# itmanagement

OKTOBER 2022

INKLUSIVE 64 SEITEN

**IT SECURITY SPEZIAL**

FINANCE & ACCOUNTING

## RAUS AUS DEM KRISENMODUS

Ralph Weiss, BlackLine und Ralf Noffke, Horváth

**DSAG Spezial**

ab Seite 15

Theobald Software

ab Seite 16

THEOBALD SOFTWARE

INFRASTRUKTUR-MONITORING

Die beste Versicherung für Rechenzentren

Aagon

# SOAR

## Mehr als nur ein BuzzWord mit

ACMP

Desktop Automation

CAWUM

Managed Software

Schwachstellen-management

- ✓ Bedrohungen frühzeitig erkennen und beheben
- ✓ Automatische Reaktions-Routinen auf Schwachstellen
- ✓ SOAR und mehr aus einer Oberfläche

Weitere Infos unter www.aagon.com

Wir sind dabei!

itsa EXPO CONGRESS

Besuchen Sie uns in Halle 6 an Stand-Nr.: 6-404

Gratis-Dauerkarte sichern mit dem Code **AagonITSA2022**

## LIEBE LESERINNEN UND LIEBE LESER,

im Oktober stehen sowohl für Unternehmen als auch für uns zwei sehr wichtige Veranstaltungen an. Zum einen der DSAG-Jahreskongress in Leipzig und zum zweiten die it-sa in Nürnberg. Doch warum wichtig?

Das Thema SAP-Migration treibt nach wie vor viele Unternehmen um. Sie ist komplex, kann sich über viele Monate oder noch länger ziehen und ein durchschlagender Erfolg ist am Ende nicht garantiert. Gerade in Zeiten der digitalen Transformation benötigen oder suchen Unternehmen Flexibilität, Support und praktikable Lösungen, die sie allein oft nicht finden. Das diesjährige Motto des DSAG-Jahreskongresses „Auf der Suche nach … Erfolg!" unterstreicht diese Aussage. Doch nicht nur die Suche nach Lösungen ist wichtig, sondern auch der rege Austausch untereinander. Was eignet sich dafür besser als ein Kongress?

Gleiches gilt für die it-sa. Cloud- und Netzwerksecurity, Ransomware-Angriffe, Datensicherheit: Themen, die Unternehmen ständig begleiten, aber nicht nur im beruflichen Umfeld, sondern auch im Privaten eine zunehmend größere Rolle spielen. Die it-sa sieht sich als Plattform für Lösungen rund um diese Problematiken und als Vernetzer zwischen „IT-Sicherheitsverantwortlichen und IT-Sicherheitsanbietern". Auch sie bringt Unternehmen, Experten und Anwender zusammen und befeuert den Diskurs, welche Strategie wohl die sinnvollste wäre.

Beiden Veranstaltungen haben wir in dieser Ausgabe viel Raum in einem Spezial gegeben.

Übrigens, besuchen Sie uns auf der it-sa, Halle 6 Stand 401, und kommen mit einem meiner Kollegen ins Gespräch!

Herzlichst

Carina Mitzschke | Redakteurin it management

40

10
COVERSTORY

# INHALT

20


34

30


Inklusive
64 Seiten

IT SECURITY SPEZIAL

37

# INTELLIGENTE AUTOMATISIERUNG

## FÜR MEHR NACHHALTIGKEIT IM UNTERNEHMEN

Immer mehr Unternehmen setzen Klimaneutralität und Nachhaltigkeit ganz oben auf ihre Agenda. Das bestätigt auch eine aktuelle Bitkom-Umfrage: 45 Prozent der Unternehmen wollen bereits bis zum Jahr 2030 klimaneutral sein – weitere 37 Prozent bis 2040.

Moderne Technologien wie Intelligente Automatisierung können Unternehmen dabei unterstützen, dem Ziel der Klimaneutralität näher zu kommen. Denn Intelligente Automatisierung sorgt für mehr Effizienz, Flexibilität, Geschwindigkeit und Einblick, was die Nachhaltigkeitsstrategie von Unternehmen voranbringt. Richtig eingesetzt bringt Intelligente Automatisierung viele Vorteile mit sich, damit Unternehmen das Ziel der Klimaneutralität erreichen können.

Viele Unternehmen setzen den ersten Schwerpunkt ihrer Automatisierungsstrategie auf die Outbound-Logistik: So nutzen Online-Händler Intelligente Automatisierung, um die Anzahl an Kundenbestellungen und Informationen über Volumen, Gewicht und Zielort der Ware einzuschätzen und Packlisten für Fahrzeuge sowie Verpackungsmaterial zu planen. Neben geringeren Transportkosten kann der Warenbestand im Lager mithilfe der Automatisierung genau verfolgt und kontrolliert werden.

Eine Effizienzsteigerung der Supply Chain durch Intelligente Automatisierung ist außerdem ein wichtiger Aspekt, um sich auf den Weg zur Klimaneutralität zu begeben. Denn die Sicherstellung maximaler Effizienz in der Lieferkette ermöglicht es Unternehmen zudem, die Energiekosten zu reduzieren. Software-Roboter (sogenannte Digitale Mitarbeiter) sind in der Lage, aus den Daten des Lieferkettenmanagements Erkenntnisse zu gewinnen, um beispielsweise Lieferrouten zu optimieren oder Lagerbestände zu kontrollieren. So werden weniger Ressourcen verschwendet. Eine effiziente Lieferkette ist daher eine wichtige Säule in der ökologischen Nachhaltigkeitsstrategie eines Herstellers, um unnötigen Rohstoffverbrauch zu vermeiden, Energiekosten zu reduzieren, papierbasierte Dokumentationen abzuschaffen und die Präsenz von Mitarbeitern und die damit verbundenen Reisen zu minimieren.

Intelligente Automatisierung ermöglicht es Versorgungsunternehmen, umfangreiche Datensätze von IoT-Sensoren und -Geräten im gesamten Energienetz zu sammeln und zu aggregieren, um eine vorausschauende Wartung und Vorhersage zu unterstützen.

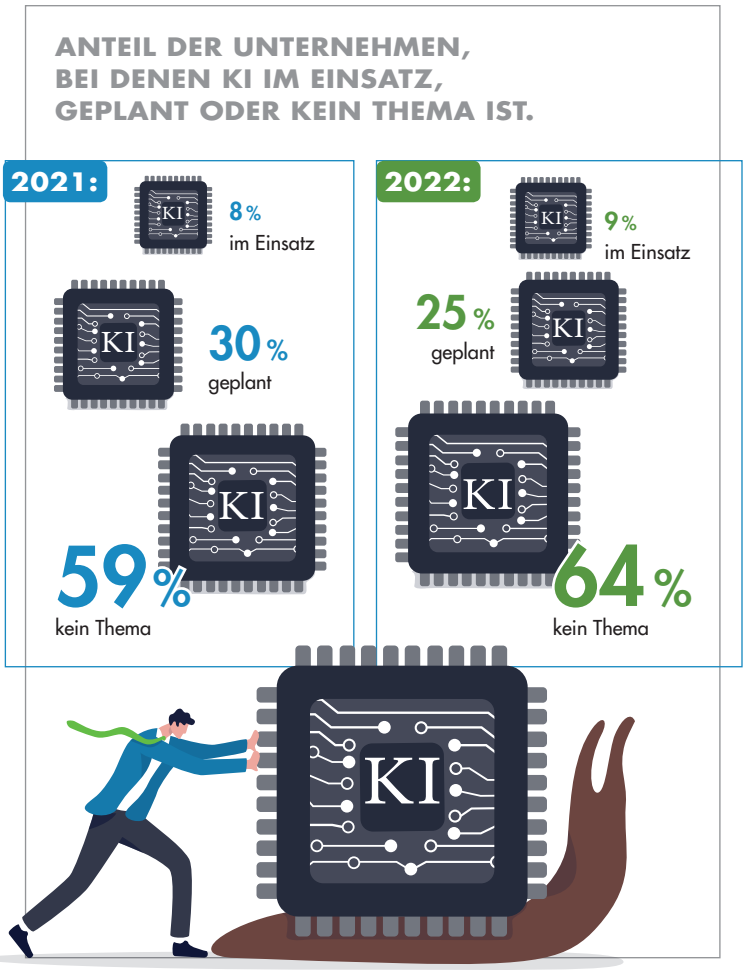
***www.blueprism.com***

# KÜNSTLICHE INTELLIGENZ

## IM SCHNECKENTEMPO VORWÄRTS

Unternehmen in Deutschland erkennen vor allem Chancen im Einsatz von Künstlicher Intelligenz und sehen verglichen mit dem Vorjahr mehr Vorteile beim Einsatz der Technologie – zugleich steigt der Anteil der Unternehmen, die KI im Einsatz haben, nur sehr langsam. Beklagt werden vor allem ein Mangel an Fachkräften und Daten. Das sind Ergebnisse einer Studie im Auftrag des Digitalverbands Bitkom. Demnach sehen 18 Prozent KI weit überwiegend als Chance für das eigene Unternehmen, 47 Prozent eher als Chance. Nur 20 Prozent sehen KI eher als Risiko, gerade einmal 1 Prozent weit überwiegend als Risiko. Allerdings geben nur 9 Prozent an, KI selbst einzusetzen. Vor einem Jahr waren es 8 Prozent. Zugleich sagen nur noch 25 Prozent, sie diskutieren oder planen den KI-Einsatz. Vor einem Jahr waren es noch 30 Prozent, vor zwei Jahren aber nur 22 Prozent. Der Anteil der Unternehmen, für die KI kein Thema ist, steigt von 59 auf 64 Prozent. „Viele Unternehmen sind gezwungen, in einen Krisenmodus zu schalten: Steigende Energiekosten und hohe Inflationsraten sowie unterbrochene Lieferketten als Folge von Corona-Pandemie und dem Krieg gegen die Ukraine setzen der Wirtschaft zu. Da bleibt wenig Raum, an neue Technologien und Geschäftsmodelle für die Zukunft zu denken", sagt Bitkom-Präsident Achim Berg.

