach erforderlichem Schutzniveau und vereinbarter Service-Pauschale entweder rund um die Uhr oder nach festgelegten Zeitfenstern von Security-Spezialisten manuell gesichtet, analysiert und bewertet. Bei der Identifikation und Behebung von sicherheitsrelevanten Vorfällen unterstützen die Experten des SOC den betroffenen Kunden bei Bedarf. Ein umfassendes Reporting rundet das Service-Spektrum ab und sorgt dafür, dass auch eine Compliance-konforme und jederzeit nachvollziehbare Dokumentation gewährleistet ist.

Damit kann sich der Auftraggeber beruhigt auf seine Kernaufgaben und Wertschöpfungsprozesse konzentrieren, während er seine Sicherheit in kompetenten Händen weiß.

Manfred Müller



LOW CODE

SO LÄSST SICH DAS PROBLEM DER SCHATTEN-IT LÖSEN

Die Entwicklung qualitativ hochwertiger Applikationen ist zeit- und ressourcenaufwändig – besonders durch sich häufig ändernde Leistungsanforderungen. Betroffene Fachbereiche wollen oft jedoch nicht lange auf die von der IT-Abteilung entwickelten Lösungen warten. Deshalb greifen sie meist auf nicht autorisierte Anwendungen und Tools zurück und entwickeln eigenständig Lösungen mit Excel, Access, Lotus Notes und ähnlicher Software – und das nicht immer zur Freude der IT-Abteilung.

Im Schatten der IT-Abteilung

Beschafft, entwickelt oder betreibt ein Mitarbeiter oder eine ganze Fachabteilung Software autonom, spricht man von Schatten-IT. Diese inoffiziellen Zweitsysteme existieren parallel zu der eigentlichen IT-Architektur – ohne Kenntnis und Kontrolle der IT-Abteilung. Oft genügen die Insellösungen nicht den organisatorischen Anforderungen von Unternehmen hinsichtlich Kontrolle, Dokumentation, Sicherheit und Zuverlässigkeit. Bereits 2018 warnten die Analysten von Gartner davor, dass durch den Einsatz nicht autorisierter IT-Lösungen das Risiko von Cyber-Attacken deutlich ansteigt. Da sie den sicherheitstechnischen Vorschriften oft nicht entsprechen, sind sie besonders anfällig für Sicherheitslücken.

DER EINSATZ VON LOW-CODE-PLATTFORMEN HILFT DABEI, UNKONTROLLIERBARE SCHATTEN-IT IN NUTZERZENTRIERTES CITIZEN DEVELOPMENT UMZUWANDELN.

Christian Kleinschroth,
CTO und Gründer von Simplifier,
www.simplifier.io

Gemeinsame Potenziale in der Anwendungsentwicklung

Nichtsdestotrotz können solche Insellösungen Innovationen antreiben und als Prototypen für zukünftige Anwendungen dienen. Um diese positiven Effekte zu nutzen, kommt es darauf an, die Eigeninitiative der Fachabteilungen in die übergeordnete IT-Strategie zu integrieren. Es gilt, einen Mittelweg zwischen Kontrolle, unternehmerischer Flexibilität und IT-Security zu finden. Dazu ist eine bessere Zusammenarbeit zwischen IT- und Fachabteilung notwendig. Die IT-Abteilung muss lernen, den Fachbereichen mehr Verantwortung zu überlassen.

Unterstützt wird die IT-Abteilung durch sogenannte Citizen Developer, die aufgrund ihrer technischen Affinität und Expertise in ihrem Fachbereich eigenständig Applikationen entwickeln. Da sie jedoch meist nicht über tiefergehende IT- und Programmierkenntnisse verfügen, sind sie dabei auf unterstützende Tools angewiesen. IT-Abteilungen müssen den Fachbereichen deshalb praktikable, einfach zu bedienende Werkzeuge zur Verfügung stellen. Da diese Anwendungen auf einer einheitlichen technologischen Basis erstellt werden, sind sie zudem von Anfang an Teil der offiziellen IT-Infrastruktur des Unternehmens.

Einfache Anwendungsentwicklung mit Low Code

Low-Code-Plattformen wie Simplifier setzen hier an und schaffen eine kontrollierbare standardisierte Entwicklungsumgebung. Gleichzeitig binden sie technologisch fragmentierte Lösungen an Standards an. Unkompliziert und ohne tiefergehende IT- und Programmier-Kenntnisse können Citizen Developer so Software-basierte Geschäftsapplikationen mit nur wenigen Klicks erstellen. Die Fachanwender profitieren dabei besonders von der einfachen Integration von Datenbanken. Außerdem lassen sich App-Designs dank benutzerfreundlicher Vorlagen und einfach zu bedienender Tools unkompliziert nach dem Baukastenprinzip erstellen.

Citizen Development

Der Einsatz von Low-Code-Plattformen hilft dabei, unkontrollierbare Schatten-IT in nutzerzentriertes Citizen Development umzuwandeln. Dabei übergibt die IT-Abteilung den Fachbereichen mehr Verantwortung. Trotzdem werden die eigens entwickelten Lösungen kontinuierlich zentral von der IT-Abteilung überwacht. So funktionieren die dokumentierten Applikationen zuverlässig und erfüllen alle sicherheitstechnischen Anforderungen.

Christian Kleinschroth

UNTERSTÜTZUNG FÜR IT-ADMINS

KONTINUIERLICHE ÜBERWACHUNG DER BERECHTIGUNGSVERGABEN IN MICROSOFT-UMGEBUNGEN

Die IT-Infrastruktur in Unternehmen beeinflusst Geschäftsprozesse heutzutage maßgeblich und sollte daher reibungslos funktionieren. An dieser Stelle kommen Administratoren ins Spiel, die für die Konfiguration, den Betrieb sowie die Kontrolle der IT-Infrastruktur verantwortlich sind. Tagtäglich haben sie zahlreiche Aufgaben zu bewältigen und tragen eine große Verantwortung – gerade was das Thema IT-Sicherheit betrifft. In Zeiten, in denen immer mehr Unternehmen Cyberattacken zum Opfer fallen, müssen sie stets darauf achten, Sicherheitslücken zu vermeiden. Dazu gehören auch veraltete Mitarbeiterkonten, über die Kriminelle auf IT-Systeme zugreifen können. Eine manuelle Analyse einzelner Berechtigungen oder gar vollständiger Berechtigungskonzepte ist aufgrund des hohen Arbeitsaufkommens jedoch kaum zu bewältigen und außerdem zu fehleranfällig. Daher bedarf es einer geeigneten Softwarelösung, die die Auswertung von Zugriffsberechtigungen automatisiert und die Ergebnisse leicht zugänglich anzeigt.

Viele Administratoren arbeiten in Microsoft-Umgebungen und sind unter anderem dafür zuständig, die Richtlinien und Berechtigungskonstellationen im Active Directory (AD) und im NTFS-Filesystem zu überwachen. Da vor allem bei großen Umgebungen schnell der Überblick verloren geht, welcher Mitarbeiter worauf zugreifen darf, benötigen sie eine entsprechende Softwareunterstützung. Denn nur so lässt sich lückenlos nachvollziehen, welche Berechtigungen an wen vergeben wurden. Hierfür eignet sich die Nutzung einer professionellen Access Governance-Lösung. Um IT-Admins wirklich zu entlasten, ist es wichtig, dass eine solche Lösung einige wesentliche Features beinhaltet.

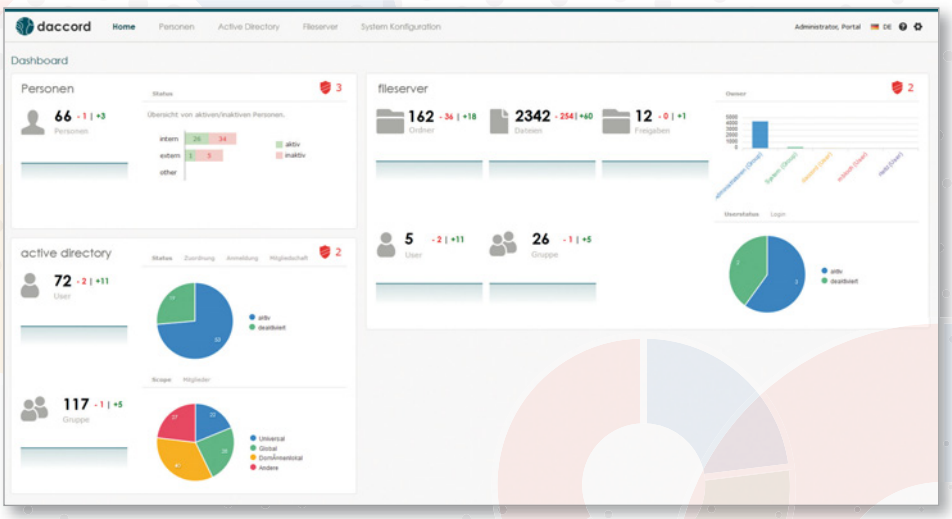
Die passende Lösung?