***www.bitkom.org***



# CLOUD COMPUTING

## ZERTIFIZIERUNG VERDREIFACHT

Die Anzahl der Cloud-Zertifizierungen bei IT-Dienstleistern ist in den vergangenen drei Jahren drastisch angestiegen. Zwischen 2020 und 2022 betrug das Wachstum mehr als 300 Prozent. Dies ist das Ergebnis einer weltweit laufenden Untersuchung der Information Services Group (ISG) bei den Ökosystemen der etablierten Cloud-Anbieter.

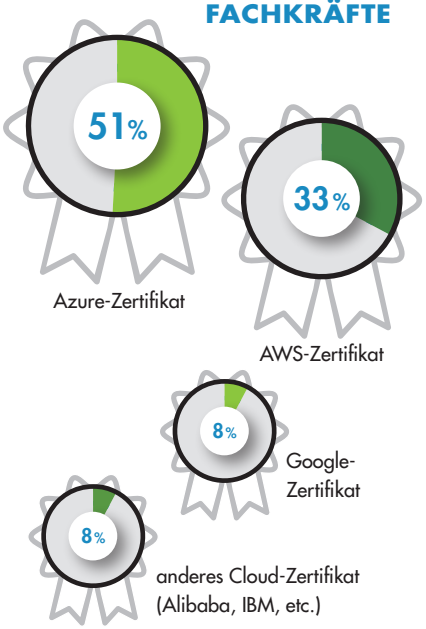
Die Gesamtheit der cloudzertifizierten Fachkräfte bei den IT-Serviceanbietern verfügt demnach zu 51 Prozent über eine Azure-Zertifizierung, zu 33 Prozent über eine Amazon Web Services-Zertifizierung sowie zu 8 Prozent über eine Google w. Andere Anbieterzertifikate kommen zusammen ebenfalls auf einen Anteil von 8 Prozent.

Treiber dieser Entwicklung ist ISG zufolge, dass die Nachfrage der Unternehmen nach IT-Modernisierung durch Cloud-Technologien so hoch ist wie nie zuvor. Ein Großteil dieser Modernisierung findet in sogenannten Hyperscale-Clouds statt. Die effektive Nutzung von Hyperscale-Cloud-Funktionen erfordert jedoch dediziertes Spezial-Know-how beim Aufbau und beim Betrieb cloudbasierter Architekturen. Um auf dieses Fachwissen zurückgreifen zu können, wenden sich Unternehmen zunehmend an IT-Dienstleister. Diese wiederum weiten Cloud-Zertifizierungen bei ihren Fachkräften drastisch aus, um der Nachfrage gerecht zu werden.

Heute bewerten Unternehmen IT-Serviceanbieter zunehmend danach, ob diese das notwendige Know-how und ausreichend Erfahrung aufweisen, Cloud-Architekturen aufzubauen und zu unterhalten. Die starke Zunahme bei der Anzahl der Zertifizierungen ist die Folge dieser Nachfrage, allerdings ist sie nicht automatisch ein Hinweis auf die zukünftige Nachfrage. Doch ist davon auszugehen, dass sich die Nachfrage nach zertifizierten Fachkräften weiter erhöhen wird, zumal bereits mehr als die Hälfte der Unternehmen eine Public Cloud nutzen. Und noch mehr planen, in Zukunft mehrere Clouds gleichzeitig zu verwenden.

***www.isg-one.com***

**CLOUDZERTIFIZIERTE FACHKRÄFTE**




---

## **E-MAIL-DIENSTLEISTER** DIE TOP 3 EIGENSCHAFTEN

Als Standard der modernen Kommunikation sind E-Mails schon lange etabliert.

Über die Hintergrundprozesse, die erfolgreiche E-Mail-Kommunikation erst ermöglichen, machen wir uns jedoch nur selten Gedanken. Meistens vertrauen wir unsere gesamte E-Mail-Kommunikation – und damit auch unsere wichtigsten Daten – einem Dienstleister an, der dies für uns übernimmt. Sicherheit ist deshalb das wichtigste Auswahlkriterium bei der Wahl eines E-Mail-Anbieters.

***mailbox.org***

**Wie erkennt man überhaupt einen sicheren E-Mail-Anbieter?**

- Server sollte ausschließlich in Deutschland betrieben werden
- Keine Verwertung von Nutzerdaten
- Verschlüsseltes Postfach

OPERATIONAL SERVICES
YOUR ICT PARTNER

Microsoft Partner

Microsoft

- Gold Cloud Platform
- Gold Datacenter
- Silver Messaging
- Silver Application Development
- Silver Collaboration and Content

# MOBILE ARBEITSPLÄTZE MIT MICROSOFT 365 KLUG DURCHDACHT

*und professionell umgesetzt*

Die Erwartungen an moderne Arbeitsplätze sind heutzutage extrem hoch. Unternehmen, die ihre Teams mit einem umfassenden Service begeistern, profitieren von der hohen Zufriedenheit und Motivation ihrer Mitarbeiter. Doch die professionelle Einrichtung und den 24/7 IT Service Desk für den sorglosen Agile Workplace können viele Betriebe nicht alleine abdecken.

Setzen Sie auf unser Microsoft-zertifiziertes Expertenteam, das Sie von der vollautomatischen Konfiguration über die Administration bis hin zu Conditional Access und Security-Konzept rundum zuverlässig mit allen wichtigen Services versorgt.

So werden mobile Arbeitsplätze auch in Ihrem Unternehmen zur Erfolgsgeschichte. Profitieren Sie von unserer Expertise als langjährig erfahrener Microsoft Gold Partner.

operational-services.de/microsoft-365

Machen Sie mit uns Agile Workplace schnell, einfach und sicher zum Firmenstandard

# RAUS AUS DEM KRISENMODUS

## REIN IN MEHR ZUVERSICHT

Ein Gespräch über die Impulskraft von Krisen, Fortschritte in der Digitalisierung und die Notwendigkeit belastbarer Finanzzahlen für die Unternehmenssteuerung.

Inspiriert durch die Herausforderungen der aktuellen wirtschaftlichen und politischen Situation und die Auswirkungen im F&A (Finance und Accounting), diskutierten Ralph Weiss (Geo VP DACH BlackLine) und Ralf Noffke (Principal Horváth) mit Ulrich Parthier, Herausgeber it management, über den Fachkräftemangel, die digitale Transformation und die Bedeutung von Blitzableitern.

? **Ulrich Parthier:** *Das Top-Management muss Unternehmen durch unruhige Zeiten navigieren. Herr Weiss, was erleben Sie, wenn Sie mit den Verantwortlichen in den Unternehmen sprechen?*

**Ralph Weiss:** Die aktuelle Dynamik bringt einen nie dagewesenen Druck mit sich. Viele Unternehmen spüren, dass sie die Komplexität der weltwirtschaftlichen und weltpolitischen Situation dann erfolgreich meistern, wenn sie ihre Prozesse anpassen. Sie müssen agil und fokussiert sein und dabei die Datenqualität im Auge behalten.

**Ralf Noffke:** Die angesprochene Dynamik zeigt, wie wichtig Finanzinformationen sind, um ein Unternehmen wirkungsvoll zu steuern. Manager müssen belastbare Entscheidungen treffen und dafür benötigen sie aktuelle und akkurate Zahlen.

> VIELE UNTERNEHMEN SPÜREN, DASS SIE DIE KOMPLEXITÄT DER WELTWIRTSCHAFTLICHEN UND WELTPOLITISCHEN SITUATION DANN ERFOLGREICH MEISTERN, WENN SIE IHRE PROZESSE ANPASSEN. SIE MÜSSEN AGIL UND FOKUSSIERT SEIN UND DABEI DIE DATENQUALITÄT IM AUGE BEHALTEN.
>
> Ralph Weiss, Geo VP DACH, BlackLine, www.blackline.com

? **Ulrich Parthier:** *Hier könnte es ja helfen, wenn die Unternehmen sich die Vorteile digitaler und automatisierter Prozesse bedienen. Was kann man da tun?*

**Ralf Noffke:** Zuerst ist es wichtig, ein klares Bild über die Strategie und die zentralen Steuerungsgrößen des eigenen Business zu haben. Darauf aufbauend müssen Unternehmen ihr Ambitionsniveau definieren und eine klare Roadmap für die Digitalisierung und Automatisierung schaffen. Dabei hilft es, cross-funktionale Teams zu bilden, die nicht nur eine Funktion oder einen Geschäftsbereich im Blick haben, sondern Zusammenhänge erkennen und Schnittstellen nutzen.

**Ralph Weiss:** Die Unternehmen benötigen ein Change-Management. Vom führenden Management bis hin zum Sachbearbeiter muss das Prozessverständnis verändert werden. Der End-to-End-Gedanke rückt bei immer mehr Unternehmen ins Bewusstsein. Das gilt für jeden Prozess. Das Umzusetzen kommt einem Paradigmenwechsel gleich.

? **Ulrich Parthier:** *Das ist leichter gesagt als getan.*

**Ralph Weiss:** Es scheint, dass ein solcher Paradigmenwechsel schwer ist. Aber lassen Sie es mich exemplarisch an den Herausforderungen im Finance und Accounting erklären. In der Finanzbuchhaltung wird das Fundament für zukunftssichere Entscheidungen gelegt. Wer hier die Möglichkeiten agiler Prozesse und moderner Softwareplattformen nutzt, kann sich langfristig von fehlerhaften, oft noch manuellen Prozessen befreien. Die Durchgängigkeit der Abläufe und deren Trans-

parenz sind das A und O. Warum? Weil es sowohl auf akkurate Daten als auch auf deren Bewertung Einfluss hat. Die Qualität ist entscheidend. Denn ist die Zahlenbasis falsch, kann das zu Fehlentscheidungen führen.

**Ralf Noffke:** Durch Standardisierung können Unternehmen Freiräume schaffen. Diesen Freiraum können die Verantwortlichen nutzen, um detaillierte Analysen zu machen und sich den wirklich wichtigen Herausforderungen zu widmen.

? **Ulrich Parthier:** *Wie sieht der Nutzen konkret aus? Die Unternehmen kämpfen um Wirtschaftlichkeit und die Sicherung ihrer Marktposition. Und das soll die Digitalisierung richten?*

**Ralf Noffke:** Definitiv. Ich kann das aus der Praxis bestätigen, weil ich mich täglich mit Finanztransformation, Prozessoptimierung und Digitalisierung beschäftige. Der Punkt ist: an der Digitalisierung kommt keiner mehr vorbei. Digitalisierung ist aber keine Insellösung etwa im Finanzbereich. Die Potenziale entstehen vor allem durch eine konsequente End-to-End-Orientierung über alle Prozesse hinweg. Die meisten davon tangieren die Finanzen und dort findet auch die Validierung und Qualitätssicherung statt. Hinzu kommt der Fachkräftemangel. Mit stupider Fleißarbeit lässt sich heute niemand mehr begeistern. Die Leute wollen wertstiftende Arbeit, etwas bewegen und Karriere machen. Für die Finanzabteilung heißt das, sie sollte zum Beispiel den Monatsabschluss optimieren und orchestrieren. Am besten strukturiert sie ihn so, dass er zu einem weitestgehend automatisierten Prozess wird.

**Ralph Weiss:** Davon profitieren nicht nur die Mitarbeiter, weil sie Zeit für wertvollere Arbeit haben. Auch der CFO ist happy, denn dank einem digitalen Modern Accounting Prozess hat er jederzeit den Überblick. Das hat noch andere positive Effekte. Unternehmen, die saubere Zahlen präsentieren, haben einen besseren Zugang zum Kapitalmarkt. Dafür müssen die Daten belastbar sein. Die Zahlen sollten kontinuierlich und nicht nur zum Periodenende validiert werden. Auch das Vertrauen potenzieller Partner, Banken oder Investoren wird größer. Dieses Vertrauen zahlt sich aus – gerade jetzt, da die Zinsen ja wieder steigen. Und noch etwas. Ich finde, dass die richtigen Finanzdaten auch eine Art Blitzableiter sind, sprich wenn die Märkte gebeutelt werden, sorgen solide Zahlen dafür, dass ein Unternehmen jederzeit weiß, wo es steht und seine Spielräume kennt.

? **Ulrich Parthier:** *Angenommen, mein Unternehmen verfügt über diese Voraussetzungen, wo sehen Sie die nächsten wichtigen Veränderungen auf uns zukommen im Bereich Finance & Accounting?*

**Ralf Noffke:** Predictive Forecasting ist für viele Unternehmen der nächste Schritt. Das ist jedoch nur sinnvoll möglich, wenn die Datenqualität korrekt und aktuell ist. Das ist mit modernen Tools wie etwa von BlackLine durchaus möglich. Weiter in die Zukunft geschaut wird Prescriptive Analytics zum Einsatz kommen. Das erscheint einem vielleicht wie ein Blick in die Glaskugel, aber die KI-Technologie wird uns zunehmend vorausschauende Prognosen ermöglichen. Das wird weit über die Analyse und Bewertung zurückliegender Daten hinausreichen. Aber das ist noch Zukunftsmusik, auch wenn es schon erste Ansätze gibt. Die Digitalisierung macht Unternehmen, die diese pro-aktiv umsetzen, zu Gewinnern in ihren Märkten. Der digitale Fortschritt hat schon immer für eine Prozessoptimierung gesorgt, für mehr Geschwindigkeit und vor allem für Innovation. Und genau das können moderne Accounting-Lösungen leisten, damit Unternehmen sicher in die Zukunft gesteuert werden.

! **Ulrich Parthier:** *Herr Weiss, Herr Noffke, herzlichen Dank für diese Einblicke und Einschätzungen.*


DER PUNKT IST: AN DER DIGITALISIERUNG KOMMT KEINER MEHR VORBEI. DIE POTENZIALE ENTSTEHEN VOR ALLEM DURCH EINE KONSEQUENTE END-TO-END-ORIENTIERUNG ÜBER ALLE PROZESSE HINWEG.

Ralf Noffke, Principal Horváth
www.horvath-partners.com

# BESCHLEUNIGER

## RISE WITH SAP UND BLACKLINE

Mit Blick auf die weltwirtschaftliche und weltpolitische Situation fühlen sich viele Unternehmen unter Druck gesetzt. Sie wissen, dass sie nur dann erfolgreich sein werden, wenn sie ihre Prozesse anpassen. Den Verantwortlichen ist klar, dass sie einerseits agiler und andererseits fokussierter vorgehen müssen. In diesem Spannungsfeld bietet das Ökosystem RISE with SAP im Zusammenspiel mit BlackLine konkrete Hilfestellungen und Lösungen für die Neuausrichtung von Finanz- und Controlling-Strukturen.

Gerade wenn es darum geht, ERP-Systeme auf das nächste Level zu heben, sind Akribie und vorausschauendes Handeln gefragt. Es werden einerseits viele Ressourcen benötigt und es besteht andererseits die Chance, alte Prozesse über Bord zu werfen. Die Cloud bietet ein so großes Spektrum an Möglichkeiten, dass sich ihr im Grunde genommen kein Unternehmen verschließen kann – sofern man nicht den Fehler macht, mit alten Daten und Prozessen umzuziehen. Zum einen müssen weniger oder keine hauseigenen Rechenzentren betrieben werden, es besteht ein automatischer Zugriff auf die aktuellsten Software-Versionen, die Einhaltung von Datenschutz und Compliance ist geregelt und – nicht zuletzt – der Aufwand seitens der IT ist wesentlich geringer, wenn Unternehmen auf die Cloud setzen.

### Akkurate Daten in Echtzeit

Aufgrund des aktuellen Transformationsdrucks müssen sich die Firmen mit neuen Technologien rüsten, um langfristig erfolgreich zu sein. Der RISE with SAP-Ansatz mit S/4HANA und BlackLine kann hier entscheidende Wettbewerbsvorteile bringen. Aus Business-Sicht geht es bei Transformationsprojekten insbesondere darum, ein solides Zahlenmaterial direkt im Zugriff zu haben, um das eigene Unternehmen optimal steuern zu können.

Der Trend geht längst weg von Individuallösungen. Entscheidet sich ein Unternehmen für den Wechsel in die Cloud und setzt dabei auf SAP und seine zahlreichen Partnerlösungen, lassen sich schnell Quick-Wins und Synergien erzielen. Im Kontext des Finance & Controllings können die hoch integrativen Lösungen von SAP und BlackLine dafür sorgen, dass das Management unkompliziert auf akkurate Daten in Echtzeit zugreifen und damit das Unternehmen gezielter steuern kann.

### Die neue Konstante: Veränderung

Aufgrund des Paradigmenwechsels von Individuallösungen hin zu schnell umsetzbaren konfigurierbaren Lösungen, benötigen die Unternehmen ein gezieltes Change-Management. Vom führenden Management bis hin zum Sachbearbeiter gilt es, das Prozessverständnis zu verändern. Alle müssen verinnerlichen, wie wichtig valide Unternehmenszahlen sind und dass jeder einzelne seinen Anteil daran hat. Der End-to-End-Gedanke rückt dabei immer mehr in den Fokus.