Zur Erleichterung des Arbeitsalltages von Administratoren muss sich die Software einfach installieren sowie konfigurieren lassen. Um zu jedem Zeitpunkt den Überblick zu behalten und keine Schwachstelle zu übersehen, brauchen Administratoren zwangsläufig eine Software, die Berechtigungen beständig überprüft. Dies gelingt nur dann, wenn der Datenbestand dauerhaft gecheckt wird. Darüber hinaus ist es essentiell, dass die Lösung dazu fähig ist, Konten, die keinem Mitarbeiter zugeordnet werden können (sogenannte verwaiste Konten), aufzudecken. Hierfür sollte die Möglichkeit bestehen, Personalstammdaten problemlos einzulesen. Eine Historienfunktion versetzt Administratoren zudem in die Lage, sich den Kontenursprung und die Berechtigungsveränderungen im Zeitablauf anzeigen zu lassen. Dies ist wichtig für die Dokumentation und äußerst hilfreich für IT-Prüfungen.

Zusätzlich sollte es eine softwarebasierte Lösung erlauben, die Berechtigungen automatisiert auf Konformität zu rechtlichen Anforderungen oder zu den Microsoft-Best-Practice Richtlinien zu überprüfen, indem vorgefertigte Richtlinienpakte zusammen mit der Software ausgeliefert werden. Wünschenswert wäre es, auch unternehmenseigene Richtlinien zu integrieren, in die kontinuierliche Auswertung einzubeziehen und bei Verstößen Handlungsempfehlungen auszusprechen. Das i-Tüpfelchen ist ein umfangreiches Dashboard, über das die IT-Admins eine anschauliche Übersicht über alle Systeme und Daten erhalten. Auf diese Weise fallen Ungereimtheiten im Daten- oder Personenbereich im Vergleich zu den Richtlinien direkt auf.

Sebastian Spethmann

www.daccord.de/microsoft



(Quelle: Pixabay)

DER WEG ZUR AGILEN ORGANISATION

EINE ERFOLGREICHE DIGITALE TRANSFORMATION SETZT EINE NEUE FÜHRUNGSKULTUR VORAUS

Die Digitale Transformation stellt Unternehmen vor große Herausforderungen. Bislang bewährte Methoden greifen aufgrund der Komplexität, Geschwindigkeit und Ausmaße der Veränderungen zu kurz. Damit der Wandel gelingen kann, braucht es ein echtes Change-Management, das alle Strukturen, Prozesse und Mitarbeiter einbezieht. Und es braucht eine neue Führungskultur.

Neue Technologien, schnellere Marktzyklen und veränderte Kundenansprüche – Unternehmen stehen heute vor der Herausforderung einer sich permanent wandelnden Umwelt. Händeringend suchen sie nach einem Organisationsdesign, das dieser Transformation gerecht wird, und müssen gleichzeitig feststellen, dass bislang bewährte Managementmethoden nicht greifen. Vielmehr sind Agilität und Innovation die einzigen Mittel, mit dem Unternehmen wettbewerbsfähig bleiben können. Um neue Kunden und Märkte zu gewinnen, sollten Firmen immer ein bisschen besser und schneller sein als die Konkurrenz. Wie schnell man beides aber auch verlieren kann, zeigen zahlreiche Negativ-Beispiele. Gerade die Digitalisierung zwingt viele Unternehmen und Branchen in eine Art Überlebenskampf – sie verändert nicht nur einzelne Produkte und Dienstleistungen, sondern komplette Wertschöpfungsketten.

Etablierte Strukturen aufbrechen

Die Transformation zur agilen Organisation gelingt nicht ohne grundlegende Veränderungen – ein echtes Change-Management setzt tiefgreifend neue Denk- und Verhaltensmuster voraus. Die neuen Werte müssen von allen Mitarbeitern verinnerlicht, die Unternehmenskultur muss umgewandelt sowie Managementsysteme und Regeln angepasst werden. Auf dem Weg dahin lauern viele Stolpersteine, gerade wenn Unternehmen unrealistische Ziele und Zeitrahmen setzen oder Strukturen und Prozesse falsch einschätzen. Die größte Herausforderung liegt jedoch im Widerstand der Mitarbeiter. Den meisten Menschen fällt es schwer, gewohnte Denk- und Verhaltensmuster, die ihnen Sicherheit vermitteln, aufzugeben. Entsprechend langwierig gestalten sich Veränderungsprozesse, bei denen viele Mitarbeiter und Teams ihr Verhalten ändern sollen.

Die Einbeziehung beziehungsweise Partizipation der Mitarbeiter in den Veränderungsprozess gilt deshalb als Schlüsselfaktor für ein erfolgreiches Change-Ma-

Die Digitalisierung ist nicht aufzuhalten – Change-Management und eine neue Führungskultur sind deshalb für viele Unternehmen das Gebot der Stunde.

nagement. Die beste Strategie hierzu ist immer noch umfassende Information und Kommunikation. Worin liegen die Gründe für den Veränderungsprozess, warum müssen sich Unternehmen und damit auch dessen Mitarbeiter neu aufstellen?

Jede Stimme zählt

Die Führungskräfte eines Unternehmens sind bei der Motivation der Mitarbeiter für die Digitale Transformation in besonderer Weise gefordert. Sie sollten soweit wie möglich Verantwortung teilen und die Ausgestaltung von einzelnen Prozessschritten ihren Mitarbeitern und deren Know-how überlassen. Das setzt einen Abschied von lieb gewonnenen hierarchischen Führungsstrukturen voraus. Es ist einfach nicht mehr sinnvoll, dass alle Entscheidungsgewalt bei einer Person liegt und Aufgaben starr verteilt werden. Vielmehr braucht es ein Miteinander, ein agiles Arbeiten, bei dem das Team im Vordergrund ist. Diese Teams setzen sich aus zur Aufgabe passenden Expertisen und Eigenschaften zusammen – der jeweilige New Leader dirigiert nicht zwingend die Richtung, sondern ist größtmöglich operativ integriert. Jeder einzelne erhält so den Raum, eigene Ideen einzubringen. Fakt ist, Innovationen können nur mit einer gewissen Risikobereitschaft geschaffen werden.

Die Digitale Transformation läutet in Unternehmen immer einen Change-Prozess ein. Jahrelang etablierte Geschäftsprozesse werden abgeändert und neue Technologien eingesetzt, die es erst einmal zu erlernen gilt. Für diese Veränderung braucht es Zeit, Offenheit und definitiv einen neuen modernen Führungsstil – ein „Das haben wir schon immer so gemacht" kann es in diesem Umfeld nicht geben. Nur durch konsequentes Hinterfragen bestehender Business-Prozesse und eine integrierende Führungskultur können Unternehmen ihre Wertschöpfungsketten wahrhaft hinterfragen und getreu einer disruptiven Business Transformation zukunftsorientiert ausrichten. Technologie – oft als zentraler Aspekt der Digitalen Transformation angesehen – ist selbst nur ein Instrument in dieser komplexen Symphonie.

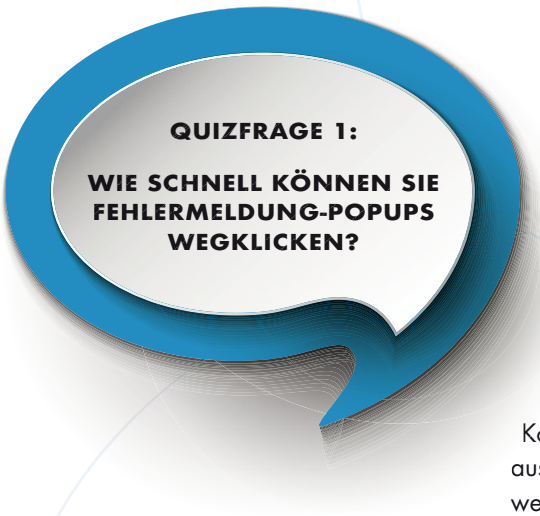
Kai Grunwitz

DIE TRANSFORMATION ZUR AGILEN ORGANISATION GELINGT NICHT OHNE GRUNDLEGENDE VERÄNDERUNGEN – EIN ECHTES CHANGE-MANAGEMENT SETZT TIEFGREIFEND NEUE DENK- UND VERHALTENSMUSTER VORAUS.

Kai Grunwitz, Geschäftsführer, NTT Ltd. Deutschland, https://hello.global.ntt/de-de/

ZERTIFIKATS-FEHLERMELDUNG

KANNSTE WEGKLICKEN



Wer kennt das nicht: Einfach mal eben eine Intranet-Seite aufrufen, mit einem Remote-Desktop verbinden, die Firewall-Oberfläche aufrufen oder eine E-Mail versenden?

Doch dann erscheint eine obskure Fehlermeldung. Bei genauerer Betrachtung stellt sich diese als Zertifikatsfehlermeldung dar. Wie bei den meisten Fehlermeldungen, wird das Ganze schnell weggeklickt. Doch es gibt auch Anwender, die lieber noch einmal bei einem Fachkundigen nachfragen. Die Antwort ist dann in den meisten Fällen: „Kannste wegklicken, Problem ist bekannt."

Das richtige Verhalten

Richtig wäre, den Fehler beim Support zu melden und erst dann weiterzumachen, wenn er behoben ist. Oft kann der manuelle Abgleich des Fingerabdrucks des Zertifikates ein zeitweiliger Workaround sein. Es muss aber richtig gemacht werden.

Wodurch entsteht aber ein Risiko, wenn das Zertifikat nicht passt? Es ist doch schließlich eine verschlüsselte Verbindung?

Und genau hier liegt der Irrtum. Eine sichere Kommunikation besteht aus zwei Komponenten: der Vertraulichkeit der Übermittlung und der Authentizität der Kommunikationsteilnehmer. Für die Authentizität ist das Zertifikat zuständig. Es ermöglicht den Kommunikationsteilnehmern, sich anderen gegenüber zu authentisieren. Schlägt die Zertifikatsprüfung fehl, dann konnte sich der entsprechende Kommunikationspartner nicht eindeutig ausweisen: andere wissen nicht, mit wem sie sich tatsächlich austauschen. Das ist, als würde jemand an der Haustür um Einlass bitten, dessen Stimme nicht zum genannten Namen passt.

Das Risiko besteht darin, dass der Anwender auf ein System umgeleitet worden sein könnte, welches nur vorgibt, der Server zu sein, mit dem sich der Anwender verbinden wollte. Wenn der Server anschließend nach vertraulichen Daten fragt, übermittelt man sie an Unbefugte.

Der Grund, warum IT-Systeme und Server mit Zertifikaten ausgestattet werden, ist eine Sicherheitsmaßnahme eines mehrschichtigen Sicherheitskonzeptes, die nicht leichtfertig ignoriert werden sollte. Leider sind in den meisten Fällen die Gründe für eine Zertifikatsfehlermeldung Unwissenheit oder Fehlverhalten der Administratoren.

Erfahrungsgemäß zählen zu den drei häufigsten Ursachen:

1. Ein selbstsigniertes Zertifikat
2. Die Angaben im Zertifikat entsprechen nicht den technischen Identifikationsmerkmalen des IT-Systems
3. Das Zertifikat ist abgelaufen

Jetzt könnte man argumentieren, dass das Zertifikat erst einen Tag abgelaufen sei. Es ist aber nicht am Anwenden zu entscheiden, ob ein Zertifikat „trotzdem" weiterverwendet werden kann. Hinzu kommt, dass eine Zertifikatsprüfung üblicherweise beim ersten Fehler abbricht. Somit könnten mehrere Unstimmigkeiten vorliegen.

Fehlermeldungen vermeiden

Das Stichwort ist Planung. Auf folgende Fragen, sollte der IT-Administrator dauerhaft eine Antwort haben:

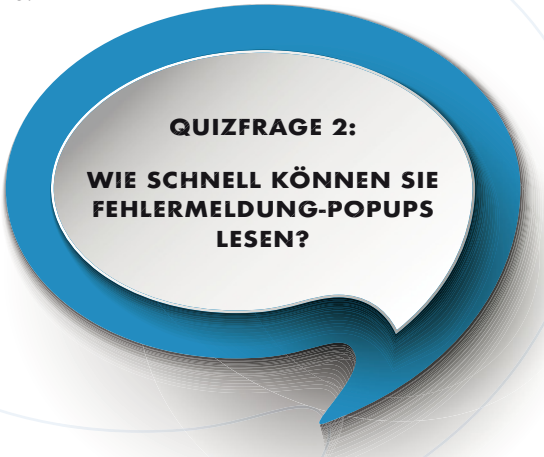
1. Auf welchen Systemen werden Zertifikate benötigt?
2. Auf welchen Systemen wurden Zertifikate ausgestellt?
3. Wann laufen welche Zertifikate aus?
4. Wie sind die Felder in einem Zertifikat richtig zu wählen?
5. Was benötigen Client-Systeme, um das Zertifikat überprüfen zu können?

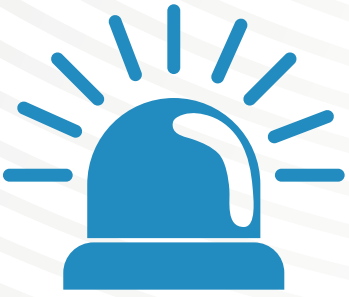
Auf selbstsignierte Zertifikate sollte vollständig verzichtet werden.

Fazit

Ein ordentliches Zertifikatsmanagement erhöht die Gesamtsicherheit nachhaltig.

Holger von Rhein
www.hisolutions.com





VOM FEHLALARM ZUR KATASTROPHE

BCM FÜR DEN ALLTAG

Es sind die großen Stromausfälle und Hacker-Angriffe, die aufhorchen lassen. Unbeachtet bleibt, dass in deutschen Unternehmen täglich ein unscheinbarer Systemausfall zu einer Katastrophe führt. BCM hilft in beiden Fällen.

Ein grundlos ausgelöster Brandmelder, die ausgefallene Klimatisierung im Rechenzentrum, der Fehlalarm im Serverraum oder der unbeabsichtigte Eingriff des Elektrikers in die IT: Es sind unscheinbare Systemfehler, die Unternehmen herausfordern. Denn sie müssen meist externe Techniker mit der Fehlersuche und -behebung beauftragen. In der Zwischenzeit übernehmen schlecht gewartete USVs. Abseits der üblichen Geschäftszeiten, bei mehreren Standorten oder Filialen oder unter dem Druck der USV-Laufzeit wird die Lage schnell unangenehm. Downtime, System-Crash und somit Daten- und Imageverlust drohen!

Schutz durch BCM

Das Business Continuity Management (BCM) ist hier entscheidend, um sich vor eben solchen Schreckensszenarien zu schützen und die IT handlungsfähig zu halten. Angefangen von Disaster Tests über Sensoren-Überwachung und Log Management bis zu Alarmierung, Shutdown und Restart: Gerade KMU befürchten oft, dass diese 360°-Sicherheit ihre Möglichkeiten übersteigt. Doch wo intern das Know-how fehlt, kann jahrelang bewährte Software-Technologie mit externer Expertise eine Lücke füllen.

So sorgt zum Beispiel iQSol mit Log Management, Alerting und Power Management für das gesamtheitliche Krisenmanagement – auch als Managed Security Service. So werden alle Events an Geräten und Software aufgezeichnet und automatisiert alarmiert, sobald etwas außergewöhnlich erscheint. Müssen Systeme heruntergefahren werden, geschieht das mithilfe der PowerApp immer mit Blick auf vorab definierte Abhängigkeiten – ebenso wie der Neustart stets geordnet erfolgt. Wenn zudem doch einmal eine Meldung an die Behörde notwendig ist, sind sämtliche Reports und forensische Ergebnisse entsprechend der Compliance-Vorgaben griffbereit. Und: Neben verschiedenen Appliances ist ein Notfallhandbuch wesentlich, um gut gerüstet zu sein. Es umfasst alle Informationen zu fest definierten Abläufen, IT-Assets, optionalen Vorgehen, Ansprechpartner und mehr, das bei kleinen Katastrophen im Alltag hilft.

www.iQSol.biz

DETECTION & RESPONSE

LÖSUNG ZAHLT SICH AUS

Eine aktuelle Untersuchung des Analystenhauses ESG ergab, dass sich der Einsatz von Lösungen zur Erkennung und Bekämpfung von Cyberangriffen (XDR) für Unternehmen auszahlt.

85 Prozent der Unternehmen gaben an, dass die Erkennung von Cyberbedrohungen und die Reaktion darauf in den letzten zwei Jahren schwieriger wurde. Gründe liegen in der anspruchsvolleren Bedrohungslandschaft, die zunehmende Komplexität der Sicherheitslösungen und dem Mangel an IT-Sicherheitsexperten.

Der Einsatz einer XDR-Lösung kann genau diese Probleme lösen. Bei heutigen Cyberangriffen ist eine schnelle Erkennung und Reaktion entscheidend. Nur so können gesetzliche Meldepflichten eingehalten und zusätzliche Schäden verhindert werden. 65 Prozent der Befragten, die eine XDR-Lösung einsetzen, erkennen Datenschutzverletzungen innerhalb weniger Tage oder schneller. Firmen, die keine solchen Systeme einsetzen, benötigen mindestens eine Woche zur Erkennung. 83 Prozent der XDR-Nutzer können betroffene Systeme innerhalb von Stunden wiederherstellen. Bei den anderen Unternehmen gelingt dies nur 66 Prozent.

www.trendmicro.com

KÖDER CORONA-KRISE

DIGITALE SIGNATUR ZUM SCHUTZ VOR PERFIDEN PHISHING-FALLEN

Die Corona-Pandemie hat die Cybergefährdungslage nochmals verschärft. Sie kommt wie gerufen für Kriminelle, die Phishing-Mails mit Bezug zu COVID-19 versenden, um Lösegelder zu kassieren oder sensible Daten abzugreifen. Die Betrüger bringen E-Mails in Umlauf, in denen sie etwa Heilmittel versprechen oder Unterstützung bei der Beantragung von Finanzhilfen der Bundesregierung anbieten. In vielen Fällen sehen die Fake-Mails täuschend real aus und sind kaum von echten zu differenzieren. Nicht selten werden als Absender bekannte Dienstleister missbraucht, sodass die Wahrscheinlichkeit nochmals größer ist, der Falle im Posteingang auf den Leim zu gehen. Der Einsatz einer digitalen Signatur könnte dies verhindern.