ES ZEICHNET SICH AB, DASS ORGANISATIONEN, DIE SICH DER DIGITALISIERUNG VERSCHLIESSEN UND DENEN ES AN DER NÖTIGEN AGILITÄT MANGELT, GERINGERE ZUKUNFTSCHANCEN HABEN.

Ralph Weiss, Geo VP DACH, BlackLine, www.blackline.com

Der RISE with SAP-Ansatz fördert diesen Veränderungsprozess nicht zuletzt deshalb so nachhaltig, weil das SAP-Ökosystem so vielfältig und innovativ ist. Es integriert nicht nur das ERP-Kernsystem, sondern auch viele weitere Funktionen und Lösungen im direkten Umfeld. Damit ist vielen Unternehmen bei der Umsetzung ihres Transformationsprozesses konkret geholfen.

Nichtsdestotrotz ist die Umstellung von der alten Welt auf eine neue Cloud-basierte Plattform ein großes Investment, das ganz klar einem definierten Return on Investment (ROI) folgen muss. Daher reicht es oft nicht aus, allein auf die Funktionalität und Mehrwerte zu vertrauen. Das Ganze muss sich rechnen. Das Zusammenspiel von BlackLine und SAP kann hier den entscheidenden Unterschied machen: Die Prozesse lassen sich in der Finanzbuchhaltung neu und zukunftsorientiert gestalten und vor allem automatisieren. Das verbessert den ROI der digitalen Transformation maßgeblich. Warum? Weil BlackLine komplementär zu RISE with SAP ist und Unternehmen die Möglichkeit bietet, mit einem integrierten Lösungsportfolio lückenlos zu digitalisieren. Die Vorteile: kurzer Wertschöpfungszyklus, geringerer TCO, kurze Amortisierung, agile Finance-Prozesse.

# DIGITALISIERUNG

**Alles aus der Automatisierung rausholen**

In der Praxis zeigt sich immer wieder, dass Unternehmen ihr Digitalisierungsvorhaben nicht isoliert betrachten dürfen. Diejenigen, die vorausschauend und ganzheitlich eine konsequente End-to-End-Orientierung im Blick haben, werden sich leichter tun als diejenigen, die noch im weitverbreiteten Silo-Denken verhaftet sind. Funktionale Fit-Gap-Analysen sind der falsche Weg, da sie in der Regel zu Punktlösungen führen. Unternehmen müssen Prozesse End-to-End denken.

Sie müssen alte Verhaltensweisen und Strukturen über Bord werfen und sollten nicht den Fehler machen, diese in die Zukunft - also die Cloudstruktur – zu überführen. Unternehmen, die bereits in der Vergangenheit ihre Finanzabteilung in weiten Teilen automatisiert haben, profitieren davon. Sie verfügen über die besten Voraussetzungen für den Wechsel in die Cloud, denn sie kämpfen nicht mehr mit den veralteten Prozessen, wie beispielsweise einem manuellen Datenabgleich, etwa beim Monatsabschluss.

Doch leider ist nach wie vor der Automatisierungsgrad in Verbindung mit dem Finanzabschluss relativ gering – er liegt durchschnittlich bei 15 Prozent. Mit BlackLine sind im Zusammenspiel mit S4/HANA bis zu 70 Prozent an Automatisierung möglich. Das wirkt sich positiv auf den gesamten Accounting- und Controlling-Prozess aus, denn es entlastet das Finance-Team maßgeblich, indem es Zeit für wichtigere Aufgaben freisetzt und liefert eine akkurate Datenbasis. Entscheidet sich ein Unternehmen, das Altsystem mit BlackLine bereits vor der Transformation zu optimieren, besteht die Chance, in der neuen Umgebung mit modernen Prozessen zu starten. Das ist für Unternehmen von entscheidender Bedeutung, denn es versetzt das Management in die Lage, Entscheidungen auf einem wesentlich gesicherteren Niveau zu treffen.

**Schon heute wissen, was morgen passiert**

Mit BlackLine wird die Wertschöpfung durch die Investition in eine Transformation wesentlich erhöht. Denn dadurch wird das gesamte Finance & Accounting sowie das Controlling in die Lage versetzt, die Struktur und die Prozesse den heutigen und künftigen Anforderungen anzupassen. Zudem trägt das Unternehmen maßgeblich zur Agilität und zur sicheren Steuerung eines Unternehmens bei. Und es kommt noch besser: Predictive Forecasting ist das neue Zauberwort. Unternehmen, die über ein Maximum an Digitalisierung verfügen und jederzeit Zugriff auf Finanzdaten in Echtzeit haben, sind schon heute in der Lage, sehr realistische Prognosen für die nächsten Monate abzugeben. Das sorgt für die allseits gewünschte Entscheidungssicherheit und versetzt die Unternehmen in die Lage, agil auf die zukünftigen Herausforderungen zu reagieren.

Es zeichnet sich ab, dass Organisationen, die sich der Digitalisierung verschließen und denen es an der nötigen Agilität mangelt, geringere Zukunftschancen haben. Umso wichtiger ist es zu begreifen, dass die Digitalisierung kein „Nice to have" ist, sondern ein überfälliges To-Do. Deshalb sollten Unternehmen unbedingt auf das richtige Pferd, pardon – Zukunftskonzept, setzen. Wie sagte schon Henry Ford: „Wenn ich die Leute gefragt hätte, was sie wollen, hätten sie gesagt: schnellere Pferde". Also – es geht darum, auf den Fortschritt zu vertrauen und den Mut zur Veränderung zu haben. Darin liegt die Zukunft.

***Ralph Weiss***

itmanagement

it-daily.net
Das Online-Portal von itmanagement & itsecurity

SAVE THE DATE

# Roadmap IT 2.0

## 19. Oktober 2022
## Digitalevent

SCAN ME

https://www.it-daily.net/roadmapit/

#roadmap22

# WILLKOMMEN IM STILLSTANDSLAND

Wer das letzte Editorial des E3-Magazins von Peter Färbinger, seines Zeichens Chefredakteur und ausgewiesener Experte der SAP-Szene gelesen hat, dürfte zusammengezuckt sein. Seine glasklare Analyse vom Zustand der SAP lässt sich kurz zusammenfassen: Keine Ideen, keine sichtbaren Innovationen, Stillstand bis Rückschritt auf allen Ebenen, Börsenvernichtungs-Weltmeister. Mit einem Satz: das perfekte Missmanagement. Im Lateinischen nennt man diese Garde die der Cunctatoren, die Zauderer, und damit das Gegenteil der Visionäre.

Wie lautete der Titel des Editorials so schön:
Nichtstun ist keine Option.
Das sollten sich die SAP-Anwender zu Herzen nehmen.

Die Lähmung der SAP-Community können jetzt nur die Partner selbst richten.
Mit neuen Produkten und Dienstleistungen und natürlich die neuen Konkurrenten der SAP, die da heißen Workday, Salesforce, AWS, ServiceNow, aber auch ein wiedererstarktes Microsoft, Google & Co.

Was erwartet Sie also auf dem diesjährigen DSAG-Kongress:
Endlich wieder vermehrter Kontakt zu Kollegen und den Anbietern und somit wieder einen regen und visionären Austausch.

EINE KLEINE AUSWAHL AN NEUIGKEITEN FINDEN SIE IN DIESEM DSAG SPEZIAL.

# KEINE KOMPROMISSE

## SCHNELLERE UND BESSERE PROZESSE IM SAP-UMFELD

Eine SAP-Integration stellt viele Unternehmen vor Herausforderungen. Schwieriges einfach zu machen, ist das Ziel von Theobald Software. Wie dies umgesetzt werden kann, was man beachten sollte und warum die Lösung relativ einfach sein kann, darüber sprach it management mit Peter Wohlfarth, Geschäftsführer Theobald Software.

**it management:** *Der diesjährige Jahreskongress der DSAG steht ganz unter dem Motto „Auf der Suche nach Erfolg". Als Geschäftsführer von Theobald Software, wie definieren Sie Erfolg für Ihr Unternehmen?*

**Peter Wohlfarth:** Erfolg ist für mich in erster Linie eins: Kunden erfolgreich machen. Wenn wir als Unternehmen mit unseren Lösungen, unserem Team und Expertise dafür sorgen, dass unsere Kunden erfolgreicher werden, weil sie beispielsweise schneller und besser in ihren Prozessen und Entscheidungen werden, dadurch Kosten sparen und effizienter werden, dann haben wir als Unternehmen Erfolg.

**it management:** *Schnellere und bessere Prozesse: Sie sprechen hier ein Thema an, das viele Unternehmen umtreibt: die SAP-Integration. Mit welchen Schwierigkeiten kämpfen beziehungsweise auf welche Probleme treffen Unternehmen hier?*

**Peter Wohlfarth:** Bevor wir uns den Schwierigkeiten widmen, sollten wir zuerst einmal betrachten, warum SAP-Integration überhaupt notwendig sein kann. In einem SAP-System fallen typischerweise sehr viele Daten an. Sollen diese Daten nun außerhalb von SAP in irgendeiner Form verarbeitet oder verwendet werden – etwa für BI & Analytics, Planung & Konsolidierung oder Prozess-Automatisierung – benötigt man eine Schnittstelle, die diesen Job im besten Fall automatisiert, sicher und performant erledigt. Je nachdem, wie man diese Herausforderung angeht, begegnet man Schwierigkeiten in unterschiedlichster Anzahl und Komplexität.