Phishing ist eine äußerst heimtückische Methode, um Schutzbarrieren zu durchbrechen und sich so Zugriff auf Unternehmensnetzwerke zu verschaffen, Datendiebstahl zu betreiben oder Schadsoftware zu platzieren. Besonders kritisch wird es, wenn Betrüger aktuelle Themen wie das Coronavirus missbrauchen, die eine Vielzahl von Personen ansprechen. Stelle man sich einmal folgendes Beispiel vor: Die Mitarbeiter eines großen Energieversorgungskonzerns erhalten eine seriös aussehende E-Mail mit dem Hinweis, dass sie – als Teil eines KRITIS-Betriebes – früher als andere eine Corona-Impfung bekommen. Sie werden gebeten, für weitere Informationen auf einen Link oder Anhang zu klicken. Hoffnungsvoll öffnet ein Großteil der Mitarbeiter die Mail und interessiert sich für die angeblich weiterführenden Details. Und schon haben die Cyberkriminellen ihr Ziel erreicht.

Natürlich gibt es Checklisten, die dabei helfen sollen, nicht auf Phishing-Mails hereinzufallen. Doch gerade wenn E-Mails auf die Schnelle geöffnet werden oder Köder wie die Corona-Krise genutzt werden, hat man fix einen Link angeklickt, ohne sich Gedanken über die zu beachtenden Punkte zu machen. Um diese Gefahr zu umgehen beziehungsweise von Anfang an ausreichend vorzusorgen, gilt es entsprechende Sicherheitsmaßnahmen zu ergreifen. Dazu gehört vor allem die Einbindung einer digitalen Signatur. Denn ein ungebrochenes Siegel signalisiert dem Empfänger, dass die eingegangene E-Mail wirklich vom angegebenen Absender stammt und auf dem Versandweg nicht verändert wurde.

Digitales Unterzeichnen elektronischer Dokumente

Eine digitale Signatur zielt darauf ab, die Identität des Unterzeichners nachzuweisen und die Authentizität und Integrität der elektronischen Nachricht sicherzustellen. Damit E-Mails mit einer Signatur versehen werden können, bedarf es eines qualifizierten Zertifikats, das sich bei einer akkreditierten Zertifizierungsstelle beantragen lässt. Diese sogenannten Certificate Authorithies (CAs), darunter zum Beispiel SwissSign, DigiCert, D-TRUST oder Sectigo, belegen schließlich, dass das Zertifikat, also der persönliche, öffentliche Schlüssel, zu einer bestimmten Person gehört. Eine moderne Lösung erlaubt es, die benötigten Zertifikate über eine Managed Public Key Infrastructure (MPKI) bei der ersten ausgehenden E-Mail des Nutzers automatisch

durch die Appliance zu beziehen. Alternativ sollten sie sich manuell für den jeweiligen User importieren lassen. Für diesen Prozess müssen sämtliche erforderlichen Funktionalitäten wie die PKI, die Konnektoren zu den offiziellen CAs sowie die Zuweisungsmöglichkeiten der Zertifikate zu den Anwendern standardmäßig in der Lösung integriert sein. Alle gängigen E-Mail-Clients unterstützen die Signaturprüfung, sodass der Empfänger keine spezifischen Tools braucht. Insgesamt minimiert eine geeignete Lösung somit den administrativen Aufwand bei der Erstellung digitaler Signaturen und sorgt dafür, den gesamten PKI-Prozess zu beschleunigen. Zudem wird mit der Signatur der öffentliche Schlüssel des Absenders verbreitet, durch den jeder Empfänger potenziell in der Lage ist, eine verschlüsselte Rückantwort zu senden.

Lückenlose E-Mail-Sicherheit

Um auf Nummer sicher zu gehen und nicht nur Phishing, sondern die gesamte Palette an Angriffsmethoden via E-Mail zu verhindern, eignet sich eine professionelle All-in-One-Lösung. Diese sollte auch die E-Mail-Verschlüsselung beinhalten, da unverschlüsselte elektronische Nachrichten problemlos von Dritten abgefangen und mitgelesen werden können. Anders als von vielen erwartet, ist die Verschlüsselung von E-Mails nicht zwangsläufig mit großem Aufwand verbunden. Es gibt bereits Lösungen, die sich durch einen hohen Benutzerkomfort auszeichnen, den gewohnten Arbeitsprozess nicht unterbrechen und eine sichere Kommunikation mit jedermann ermöglichen. Zur Abdeckung der Signatur und der Verschlüsselung eignet sich die Nutzung eines Secure E-Mail Gateway, das beides beherrscht. Das Gateway sollte zusätzlich die Möglichkeit bieten, auch übergroße Dateien geschützt zu übermitteln, damit auf keine unsicheren, kostenfreien Filehosting-Dienste zurückgegriffen werden muss. Zu guter Letzt ist außerdem ein Central Disclaimer Management ratsam, das die E-Mails zentral mit Firmeninformationen ergänzt und das Komplettpaket so optimal abrundet.

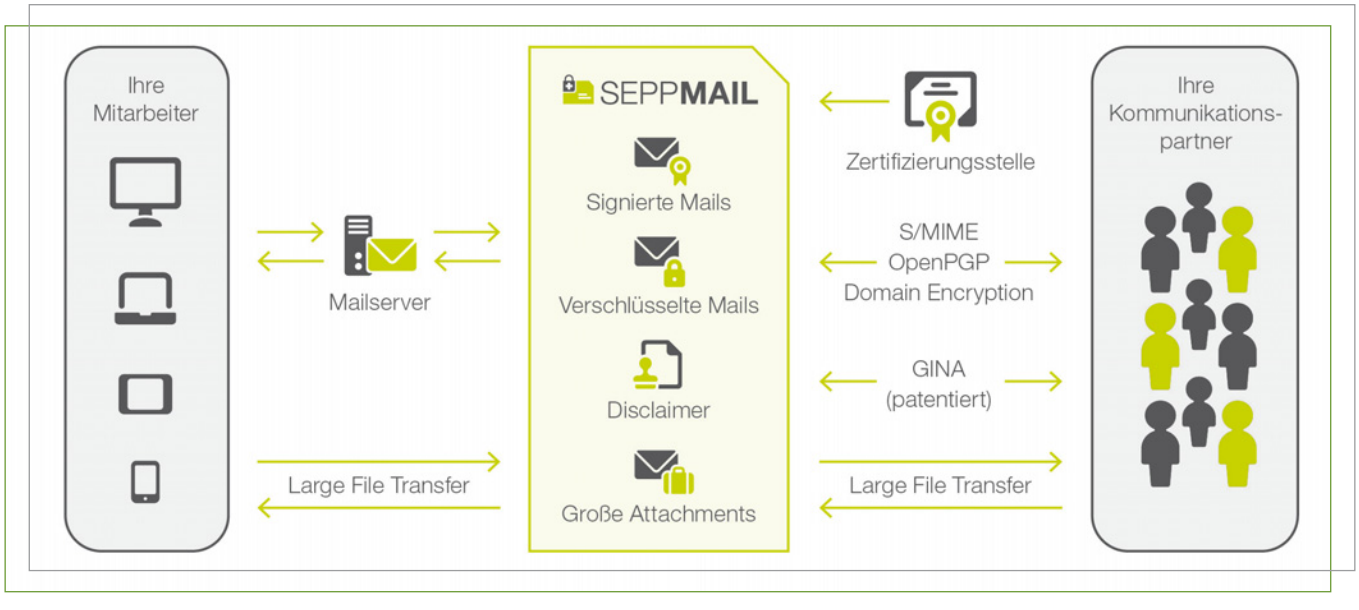
DURCH DIE VERMEHRTE IMPLEMENTIERUNG DIGITALER SIGNATUREN WÜRDEN VIEL WENIGER PHISHING-ATTACKEN ERFOLGREICH ABLAUFEN.

Günter Esch, Geschäftsführer, SEPPmail – Deutschland GmbH, www.seppmail.de

Fazit

Zahlreiche Hacker nutzen die Ängste und Hoffnungen der Menschen hinsichtlich des Coronavirus schamlos aus. Sie locken Firmen mit Phishing-Mails und platzieren auf diese Weise Schadsoftware oder machen sich unternehmensrelevante Informationen zu eigen. Durch die vermehrte Implementierung digitaler Signaturen hingegen würden viel weniger Phishing-Attacken erfolgreich ablaufen. Versehen Unternehmen E-Mails mit einer Signatur, trägt dies sowohl zu einer gesteigerten Sicherheit als auch zu einem verbesserten Image bei. Zur Gewährleistung eines durchgängigen E-Mail-Security-Konzepts sollte auf eine Komplettlösung zurückgegriffen werden, die neben der Signatur auch die E-Mail-Verschlüsselung, den Large File Transfer und das Central Disclaimer Management unterstützt. Mit einer derartigen All-in-One-Lösung ist es nicht länger notwendig, die Mails vor dem Öffnen detailliert zu prüfen, denn man kann sich sicher sein: Sie sind in jeder Hinsicht vertrauenswürdig.

Günter Esch



STUDIE ZUR IT-SICHERHEIT

ENDPOINTS UND ZERO TRUST

DriveLock veröffentlichte als Kooperationspartner der aktuellen Studie „Cyber Security 2020" die wichtigsten Herausforderungen und Strategien beim Schutz von IT-Systemen.

„Die Studienergebnisse zeigen große Unterschiede in der Wahrnehmung der Cyberrisiken zwischen Befragten aus der Führungsebene und aus den Fachbereichen", kommentiert Anton Kreuzer, CEO von DriveLock. Mit 38 Prozent bewerten C-Level-Entscheider den Schutz der Endpunkte als größte Herausforderung, während in den Fachbereichen die externe Bedrohungslage mit 51 Prozent an der Spitze steht.

Das Security-Budget wird von 27 Prozent aller Befragten als weiterer wichtiger Punkt in Bezug auf IT-Security genannt und liegt somit an dritter Stelle der genannten Herausforderungen für die IT-Security. Überraschend an den Ergebnissen ist, welche Aspekte das Schlusslicht bilden und somit als geringstes Risiko eingestuft werden. Die Studie wurde im Juli dieses Jahres erhoben. Zu diesem Zeitpunkt hatten bereits viele Unternehmen im Zuge der Corona-Pandemie auf Homeoffice umgestellt. Dennoch haben insgesamt nur etwa 11 Prozent aller Befragten Remote Work als Herausforderung für die IT-Sicherheit angegeben. Ein Grund dafür kann sein, dass mit dem Schutz von Endpunkten dieser Punkt bereits abgedeckt wird. Allerdings stellen zahlreiche Phishing-E-Mails mit Corona-Bezug oder mögliche Sicherheitslücken bei der Vielzahl neuer Geräte ein nicht zu unterschätzendes Risiko dar.

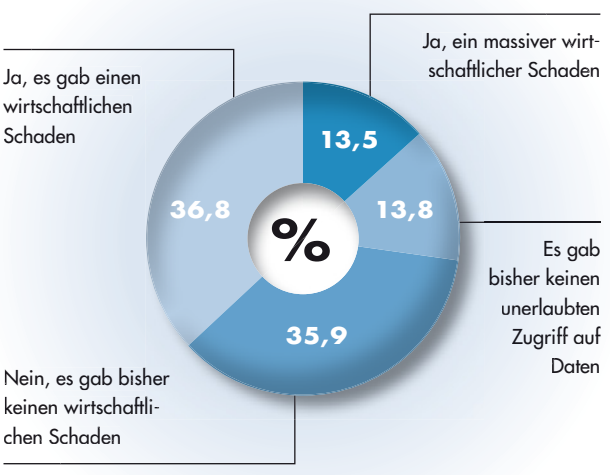
Zero Trust ist angekommen

93 Prozent der Befragten gaben an, dass sich ihr Unternehmen mit dem Security-Konzept Zero Trust beschäftigt. Und das obwohl nur wenige Unternehmen konkrete Investitionen dafür vorgesehen hatten. Die Top 3 Bereiche, in die investiert wird, sind Angriffsabwehr (46 %), Netzwerk-Security (42 %) und Cloud Security (39 %).

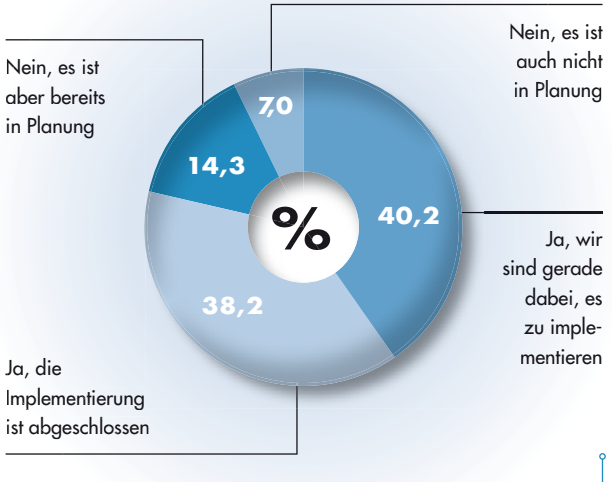
Andreas Fuchs, Vice President Product Management bei Drive Lock erklärt: „Das Zero Trust-Modell ist ein ganzheitlicher Security-Ansatz und umfasst mehrere Sicherheitslösungen. Netzwerk-Sicherheit ist ein ebenso wichtiger Bestandteil in Zero Trust wie Endpoint Detection & Response. Wichtig ist das nahtlose Zusammenspiel aller Security-Module auf einer Zero Trust-Plattform." Das bedeutet, dass Unternehmen zwar nicht direkt in den fortschrittlichen IT-Sicherheitsansatz investieren, aber in Lösungen und Funktionalitäten, die wesentliche Elemente eines Zero Trust-Modells bilden.

www.drivelock.de

IST IN IHREM UNTERNEHMEN DURCH EINEN CYBER-ANGRIFF SCHON EINMAL WIRTSCHAFTLICHER SCHADEN ENTSTANDEN?



HABEN SIE EIN ZERO TRUST-MODELL IMPLEMENTIERT?



MOBILE PROZESSE

FLEXIBEL UND SICHER BESCHLEUNIGEN

Auch in der Fertigungsindustrie setzen sich mobile Prozesse mehr und mehr durch. Mit der zunehmenden Relevanz mobiler Endgeräte in der Produktionsbranche werden auch unternehmenseigene Apps immer wichtiger. Apps machen Produktionssteuerung, Lagerverwaltung und andere Abläufe mobil, damit Mitarbeiter effizienter und komfortabler arbeiten. Unternehmen wiederum erreichen ihre Geschäftsziele deutlich leichter und schneller und profitieren von einem klaren Wettbewerbsvorteil.

Bei all der mobilen Flexibilität stellt sich besonders auch in der Fertigung die Frage nach der Sicherheit. Unternehmen sollten deshalb für den mobilen Einsatz eine Lösung finden, die beides berücksichtigt.

Mehr Zeit für das Wesentliche

Neben der Sicherheit ist Geschwindigkeit ein weiterer entscheidender Faktor. Sobald die internen Apps selbstständig, automatisiert und einfach veröffentlicht werden können, verkürzen sich App-Releases auf wenige Minuten bis Stunden. Das verschafft Unternehmen mehr Zeit für dringendere Aufgaben.

Der Landmaschinenhersteller Claas beispielsweise, nutzt dazu die Technologie von incapptic Connect. Die Implementierungen und Prozessumstellungen dauerten bei Claas insgesamt nur 3 Tage. Seitdem spart sich das Unternehmen bei jeder App-Aktualisierung bis zu drei Stunden. Mittlerweile hat Claas schon zahlreiche Anwendungen mit der incapptic Connect-Lösung entwickelt und über die Unified Endpoint Management-Lösung (UEM) von MobileIron automatisiert auf den mobilen Endgeräten installiert.

Zero-Trust-Ansatz

Durch die mobile Vernetzung vergrößert sich allerdings die Angriffsfläche von Unternehmensnetzwerken. Hier ist von Vorteil, wenn die eingesetzte UEM-Lösung die Distribution der Anwendungen nur an befugte Nutzer und Geräte zulässt.

Dies sollte aber nur der Anfang sein und durch ein transparentes Sicherheitsmodell ergänzt werden, das per default keiner App, keinem Netzwerk und keinem Endgerät vertraut – den Zero-Trust-Ansatz. Passwörter zur Authentifizierung sind anfällig für Missbrauch durch Dritte, sie sind unbequem und nicht mehr zeitgemäß. Wird stattdessen das Mobilgerät der Angestellten zur ID, identifizieren sich Anwender einfach aber unverwechselbar mit dem Gerät, das sie immer mit sich führen.

Fazit

In der Fertigung ist dabei entscheidend, dass all die genannten Funktionalitäten nicht nur auf gängigen Smartphones und Tablets anwendbar, sondern auch auf mobilen Geräten zur Verfügung stehen, die speziell für die Datenerfassung und -verarbeitung in der Industrie hergestellt werden.

Wenn die genannten Faktoren erfüllt sind, können Unternehmen der Fertigungsbranche von der Flexibilität und den Effizienz-Vorteilen mobiler Prozesse profitieren, aber gleichzeitig einfachen und sicheren Zugriff auf die Firmendaten bieten. Das schützt wertvolle Daten und Prozesse und gibt den Mitarbeitern wertvolle Zeit für geschäftsentscheidende Produktinnovationen.

www.mobileIron.com/de

DER MENSCH, DAS SCHWÄC

MIT MANAGED DETECTION & RESPONSE

Manchmal muss man Dinge aus der Hand geben, um sie im Griff zu behalten. Während in Hollywood-Filmen Hacker stets mit großem Aufwand Sicherheitssysteme und Firewalls knacken, sieht die Realität ganz anders aus. Nur ein Bruchteil aller Angriffe erfordert ein solches Maß an intensiver Arbeit. Nachlässige Angestellte und falsch konfigurierte Systeme übernehmen meist die Schwerstarbeit für die Cyberkriminellen und schaffen verwundbare Punkte. Die Cyber-Kill-Kette sucht sich dabei das schwächste Glied der Unternehmenssicherheit - und das ist oft ein Mitarbeiter.