Bei eigenentwickelten Lösungen sind es die fehlende Wartbarkeit und Flexibilität, um auf Updates, neue Anforderungen und andere Änderungen in der Systemumgebung reagieren zu können. Der Aufwand, diese zu entwickeln und zu warten, wird häufig unterschätzt. Zudem ist die Abwanderung von Knowhow ein wichtiger Aspekt: Sobald Mitarbeiter, die mit der Entwicklung betraut waren, das Unternehmen verlassen, kann Expertise verlorengehen. Explodierende Kosten sind die Folge.

SAP selbst bietet auch Software an, um Daten auszuwerten und weiterzuverarbeiten. Man bewegt sich also komplett im SAP-Universum – eine One-Vendor-Strategie, denen viele Unternehmen kritisch gegenüberstehen, da homogene IT-Landschaften schnell eine Abhängigkeit erzeugen können.

SAP-eigene Lösungen erweisen sich zudem oft als weniger performant, sind kostenintensiv und erfordern nicht selten einen hohen Beratungs- und Schulungsaufwand. Auch die offenen Standards, die SAP in der Vergangenheit geschaffen hat, genügen oft nicht den Ansprüchen der Unternehmen und Anwender.

Es können aber auch noch einige sehr elementare Schwierigkeiten auftreten, völlig losgelöst von der Frage, welche Tools man einsetzen sollte. Eine SAP-Integration entbindet mich nicht von fachlichen Problemen: Das eine ist die Datenqualität. Schlechte Stammdaten werden durch SAP-Integration nicht besser. Darüber hin-

aus muss ich es fachlich verstehen, damit ich etwas Sinnvolles daraus ableiten kann. Was möchte ich eigentlich erreichen, was ist mein Use Case? Eine SAP-Integration beispielsweise verbunden mit Ansätzen von Self-Service BI ist eine großartige Sache, löst aber nicht alle Probleme, sondern schafft womöglich neue, vor allem wenn es um die Dateninterpretation geht.

**it management:** *Kurz gesagt extrahiert Theobald Software Daten aus SAP, um sie in diversen Datenbanken bereitzustellen. Können Sie dies kurz näher erläutern?*

**Peter Wohlfarth:** Wir stellen SAP-Daten nicht nur in Datenbanken zur Verfügung, sondern in nahezu jedem Drittsystem. Dazu gehören neben klassischen Datenbanken Cloud-Storages, Data Lakes sowie BI- und Analytics Tools. Diesen Bereich bezeichnen wir gerne als (Massen-) Datenextraktion, wobei es – je nach Use Case – nicht nur um die Extraktion von SAP-Daten geht, sondern auch um das Zurückschreiben in SAP. Es werden nicht selten mehrere Hundert Millionen Datensätze extrahiert.

Wir sind jedoch nicht „nur" eine Schnittstelle, die Daten von A nach B schieben kann. Das ist die rein technische Betrachtung. Doch was haben Kunden und Nutzer eigentlich davon, wenn SAP-Daten in anderen Systemen zur Verfügung stehen? Für uns geht es immer um die Frage, welchen Mehrwert – oder neudeutsch Business Value – wir den Kunden bieten. Neben Kosteneinsparungen und einer sicheren, flexiblen und skalierbaren Datenextraktion ist es vor allem eins: Wir möchten Menschen befähigen, bessere Entscheidungen zu treffen. Und das können Sie, indem ihnen eine valide Datenbasis schnell verfügbar gemacht wird.

**it management:** *Datenextraktion ist kein einfaches Thema. Wie einfach könnte es aber sein?*

**Peter Wohlfarth:** Datenextraktion an sich muss nicht schwierig sein. Sie wird aber vor allem dann schwierig, wenn es kom-

WIR MÖCHTEN MENSCHEN BEFÄHIGEN, BESSERE ENTSCHEIDUNGEN ZU TREFFEN. UND DAS KÖNNEN SIE, INDEM IHNEN EINE VALIDE DATENBASIS SCHNELL VERFÜGBAR GEMACHT WIRD.

Peter Wohlfarth, Geschäftsführer, Theobald Software, www.theobald-software.com

plex wird. Der Prozess muss zuverlässig, performant und skalierbar für Millionen von Datensätzen sein. Er muss zudem sicher, auditierbar und im besten Fall kostengünstig in Anschaffung, Implementierung (Stichwort Low-Code/No-Code) und Wartung sein. Daten existieren an unterschiedlichen Orten und in unterschiedlichen Formaten in SAP – den Zugriff auf all diese SAP-Daten zu ermöglichen, das ist eine Herausforderung. Die oben erwähnten Schwierigkeiten durch etwa eigenentwickelte Softwarelösungen potenzieren sich hier.

**it management:** *Thema New Normal: Dieses wirkt sich natürlich auch auf die SAP-Anwenderlandschaft und -Systeme aus. Gerade die Integration von SAP-Prozessen in die Cloud stellt Unternehmen vor Herausforderungen, weckt aber auch Chancen.*

**Peter Wohlfarth:** SAP-Prozessintegration, egal ob von On-Prem in die Cloud oder von Cloud zu Cloud, ist per se kompliziert. Es ist technisch sehr anspruchsvoll, allein schon aus Sicherheitsgründen, es müssen technische Grenzen überschritten werden. Aber es ist eben auch ein wunderbar spannendes Thema mit unendlich vielen Use Cases. Beispielsweise beginnt ein Prozess in SAP und endet außerhalb von SAP: das könnte ein Kundenauftrag in SAP sein, der anschließend noch in das externe Logistiksystem übertragen wird. Oder in die andere Richtung: Eine Stammdatenanlage muss außerhalb des SAP-Systems einen Workflow durchlaufen und wird schlussendlich in SAP entsprechend verbucht. Die spannende Frage ist hier: Warum macht man das? In erster Linie aus Effizienzgründen. Der User muss seine gewohnte Umgebung nicht verlassen. Er kann alles in seinem cloud-basierten CRM-System machen, auch wenn er zwischendurch Daten aus dem SAP-System benötigt. Er benötigt hierfür aber weder einen direkten Zugang zu SAP noch muss er zwischen den Systemen hin- und herwechseln.

**it management:** *Was ist das Besondere an Ihrer Lösung?*

**Peter Wohlfarth:** Mit einer unabhängigen Schnittstellen-Suite wie unserer entledigt man sich der oben beschriebenen Schwierigkeiten. Wir sorgen für nahezu uneingeschränkte Freiheit bei der Auswahl der Anwendungssoftware, da die zuständigen IT-Entscheider keine Kompromisse in puncto Kompatibilität eingehen müssen. Wichtig zu erwähnen ist zudem die Agilität unserer Schnittstelle, denn sie ist besonders einfach auf andere benötigte Daten oder neue Zielumgebungen adaptierbar.

Darüber hinaus können Unternehmen den Zugriff auf die Daten im SAP-System auf die notwendigen Informationen beschränken, um so die Sicherheit des Systems zu verbessern. Der IT steht damit ein ganzheitliches Werkzeug zur Verfügung, um alle Systeme miteinander zu verknüpfen und auch zukünftige Zielsysteme sicher einzubinden.

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

# MITTELSTANDSSTUDIE 2022

## DIGITALISIERUNG VON GESCHÄFTSREISEN

Bei Geschäftsreisen sind manuelle und papierbasierte Prozesse eine Last, die den heutigen Erwartungen der Mitarbeitenden widerspricht. Die Lust, geschäftlich zu verreisen und Kunden oder Partner persönlich zu treffen, ist groß. Sie vergeht aber schnell, wenn sich im Gepäck wieder Formulare und Belege sammeln. Im Zuge der COVID-19-Pandemie hat gerade der Mittelstand viel in IT-Infrastrukturen und digitale Tools investiert. Laut der jährlichen Mittelstandsstudie von SAP Concur sind 40 Prozent der Mitarbeitenden im deutschen Mittelstand durch die COVID-19-Pandemie aber auch anspruchsvoller geworden, was den Einsatz digitaler Tools bei ihrem Arbeitgeber angeht. Die Studie verdeutlicht, wie Unternehmen die Digitalisierung beim Reise- und Ausgabenmanagement gezielt für sich nutzen und die Bedürfnisse der Mitarbeitenden auf ihrem Weg zurück an den Arbeitsplatz und raus in die Welt erfüllen können.

### Fokussiert arbeiten

Digitale Meetings am geschäftlichen Laptop oder Diensthandy sind durch den Wechsel zwischen Büro und Homeoffice zum Alltag bei vielen Mittelständlern geworden. Vier von zehn Mitarbeitende im Mittelstand (42 %) sind der Meinung, dass weitere IT-Lösungen zu einer Verbesserung virtueller Arbeitsumgebungen führen sollen. Sie sagen aber auch, dass Geschäftsreiseaktivitäten dadurch nicht ersetzt werden können. Vielmehr hat ein gutes Drittel der Befragten (35 %) nun die Erwartung, dass ihr Arbeitgeber auch Apps bereitstellt, die Geschäftsreisen einfacher gestalten – gerade mit Blick auf Flugchaos, weltweite Krisen oder Pandemieregeln.