Ein paar Beispiele: Fehlkonfigurationen von Endpunkten sind für ein Drittel aller Sicherheitsvorfälle verantwortlich; ungenaue Fernverwaltungsrichtlinien sorgen für Hunderttausende anfälliger Systeme; 93 Prozent der Mitarbeiter recyceln alte Passwörter. Dies besagt die Telemetrie der Security Intelligence Cloud von Bitdefender, die weit über 500 Millionen Endpunkte analysiert.

Sicherheit erfordert Pflege

Unternehmen versuchen oft nach dem Motto „Deploy and forget", Sicherheitsherausforderungen zu lösen. Das heißt, sie kaufen spezielle Lösungen und übertragen einem ohnehin überlasteten IT-Team einfach noch mehr Verantwortung.

Doch Sicherheitssysteme, die unzureichend gepflegt und überwacht werden, bieten keine Sicherheit. Die Kombination von Lösungen mit spezialisierten Sicherheitsdienstleistungen aber schon. Bisher war die Einrichtung von Security Operations Centers (SOCs) der Königsweg, aber nur für große Unternehmen mit großen Budgets und spezialisierten Mitarbeitern eine Option. Doch der Markt hat sich demokratisiert und für kleinere Unternehmen geöffnet. Künftig werden immer mehr Managed Service Providers Pakete aus MDR-, EDR- und SOC-Diensten anbieten.

Trotz der unzähligen Sicherheitsvorkehrungen von Organisationen, ist der Faktor „Mensch" eine Herausforderung. Menschliches Versagen gibt es bei weitem nicht nur beim User, der einen Anhang mit Malware öffnet oder auf ein Phishing-Programm hereinfällt. Stattdessen umfasst er alles, was schief geht, damit diese Nachricht den Mitarbeiter erreicht, die Malware Fuß fassen und das Sicherheitsereignis unbemerkt bleibt.

Fehlkonfiguriertes WinRM

Auch hier ein paar Beispiele: Das Risiko beginnt mit Fehlkonfigurationen der unternehmensweiten Sicherheitsrichtlinien. Für Hacker sind sie der Himmel auf Erden. So zeigt die Analyse der Bitdefender-Telemetrie beispielsweise, dass Windows Remote Management (WinRM) in der ersten Hälfte des Jahres 2020 mit 55,5 Prozent aller gescannten Endpunkte die Liste der Fehlkonfigurationen anführte. Angreifer suchen nach WinRM-Schwachstellen und falsch konfigurierten Richtlinien, weil sie damit eine vollständige Fernsteuerung erhalten. So können sie Schadcode ausführen, Registrierungsschlüssel ändern, PowerShell-Zugriff gewähren oder sich einfach remote in Computer einwählen.

Aber das Windows-Betriebssystem und „Living-off-the-land"-Tools in Organisationen stellen nur die Spitze des Eisbergs dar. Ein kürzlich veröffentlichter Bericht von Bitdefender und den Marktforschern von ESG zeigt, dass eine Fehlkonfiguration der Endpunkte in 27 Prozent der Fälle der von den Angreifern ausgenutzte Einstiegspunkt ist. Unpassende Richtlinien im Zusammenhang mit Konten, Passwortspeicherung und Passwortverwaltung sind dabei mit 12,5 Prozent die am häufigsten von Einzelpersonen verursachten Fehlkonfigurationen von Endpunkten. Internet-Einstellungen sind eine weitere wichtige und oft übersehene Sicherheitskategorie, auf die 73,1 Prozent aller Fehlkonfigurationen von Endpunkten entfallen. Und ein weiteres Problem entsteht bei SSL 3.0-Downgrade-Angriffen, die es Cyberkriminellen ermöglichen, Man-in-the-Middle-Attacken auf die ansonsten verschlüsselte Kommunikation durchzuführen.

> SICHERHEITSSYSTEME, DIE UNZUREICHEND GEPFLEGT UND ÜBERWACHT WARDEN, BIETEN KEINE SICHERHEIT. DIE EINZIG VERNÜNFTIGE ALTERNATIVE: MANAGED DETECTION & RESPONSE.
>
> Thomas Ehrlich, Regional Sales Director DACH, Bitdefender, www.bitdefender.de

HSTE GLIED IN DER KETTE

(MDR) CYBERRISIKEN IM GRIFF BEHALTEN

Darüber hinaus gefährden Mitarbeiter die Sicherheit, indem sie Sicherheitsrichtlinien zugunsten von anfälligeren Verfahren umgehen, die ihnen schneller und einfacher erscheinen. Hier braucht es klare Richtlinien, die verhindern, dass Mitarbeiter in Sicherheitsverfahren eingreifen. Dabei gilt die Wiederverwendung von Passwörtern als das häufigste menschliche Risiko in einem Unternehmen. Satte 93,1 Prozent der Mitarbeiter verwenden Logindaten, die sie bereits früher genutzt haben. Die Unternehmen tragen Mitschuld an der Misere, denn sie geben den Mitarbeitern die Möglichkeit, diese Passwörter zu wählen.

IT-Abteilungen am Limit

Durch die zunehmende Raffinesse und Diversifizierung von Cyberangriffen und eine personelle Unterbesetzung der IT-Sicherheitsabteilung stehen viele Unternehmen unter Druck. Größere Unternehmen können sich für die Implementierung eines SOC entscheiden, aber diese Kosten sind für KMU schwer zu tragen. In diesem Fall ist die einzig vernünftige Alternative, die Sicherheit in gute Hände zu geben: Managed Detection & Response (MDR).

Mittelständische Unternehmen sollten auf eine integrierte Endpunktkonfiguration setzen, bei der die Sicherheit eines Unternehmens in der Verantwortung eines dedizierten Teams bleibt, das aus der Ferne einen vollständigen Einblick in die Infrastruktur hat. Wie bei einem System-Audit sollten Unternehmen dabei mit einer umfassenden Endpunkt-Risikoanalyse versorgt werden - sowohl aus technischer Sicht als auch mit Blick auf den Schwachpunkt Mensch.

MDR bietet die Vorteile eines SOC zu einem Bruchteil der Kosten. MDR-Teams können mit jedem Unternehmen zusammenarbeiten, um vorab genehmigte Szenarien für die Reaktion auf Vorfälle zu erstellen und so die Reaktionszeiten zu beschleunigen, so dass die richtigen Sicherheitsvorkehrungen getroffen werden, lange bevor ein Angreifer die Infrastruktur kompromittiert.

Bitdefender bietet erweitertes MDR-Portfolio

Dieser Grad an Transparenz kann erreicht werden, wenn man sich an Sicherheitsteams wendet, die über umfangreiche Cybersicherheits-Expertise in anspruchsvollen kommerziellen und nationalen Sicherheitsumgebungen verfügen und aufgrund ihrer Aufgaben und Verantwortlichkeiten von der Industrie zertifiziert (GCIA, GCIH und/oder SANS) sind. Sie müssen in der Lage sein, Richtlinien und Konfigurationen auf die Bedürfnisse einer Organisation zuzuschneiden, um blinde Flecken abzudecken.

Die MDR-Angebote und -Funktionalitäten von Bitdefender orientieren sich eng an diesen Sicherheitsbedürfnissen und senken gleichzeitig die Barrieren, denen sich Unternehmen bei der Nutzung von MDR gegenübersehen. Das Angebot kombiniert Bitdefenders Sicherheitstechnologien für Endpunkt-Detection und Analysen des Netzwerkverkehrs mit der Expertise hochqualifizierter Analysten. Der Dienst identifiziert Sicherheitsvorfälle und sorgt für eine schnelle Reaktion zur Abwendung von Angriffen oder Eindämmung von Schäden. Sie unterstützen damit Kunden, die sich eingestanden haben, ihre Sicherheit nicht mehr voll im Griff zu haben - damit deren Bedrohungserkennung, Reaktionsfähigkeit und Cyberresilienz jederzeit auf dem höchsten Stand ist.

Thomas Ehrlich

WELCHE STRATEGIE SCHÜTZT DEN ENDPUNKT?

DAS GESAMTBILD IM AUGE BEHALTEN

In einer perfekten Welt wäre Software vollkommen sicher und Angriffe wären unmöglich. Sie ist jedoch zu komplex, um perfekt entworfen oder programmiert werden zu können, jedenfalls, wenn Menschen im Spiel sind. Selbst die sichersten Anwendungen haben Fehler.

Um diesem Problem Rechnung zu tragen, wurden im Lauf der Zeit zahlreiche Best Practices entwickelt. Diese sind im Großen und Ganzen seit Jahren gleichgeblieben: „Inventarisieren Sie präzise alle Ihre IT-Assets, führen Sie regelmäßig Scans durch, wenden Sie Software-Patches an und kümmern Sie sich um Schwachstellen, sobald sie entdeckt werden". Allerdings kann es wesentlich schwieriger werden, diese Best Practices umzusetzen, wenn es in großem Stil geschehen muss.

DAS ZIEL VON EDR IST DIE ERKENNUNG UND REAKTION – DOCH UM BEDROHUNGEN EFFEKTIV FINDEN UND BESEITIGEN ZU KÖNNEN, BRAUCHEN DIE UNTERNEHMEN EINE GANZHEITLICHE SICHT.

Jörg Vollmer, General Manager Field Operations DACH und CEE, Qualys, www.qualys.com

Die gute, schlechte alte Zeit

Wie COVID-19 gezeigt hat, können diese Verfahren leicht an ihre Grenzen stoßen, für selbstverständlich gehalten oder falsch angewendet werden. Die jetzige Situation mit zahlreichen verteilten und mobilen Mitarbeitern hat erhebliche Anpassungen nötig gemacht.

Für viele Unternehmen ist die Verwaltung ihrer IT-Assets ein hartes Stück Arbeit. Sie erfordert, ein genaues Inventar aller IT-Assets zu erstellen und dann laufend zu aktualisieren. Ohne ein solches Asset-Inventar kann jedoch kein Unternehmen von sich sagen, dass es sicher ist. Denn wenn IT-Assets vorhanden sind, von denen das Unternehmen nichts weiß – die sogenannte Schatten-IT –, woher will es dann die Gewissheit nehmen, dass diese Assets geschützt und auf dem neuesten Stand sind? In ähnlicher Weise ist das Scannen der Assets und Webanwendungen auf potenzielle Sicherheitsprobleme seit jeher ein notwendiger Prozess, der Probleme aufzeigen kann.

Gepatcht wird schon seit der Entwicklung der ersten Softwareprogramme. Der Begriff Patch stammt aus der Zeit, als noch Lochkarten verwendet wurden und Korrekturen an einem Programm durch Stanzen oder Zukleben einzelner Löcher vorgenommen werden konnten. Diese Metapher trifft es sehr gut: Software ist zu oft ein Flickenteppich.

Heute bringen Microsoft, Adobe und andere Hersteller regelmäßig Patch-Pakete heraus, um den Unternehmen die Möglichkeit zu geben, Schwachstellen zu beheben. Es kann jedoch Wochen oder gar Monate dauern, bis die Patches wirklich im operativen Betrieb angewandt werden. Genau aus diesem Grund ist es von großer Bedeutung, dass die Endgeräte selbst geschützt werden. Dies nicht zuletzt durch die steigende Anzahl an Mitarbeitern, die im Homeoffice arbeiten. Ist das Gerät nicht mehr direkt an die Unternehmensinfrastruktur gekoppelt, wird es zur leichten Zielscheibe für Angreifer.

Vor- und Nachteile von EDR-Tools

In der letzten Dekade sind EDR-Tools (Endpoint Detection & Response) auf den Markt gekommen, die den Schutz an den Endpunkten verstärken und effektivere Reaktionen auf neuere und sich entwickelnde Bedrohungen ermöglichen sollen. EDR hat die Endpunktsicherheit für viele Unternehmen verbessert. Jedoch können EDR-Lösungen auch neue Schwierigkeiten für das IT-Sicherheitsteam mit sich bringen und als Verteidigung gegen raffiniertere Angriffe möglicherweise unwirksam sein. Der Grund: Herkömmliche EDR-Lösungen konzentrieren sich meistens nur auf die Aktivitäten auf den Endpunkten. Dadurch fehlt der nötige Kontext zur genauen Analyse von Angriffen. Es werden zahlreiche Fehlalarme ausgegeben. Das kann die Incident-Response-Teams unnötig belasten und dazu führen, dass zahlreiche punktuelle Lösungen eingesetzt werden müssen, um Licht ins Dunkel zu bringen.

Das Ziel von EDR ist die Erkennung und Reaktion – doch um Bedrohungen effektiv finden und beseitigen zu können, brauchen die Unternehmen eine ganzheitliche Sicht. Wenn eine Bedrohung oder verdächtige Aktivität entdeckt wird, müssen sie schnell handeln, um festzustellen, was die Information oder der Indikator bedeutet und mit welchen Maßnahmen Sie weitere Kompromittierungen verhindern können.

Umfassender Schutz

Viele Angreifer setzen heute Automatisierungstechniken ein. Das wirft für die IT-Sicherheit ein neues Problem auf. Um die nötige Skalierbarkeit zu gewährleisten, sollten die Sicherheitsteams, sofern möglich, Aktionen automatisieren – seien es Konfigurationsänderungen, die Implementierung von Patches und Updates oder das Blockieren des Datenverkehrs einer bestimmten IP-Adresse. Das verkürzt die Reaktionszeit und verringert die Belastungen für die IT-Mitarbeiter. Darüber hinaus müssen die Teams aber auch schnell und einfach feststellen können, welche anderen Systeme im Netzwerk anfällig sind, und Korrekturmaßnahmen in der gesamten Umgebung automatisieren.

Qualys Multi-Vector EDR wurde entwickelt, um die Stärken von EDR wirksam einzusetzen, zugleich aber die Sichtbarkeit und die Funktionalitäten über den Endpunkt hinaus zu erweitern und dadurch umfassenderen Schutz zu bieten. Es macht sich die native Leistungskraft, Skalierbarkeit und Präzision der Cloud-Plattform zunutze. Dadurch kann die Lösung Unternehmen umfassende Übersicht vermitteln und Telemetriedaten aus ihrer gesamten Umgebung verfügbar machen.

Es handelt sich um einen völlig neuen Ansatz für EDR. Das Unternehmen geht vom herkömmlichen EDR-Konzept aus – also von einer Lösung, die speziell auf den Schutz von Endpunkten zugeschnitten ist – und weitet dieses Konzept auf das übrige Netzwerk aus. Der Grund dazu ist, dass viele Angriffe heute mehrschichtig sind. Die verdächtige oder böswillige Aktivität, die am Endpunkt entdeckt wird, ist oft nur ein kleiner Teil eines größeren, komplexeren Angriffs. Die Organisationen brauchen deshalb Übersicht über die gesamte Umgebung, um den Angriff und seine Auswirkungen auf den Endpunkt sowie die möglichen Folgen an anderen Stellen des Netzwerks wirklich vollständig zu verstehen. Ein Eckpfeiler ist dabei die Fähigkeit, die Kontextdaten zu jedem Asset zu erfassen und zu bewerten.

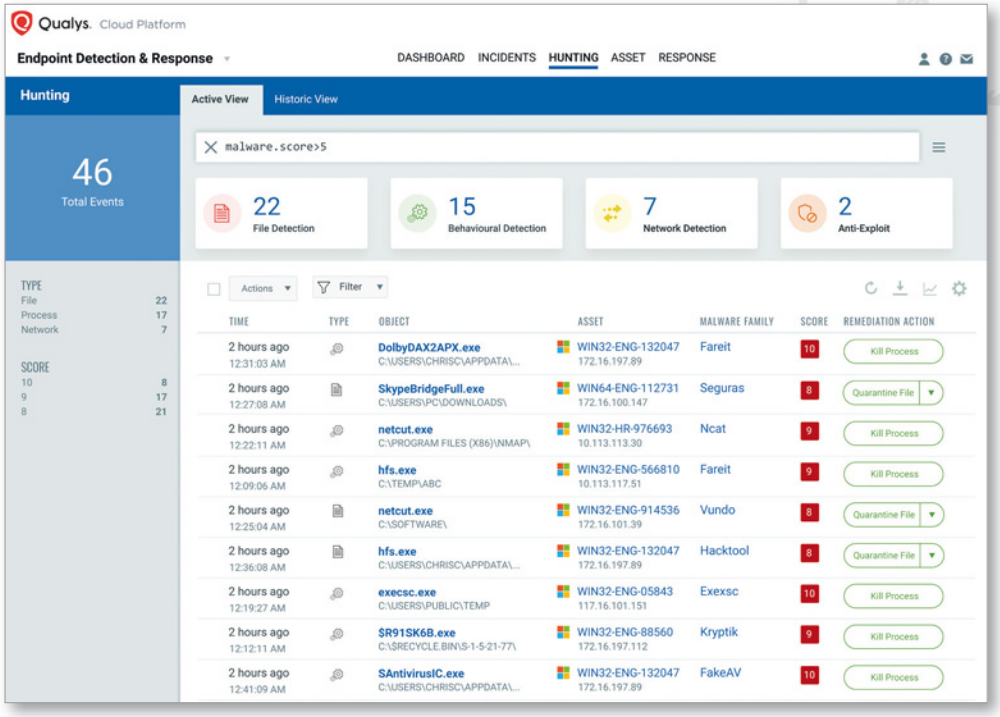
Es ist notwendig, Überblick über die gesamte Angriffskette zu erlangen und gleichzeitig die Zahl der False Positives und False Negatives zu verringern.

Wenn Mitarbeiter von zu Hause aus arbeiten und dabei Geräte des Unternehmens oder eigene Systeme nutzen, ist es wichtiger denn je, das Gesamtbild im Auge zu behalten, auch wenn sich der Perimeter weiter verschiebt.

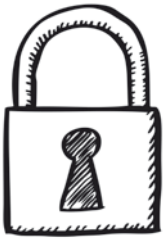
Planen für die Zukunft

Die COVID-19-Pandemie hat CISOs gezwungen, zu überdenken, was Sicherheit für das Unternehmen wirklich bedeutet. Der Wechsel zur Telearbeit hat bewirkt, dass eine Reihe schwieriger Entscheidungen getroffen werden mussten. Und angesichts der wirtschaftlichen Auswirkungen der Krise, wird die IT-Sicherheit besser belegen müssen, dass sie ihre Ziele tatsächlich erreicht. Denn nun geht es noch mehr darum, den Security-Ansatz über das Modell Form-follows-Function zu belegen. Denn nicht zuletzt ist Sicherheit ein Bestandteil der Funktion selbst.