### Ein langer Weg zur papierlosen Reise

Digitale Lösungen vereinfachen die Abrechnung von Mitarbeiterausgaben wie Reisekostenabrechnungen. Immerhin bei einem Drittel der Unternehmen aus dem Mittelstand (32 %) können eingescannte Belege schon digital eingereicht werden. Bei ebenfalls einem Drittel (33 %) der Mitarbeitenden von mittelständischen Unternehmen ist das Einreichen von Belegen für Reisekosten und Spesen bisher hingegen nur in Papierform möglich. Beim Ansammeln von Quittungen können Papierbelege jedoch für immer verloren gehen, und Mitarbeiter bleiben deswegen auf Kosten sitzen.

### Zettelwirtschaft kostet Nerven und Zeit

Zurück im Büro muss sich einer von vier Befragten (26 %) relativ lange mit der Reisekostenabrechnung beschäftigen. Dabei werden Abrechnungen nicht selten beanstandet, sodass Informationen nachgereicht werden müssen. Danach beginnt oftmals das Warten: Zwar gibt bereits ein Drittel (33 %) der Befragten an, dass die Rückerstattung der Kosten seit der Prozessoptimierung kürzer als eine Woche dauert, 28 Prozent der Mitarbeitenden warten dafür aber noch zwei bis vier Wochen auf ihr Geld.

Der Prozess zur Genehmigung und Abrechnung von Geschäftsreisen wird im Vergleich zu 2021 deutlich positiver wahrgenommen. Während sich im vergangenen Jahr noch einer von fünf Mitarbeitenden (21 %) davon im Arbeitsalltag ausgebremst fühlte, sind es 2022 noch 10 Prozent.

***www.concur.de***

### REISEKOSTENABRECHNUNG

**33 %**
der Mitarbeitenden im Mittelstand müssen Belege in Papierform einreichen

**17 %**
der Mitarbeitenden im Mittelstand verlieren Belege regelmäßig unterwegs und bleiben auf Kosten sitzen

**28 %**
der Mitarbeitenden im Mittelstand warten zwei bis vier Wochen auf die Rückerstattung der Kosten

NetApp

# SAP in der Cloud

Flexibel, einfach, sicher, ressourcenschonend und skalierbar mit Amazon FSx for NetApp ONTAP

Amazon FSx for NetApp ONTAP ist ein zertifizierter Managed Service von AWS für SAP HANA – Datenmanagement der Enterprise-Klasse mit garantierter Performance und Datensicherheit inklusive

SAP on AWS mit NetApp
**netapp.com/de/sap-solutions**

# CARVE-OUT, S/4-MIGRATION UND WECHSEL IN DIE CLOUD

## KOMPLEXE HERAUSFORDERUNGEN IN EINEM SCHRITT MEISTERN

Die BSW-Gruppe ist das größte integrierte Forstunternehmen im Vereinigten Königreich und fertigt und verkauft eine breite Palette von qualitativ hochwertigen, FSC-zertifizierten Schnittholzprodukten an verschiedene Branchen.

Nach dem Verkauf des Geschäftsbereichs Building and Supply Solutions von SCA Wood UK mussten die ausgegliederten Einheiten aus dem globalen SAP ECC-System von SCA in ein neues, dediziertes SAP-System für BSW in der Azure Cloud verlagert werden.

### Die Herausforderung

Aufgrund der engen Zeitvorgaben im Zusammenhang mit dem Transitional Service Agreement (TSA) bestand die ursprüngliche Anforderung darin, für BSW einen 1:1-Carve-out von ECC nach ECC durchzuführen, gefolgt von einem späteren Projekt zur Durchführung eines Brownfield-Upgrade auf S/4HANA nach der Ausgliederung.

In der Anfangsphase des Projekts äußerte BSW Bedenken, dass es bei dem Carve-out und dem Brownfield-Projekt zu zahlreichen Betriebsunterbrechungen kommen könnte. Infolgedessen und auf Empfehlung von SNP wurde das Projekt zu einem Bluefield-Projekt mit Carve-out nach S/4HANA, bei dem der Carve-out, die Migration nach S/4HANA und der Wechsel in die Cloud in einem einzigen Projekt mit einer Reihe von Tests und einem einzigen Go-live kombiniert wurden.

> ANGESICHTS DER KOMPLEXEN HERAUSFORDERUNG EINES CARVE-OUT VON SAP-DATEN, EINER PROJEKT-INTEGRATION UND S/4HANA-TRANSFORMATION HABEN WIR CENTIQ UND SNP DAMIT BEAUFTRAGT, DIESES PROJEKT MIT MINIMALEN GESCHÄFTSUNTERBRECHUNGEN UND AUSFALLZEITEN UMZUSETZEN.
>
> David Robinson, Head of IT, BSW Group

### Die Lösung

SNP wurde mit der Durchführung des Carve-out und der Migration beauftragt, und war für die Planung und den Aufbau der Infrastruktur sowie die Projektbasisaktivitäten verantwortlich. Das Projekt wurde in Zusammenarbeit mit dem Partner Centiq durchgeführt. Das Team von Centiq erfüllte alle erforderlichen Netzwerk- und Infrastrukturanforderungen für Azure. Centiq leistete während des gesamten Projekts wichti-

ge Unterstützung, um sicherzustellen, dass der Wechsel innerhalb der vorgegebenen Ausfallzeit erfolgen konnte. Der SNP-Ansatz für die Projektdurchführung umfasste zwei Testzyklen und eine Generalprobe vor dem Cutover. Der Cutover wurde in etwa zwei Tagen erfolgreich durchgeführt und umfasste den Carve-out der für BSW relevanten Daten, die Migration nach S/4HANA und den Wechsel in die Azure Cloud. All dies wurde in nur sechs Monaten realisiert, und das Projekt konnte am 31. Dezember 2021 live gehen.

**Bluefield-Ansatz**

Der Bluefield-Ansatz von SNP minimierte die Ausfallzeiten und Kosten für BSW erheblich, da kein separates, späteres Projekt zur Durchführung eines Brownfield-Upgrade auf S/4HANA mehr erforderlich war. Der automatisierte Ansatz und die Software von SNP verkürzten die Projektdauer um mehrere Monate und ermöglichten es, das Projekt früher als geplant abzuschließen.

***Michelle Janz***

## VORTEILE

- Ein einziges Projekt für den Carve-out der relevanten Daten und den Wechsel nach S/4HANA on Azure.
- Automatisierte Systemanalysen, die eine einfache Bewertung der Systemlandschaft, der relevanten Organisationseinheiten und der Vorgehensweise bei der Migration ermöglichten.
- Der bewährte SNP-Ansatz von ECC nach S/4HANA ermöglichte es, das Projekt rechtzeitig vor Ablaufen des TSA abzuschließen und die gewünschte Ausfallzeit des Unternehmens einzuhalten.

Michelle Janz,
SNP U.K. Marketing,
www.snpgroupcom

Treffen Sie die SNP-Experten auf dem **DSAG-Jahreskongress** Stand N4

# SAP S/4HANA TRIFFT ECM

## WAS SIE FÜR EINE ERFOLGREICHE MIGRATIONSSTRATEGIE BEACHTEN SOLLTEN


Um am Markt erfolgreich zu bleiben, müssen Unternehmen immer schneller reagieren: Wie ist der Absatz in Nordamerika? Wie sieht die Produktion in Asien aus? Digitalisierung stellt viele Unternehmen vor große Herausforderungen. Daten, Kennzahlen und Prozesse müssen in Echtzeit analysiert werden, um eine fundierte Basis für zukünftige Entscheidungen bereitstellen zu können.

Zwei der wegweisenden Lösungen für Unternehmen sind zweifelsohne SAP HANA und SAP S/4HANA. Fest steht: An einem Umstieg kommen nur die Wenigsten vorbei. Dafür ist der Entwicklungsschritt, den SAP mit der neuen Produktgeneration gemacht hat, einfach zu groß. Wir bieten Ihnen für diese Problemstellung in diesem Whitepaper verschiedene Lösungsmöglichkeiten an. Anhand von sechs Thesen zum Thema beleuchten wir die wichtigsten Aspekte und geben Tipps für eine erfolgreiche Digitalisierungsstrategie.

**WHITEPAPER DOWNLOAD**

Das Whitepaper umfasst 12 Seiten und steht zum kostenlosen Download bereit: ***www.it-daily.net/download***

---


**WHITEPAPER DOWNLOAD**

Das Whitepaper umfasst 13 Seiten und steht zum kostenlosen Download bereit: ***www.it-daily.net/download***

# DATENSPEICHER NEU GEDACHT

## LEITFADEN FÜR EINE ERFOLGREICHE IT-TRANSFORMATION

In den letzten zehn Jahren hat das rasante Tempo mit dem sich die IT-Technologie weiterentwickelt, die zugrunde liegende Datenspeicherinfrastruktur enorm unter Druck gesetzt. Um mit den gestiegenen Anforderungen Schritt zu halten, hat Software-Defined Storage kontinuierlich bewiesen, die optimale Grundlage für jede Speicherinfrastruktur zu sein.