Jörg Vollmer



Mittels Suchfunktion können betroffene Systeme innerhalb weniger Augenblicke gefunden werden.



MIKRO-SEGMENTIERUNG

DAS NETZWERK SICHERN WIE DEN FIRMEN-KOMPLEX

Ransomware-Angriffe nehmen mehr und mehr zu, nicht zuletzt begünstigt durch die fortschreitende Digitalisierung, Cloudmigration und breit angelegte Tele-Arbeit. Nun gilt es, die Strategie für Netzwerksicherheit ebenfalls zu adaptieren.

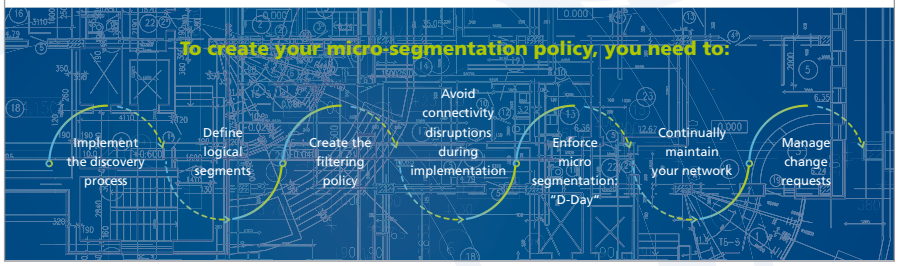
Mehr Homeoffice. Mehr Cloud. Mehr Einfallstore. All das sind Resultate der Entwicklungen, die Firmen und deren digitale Infrastruktur in den vergangenen Monaten beobachtet haben. Die Entwicklungen mussten dabei aufgrund der COVID-19-Pandemie und subsequenter Lockdowns oftmals im halsbrecherischen Tempo durchgeführt werden, um die Handlungsfähigkeit trotz aller Umstände für Unternehmen und Mitarbeiter garantieren zu können. Was dabei oftmals dem wirtschaftlichen Interesse untergeordnet wurde, war der Sicherheitsgedanke. Während Mitarbeiter mit Fernzugriffen versorgt und Services und Applikationen in die Cloud verlagert wurden, wurden auch unzählige neue Einfallstore für Cyberkriminelle geschaffen – ein Nebeneffekt, der immer mehr zum Problem wird.

Erpressungswelle rollt über digitale Landschaft

Ransomware ist keine neue Bedrohungsart, sie existiert seit Jahren und schickt sich an, Unternehmen zu erpressen, indem sie Daten verschlüsselt und Zugriffe verhindert. Ist solch eine Schadsoftware erst einmal im System, so kann sie für Firmen existenzbedrohend sein, warnt unter anderem auch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Durch die eingangs erwähnten Entwicklungen während der Pandemie hin zu einer Neuen Normalität mit vermehrter Tele-Arbeit und neuen Netzwerkstrukturen mit Cloud- und Multi-Cloud-Lösungen haben sich jedoch noch einmal mehr Angriffsvektoren für Cyberattacken eröffnet. Das hat dazu geführt, dass die Anzahl der Ransomware-Angriffe in den vergangenen Monaten durch die Decke ging.

Dabei legen die Übeltäter mehr und mehr Skrupellosigkeit an den Tag. Während früher besonders Banken und andere Finanzdienstleister im Fokus der Attacken waren, da sie mit hohen potenziellen Lösegeldern und heiklen persönlichen Daten lockten, haben sich auch die Kriminellen an die Gesundheitskrise angepasst: Sie haben Krankenhäuser und Kliniken als neue Opfer ausgespäht. Diese sind durch oftmals mangelndes Fachwissen im Bereich IT und die Überbelastung durch Covid-19 leichte Beute.

A Blueprint for Creating a Micro-segmentation Policy



Mit Mikro-Segmentierung gegen digitale Eindringlinge

Eine effektive Möglichkeit, wie man sich gegen Ransomware verteidigen kann, ist die Mikro-Segmentierung. Dahinter verbirgt sich die Strategie, das Netzwerk in kleine Bereiche zu teilen und an den Grenzen den Netzwerkverkehr zu überwachen. Auf diese Weise können die Segmente isoliert betrieben werden, Zugriffe lassen sich genau kontrollieren und Angreifer – oder deren Schadsoftware – die in eines der Segmente vordringen, sitzen dort fest. Selbst wenn der äußere Schutzring eines Unternehmens durchbrochen wird, kann der Schaden trotzdem in Grenzen gehalten werden. IT-Sicherheitsfachleute haben zudem eine längere Reaktionszeit, um gegen den Angriff vorzugehen.

EINE EFFEKTIVE MÖGLICHKEIT, WIE MAN SICH GEGEN RANSOMWARE VERTEIDIGEN KANN, IST DIE MIKRO-SEGMENTIERUNG.

Elmar Albinger,
Regional Sales Director, AlgoSec,
www.algosec.com

Die Strategie dabei ist dieselbe, wie sie viele Unternehmen auch in der Absicherung des eigenen Bürokomplexes anwenden: restriktive Bewegung zwischen den einzelnen Gebäuden und Überwachung der Zu- und Ausgänge. Was in der physischen Welt dabei hilft, selbst bei Einbrüchen den Schaden an der Firma zu minimieren, hilft auch in der virtuellen. Werden die entsprechenden Sicherheitsmaßnahmen jedoch nicht umgesetzt, drohen in beiden Welten – digital und analog – die gleichen Konsequenzen: finanzieller Schaden für das Unternehmen und irreparabler Vertrauensverlust bei Kunden und Partnern.

IT-Sicherheit erfordert proaktives Handeln

Solange die virale Pandemie die Welt in Atem hält, solange wird auch die virtuelle Pandemie mit Schadsoftware-Angriffen und Erpressungsversuchen Hoch-Konjunktur haben. Entsprechend müssen Unternehmen proaktiv damit beginnen, ihre Netzwerke gegen Angreifer und Malware zu wappnen. Mikro-Segmentierung bietet dabei einen einfachen Ansatz, der bei der richtigen Implementierung zu einem Stützpfeiler der eigenen Sicherheits-Architektur werden kann.

Elmar Albinger

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Elmar Albinger, Thomas Ehrlich, Günter Esch, Uwe Gries, Kai Grunwitz, Christian Kleinschroth, Carsten Marmulla, Carina Mitzschke, Manfred Müller, Silvia Parthier, Ulrich Parthier, Holger von Rhein, Sebastian Spethmann, Jörg Vollmer, Stefan Vollmer

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 Datenver arbeitungsanlagen 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.

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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. 28.
Preisliste gültig ab 1. Oktober 2020.

Mediaberatung & Content Marketing-Lösungen it management | it security | it daily.net:
Kerstin Fraenzke
Telefon: 08104-6494-19
E-Mail: fraenzke@it-verlag.de

Karen Reetz-Resch
Home Office: 08121-9775-94,
Mobil: 0172-5994 391
E-Mail: reetz@it-verlag.de

Online Campaign Manager:
Vicky Miridakis
Telefon: 08104-6494-21
miridakis@it-verlag.de

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

Erscheinungsweise:
10x pro Jahr

Verkaufspreis:
Einzelheft 10 Euro (Inland),
Jahresabonnement, 100 Euro (Inland),
110 Euro (Ausland), Probe-Abonnement
für drei Ausgaben 15 Euro.

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 Bezugs zeitraumes 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

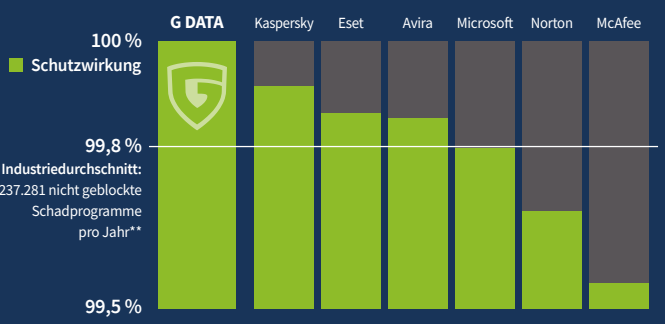
G DATA

TRUST IN
GERMAN
SICHERHEIT

Manchmal braucht man einfach **verlässlichen Schutz.**

Beste IT-Sicherheit. Unabhängig geprüft. **Top bewertet**.

gdata.de/beste-sicherheit



*Durchschnitt abgewehrter Angriffe aus den folgenden drei Tests:
AV-Comparatives Malware Protection Test 09/2020, AV-Comparatives Real-World Protection Test 09/2020, AV-Test 08/2020 zu 0-Day Malware und weit verbreiteter Malware.

**117,4 Millionen Schadprogramm-Varianten pro Jahr laut BSI Jahresbericht 2020

3 Tests, 1 Bestergebnis:

G DATA Internet Security ist die einzige Antiviren-Software, die in allen drei aktuellen Vergleichstests* 100 % aller Gefahren abwehrte.

AV-TEST CERTIFIED WINDOWS 09/2020 TOP PRODUCT

AV comparatives ADVANCED+ Malware Protection SEP 2020