Dank ihrer extremen Flexibilität und nie dagewesenen Agilität erobern sich softwaredefinierte Technologien stetig neue Bereiche. Durch die Abstrahierung der Speicherdienste von der Speicherhardware gewinnen IT-Abteilungen beispiellose Kontrolle über die Speicherung, den Schutz und den Abruf von Daten.

# PRAXISERFAHRUNGEN

## HÜRDENLOS INS SAP-PERSONALAKTENPROJEKT

Nur selten sind es technische Hürden, die den Weg zum erfolgreichen Digitalprojekt versperren. Torsten Unger, Teamleiter SAP-Personalmanagement der DVV, verrät im Interview mit dem Sales-Experten Moritz Basler der EASY SOFTWARE AG, welche methodischen Kniffe über den Projekterfolg entscheiden.

? **Moritz Basler:** *Herr Unger, die Duisburger Versorgungs- und Verkehrsgesellschaft (DVV) hat ihr Personalaktenmanagement erfolgreich mit einer SAP-integrierten Lösung digitalisiert. Welche Tipps können Sie anderen Unternehmen mitgeben, um Stolpersteine schon auf dem Weg zum Startblock beiseitezuräumen?*

**Torsten Unger:** Als erstes sollten wir uns immer fragen: Wie arbeitet unser Personalwesen heute? Wo liegen die Stärken und Schwächen unserer Arbeitsweise? Außerdem: Was sind aktuelle Trends oder Best-Practices der Vorreiter im Markt? Mit einem Blick nach außen können wir besser einschätzen, was möglich ist und wo wir selbst stehen.

? **Moritz Basler:** *Haben Sie ein Beispiel für ein Problem, das Sie auf diese Weise bewältigt haben?*

**Torsten Unger:** Jede nicht-digitalisierte Personalabteilung kennt das Problem der Schattenakten: Teams reichen Personalakten von Schreibtisch zu Schreibtisch. Und damit alle parallel arbeiten können, fertigen sie Kopien der einzelnen Akten an. Das allein ist eine datenschutztechnische Zeitbombe. Wenn man dann auch noch über mehrere Standorte verteilt arbeitet, wird es schnell unmöglich zu sagen, welche Kopien veraltete Informationen enthalten.

Das tatsächliche Ausmaß der Komplexität haben wir erst erkannt, als wir uns kritisch hinterfragt haben. Mit unserem digitalen Personalakten-Management in SAP arbeiten nun alle Mitarbeitenden stets im Originaldokument. Denn alle haben von ihrem Gerät aus ortsunabhängig darauf Zugriff – sogar zeitgleich.

? **Moritz Basler:** *Beim Konzipieren digitaler Prozesse hängen Kunden häufig an ihrer bisherigen Arbeitsweise – also den Prozessen, die ihre Teams seit Jahren gewohnt sind. Wie sah das bei der DVV aus?*

**Torsten Unger:** Hätten wir auf unsere bisherigen Prozessabläufe gepocht, hätte das viel individuelle Anpassungsarbeit in der Software bedeutet.

Was wir zum Glück früh gemerkt haben, ist: Ein Dokument, das auf einem Monitor angezeigt wird, ist noch kein digitaler Prozess. Denn ein verstaubter manueller Prozess wird, ohne ihn neuzudenken, einfach nur zu einem verstaubten digitalen Prozess.

Best-Practices für automatisierte, digitale Prozesse, die sich auch im SAP-Bereich etabliert haben, existieren nicht ohne Grund. Sind unsere eigenen Prozesse wirklich so besonders, dass wir aufwendige Anpassungen brauchen? Es braucht Mut zur Veränderung!

? **Moritz Basler:** *Gibt es bestimmte Herausforderungen und Potenziale bei der Planung eines Digitalisierungsprojekts, die Personalabteilungen besonders im Blick haben sollten?*

**Torsten Unger:** Grundsätzlich sollte jede Abteilung beim Planen ihres Digitalisierungsprojekts die gesamte Unternehmensstrategie berücksichtigen. Wenn wir wissen, wie unsere Anliegen zu den übergreifenden Zielen und Leitbildern passen, wird es deutlich einfacher, Unterstützung für unser Projekt zu bekommen.

DIGITALISIERUNG HEISST NICHT EINEN MANUELLEN PROZESS DIGITAL ABZUBILDEN. DIGITALISIERUNG BEDEUTET PROZESSE NEU ZU DENKEN.

Moritz Basler,
Sales-Experte, EASY SOTWARE AG,
www.easy-software.com

Darüber hinaus sind Personalprozesse naturgemäß ein persönlicheres Thema als zum Beispiel Rechnungen. Mit einer hochwertigen Lösung, die nahtlos in SAP integriert ist und perspektivisch sogar Self-Services für Mitarbeitende ermöglicht, signalisieren Sie: Wir legen hohen Wert auf den Schutz der persönlichen Daten unserer Mitarbeitenden – und darauf, die Prozesse so effizient und komfortabel wie möglich zu gestalten. Klar strukturierte, moderne Personalprozesse kommunizieren eine positive Botschaft, die die Wahrnehmung des Unternehmens nach innen beeinflusst.

! **Moritz Basler:** *Herr Unger, wir danken für dieses Gespräch.*

Besuchen Sie EASY SOFTWARE auf dem **DSAG-Kongress** in **Halle 2, Stand H2** und während des Vortrages von Torsten Unger und Moritz Basler am 12.10.22 um 18:45 Uhr.

# CLOUD-MIGRATION

## SO ZIEHT IHR UNTERNEHMEN SCHNELL UND UNKOMPLIZIERT AUF SAP S/4HANA UM

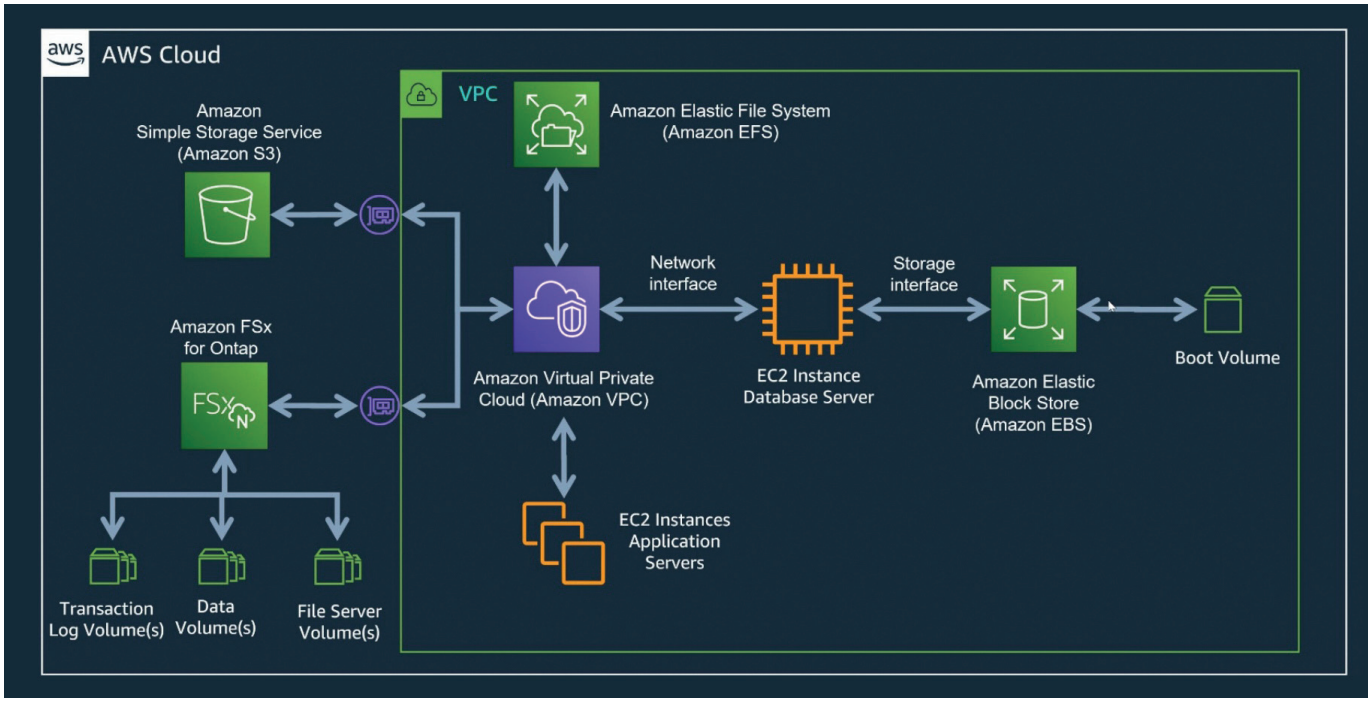
SAP zieht in die Cloud. Da 2027 der Support für SAP ECC 6.0 endet, ist die notwendige Migration auf SAP S/4HANA auch im Mittelstand ein drängendes Thema. Der Umstieg auf das neue System bedeutet für viele Kunden, von On-Premises-Lösungen zu Cloud-Infrastrukturen wie AWS umzusteigen sowie neue Prozesse und Betriebsmodelle aufzusetzen. Die exklusive Managed Service-Kollaboration Amazon FSx für NetApp ONTAP ermöglicht dabei einen einfachen Umzug von On-Premises auf AWS und einen schnellen, sicheren sowie datenschutzkonformen Betrieb von SAP HANA-Landschaften.

„Never change a running system!" – diese Grundhaltung besitzt für viele IT-Verwalter seinen Reiz, gerade wenn es um das Management von unternehmenskritischen On-Premises-Datenbanken geht. Mittelständischen Unternehmen ist jedoch bewusst, dass ein technischer Status Quo im internationalen Wettbewerb nicht ewig halten kann. Dafür bietet die Cloud zu viele Wettbewerbsvorteile gegenüber On-Premises. Besonders das nahende Supportende für den Klassiker SAP ECC 6.0 mahnt Unternehmen dazu, nicht zu lange mit der Migration auf Cloud-basierte oder hybride Nachfolger-Lösungen wie S/4HANA zu warten. Hohe EDA-Kosten und die zunehmende Spezialisierung von SAP-Fachkräften auf die Cloud mit der sinkenden Attraktivität von On-Premises sind weitere Gründe für einen zügigen Umstieg. So planen 73 Prozent aller SAP-Kunden weltweit den Umstieg auf S/4HANA.

Um geschäftskritische SAP-Workloads schnell und nahtlos ohne Refactoring und Umstrukturierung in die Cloud zu migrieren, braucht es eine Fully-Managed-Lösung. Nur so können die hohe Performance, Datensicherheit und Bedienbarkeit von On-Premises-Lösungen mit der Schnelligkeit, Skalierbarkeit und Einfachheit von Cloud-Infrastrukturen wie AWS verbunden werden.

### Fully Managed? Kein Problem!

Amazon FSx für NetApp ONTAP ist ein für SAP HANA zertifizierter Fully-Managed-Cloud-Service, der alle erforderlichen Funktionen und Leistungen für SAP-Deployments auf Anwendungsebene bereitstellt. Die gemeinsam von NetApp und Amazon entwickelte Lösung hat das Ziel, die Flexibilität und Skalierbarkeit von AWS zertifizierter Cloud-Infrastruktur mit den erweiterten Speicher- und Datenmanagement-Funktionen von NetApp ONTAP zu vereinen. FSx für ONTAP ermöglicht somit die Cloud-Migration von HANA zu AWS ohne Refactoring und Umstrukturierung. Zudem bietet der Service Cloud-basierte Backups und Disaster Recovery, Thin Pro-



DIE KOLLABORATION VON NETAPP, SAP UND AMAZON VERBINDET ERFOLGREICH DIE EINFACHE, SICHERE VERWALTUNG VON ON-PREMISES-LÖSUNGEN MIT DER SKALIERBARKEIT UND SCHNELLIGKEIT DER CLOUD.

Thomas Herrmann, Manager Business Development SAP, NetApp, www.netapp.com

visioning und nahezu sofortiges Klonen von SAP-Datenbanken sowie schnellere Entwicklungs- und Testzyklen. Das NetApp SnapCenter stellt zahlreiche Datenschutz-, Backup-, und Sicherheitsmaßnahmen zur Verfügung. Die Managementplattform erlaubt Snapshot-basierte Datenschutzfunktionen zentral zu administrieren. Zu diesem Zweck werden Aufgaben wie Backup-, Wiederherstellungs- und Klon-Lifecycle-Management an den Anwendungseigentümer übertragen. Möglichkeiten zur Überwachung auf den Storage-Systemen bleiben dabei unbeeinträchtigt. Das macht den Service auch für Betriebe attraktiv, die strikte Compliance-Vorgaben zu erfüllen haben.

Der Umstieg in die Cloud erfolgt dabei in drei simplen Schritten. Als erstes wird ein AWS-Account benötigt. Nach der Erstellung eines Accounts können im zweiten Schritt File-Systeme in Amazon FSx für NetApp ONTAP erstellt und gemanagt werden. Zu diesem Zweck gibt es einen simplen Wizard. Im dritten Schritt verbindet das Unternehmen den Datenspeicher mit den verschiedenen Anwendungsservern und Endbenutzer-Computer-Instanzen. Nach der Migration kann das Unternehmen schnell und sicher File Sharing über die gesamte Infrastruktur hinweg betreiben. Die Verbindung von intuitivem AWS File System und erweiterten ONTAP Datenmanagement-Funktionen macht es möglich.

## Bessere Performance heißt kürzere Projektlaufzeiten

In Hinsicht auf Performance erfüllt Amazon FSx für NetApp ONTAP die strikten Latenz-Anforderungen, die von SAP für SAP HANA Workloads veranschlagt werden. Zudem lässt sich die benötigte Durchsatzleistung von Workloads für das jeweilige File System frei skalieren und jederzeit ändern.

Eine SAP HANA-Umgebung, die auf dem zertifizierten FSx für NetApp ONTAP läuft, verkürzt zum Beispiel in der Applikationsentwicklung die Zeit bis zum Go-to-Market um bis zu 40 Prozent. Weitere Vorteile sind:

- Reduzierte PoC-/Auslieferungsrisiken
- Verbesserte Testzyklen durch schnell bereitgestellte Datensätze (Klone)
- Innovationen in F&E und Lieferketten unter Verwendung digitaler Zwillinge
- Automatisiertes Backup, Restore und Klonen von SAP HANA Datenbanken mit der NetApp SnapCenter Software
- Eine 99,99 Prozent garantierte Uptime und Verfügbarkeit

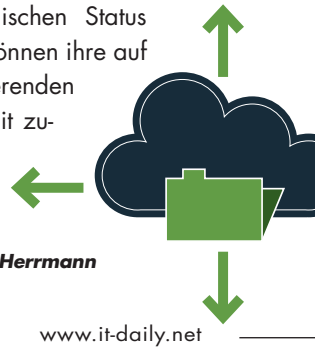
## Will ich meine Daten wirklich in der Cloud haben?

Daten sind das wertvollste Gut jedes Unternehmens. Deshalb ist es von größter Bedeutung, diese vor Angriffen und Verlust zu schützen. Mit fortschrittlichen Schutzfunktionen sichert die Fully-Managed-Lösung Daten vor Ransomware und anderen externen Bedrohungen ab. Disaster Recovery ist ebenfalls ein Bereich, der immer mehr an Bedeutung gewinnt, vor allem, wenn es darum geht, geschäftskritische Anwendungen wie SAP HANA in der Cloud auszuführen. FSx für NetApp ONTAP verbessert die Datenaufbewahrung und Disaster Recovery mit automatischen täglichen Backups und Replikationen zwischen den lokalen Dateiservern und AWS. Der Service ermöglicht es außerdem, Daten schnell und effizient über Standorte hinweg zu verschieben, wenn Sekundärkopien zum Schutz vor Standortausfällen erstellt werden müssen. Als weitere Sicherheitsmaßnahme erlaubt NetApp FPolicy ein intuitives Audit von Dateizugriffen der Endbenutzer, während Vscan einen effizienten Virenschutz bietet. Durch die hohe Verfügbarkeit und Sicherheit macht Amazon FSx für NetApp ONTAP die Cloud auch für diejenigen Betriebe attraktiv, die bisher wegen strenger Compliance-Vorgaben den Umstieg hinausgezögert haben.

## Fazit

Mit dem nahenden Support-Ende für SAP ECC 6.0 und dem allmählich beginnenden Roll-Out von SAP S4/HANA wird die Cloud-Transformation in mittelständischen Unternehmen enorm beschleunigt. Die exklusive Fully-Managed-Lösung Amazon FSx für NetApp ONTAP erleichtert dabei den Umstieg und ermöglicht es, die Funktionen der Cloud-Infrastruktur voll auszunutzen. Zudem machen die erweiterten Datenschutz- und Backup-Funktionen diese Kombination auch für Betriebe interessant, die in der Vergangenheit gezögert haben, ihre Daten bei amerikanischen Cloud-Anbietern zu speichern. Die Kollaboration von NetApp, SAP und Amazon verbindet erfolgreich die einfache, sichere Verwaltung von On-Premises-Lösungen mit der Skalierbarkeit und Schnelligkeit der Cloud. Daraus ergibt sich der zusätzliche Effekt, dass Unternehmen Zeit, Kosten und Ressourcen sparen. Unternehmen, die den technischen Status Quo durchbrechen, können ihre auf SAP S/4HANA basierenden Systeme in AWS somit zukunftsfest gestalten und im Wettbewerb mithalten.

***Thomas Herrmann***



# HERAUSFORDERUNG TRANSFORMATION

## 49 PROZENT DER UNTERNEHMEN ERREICHEN IHRE TRANSFORMATIONSZIELE NICHT VOLLSTÄNDIG

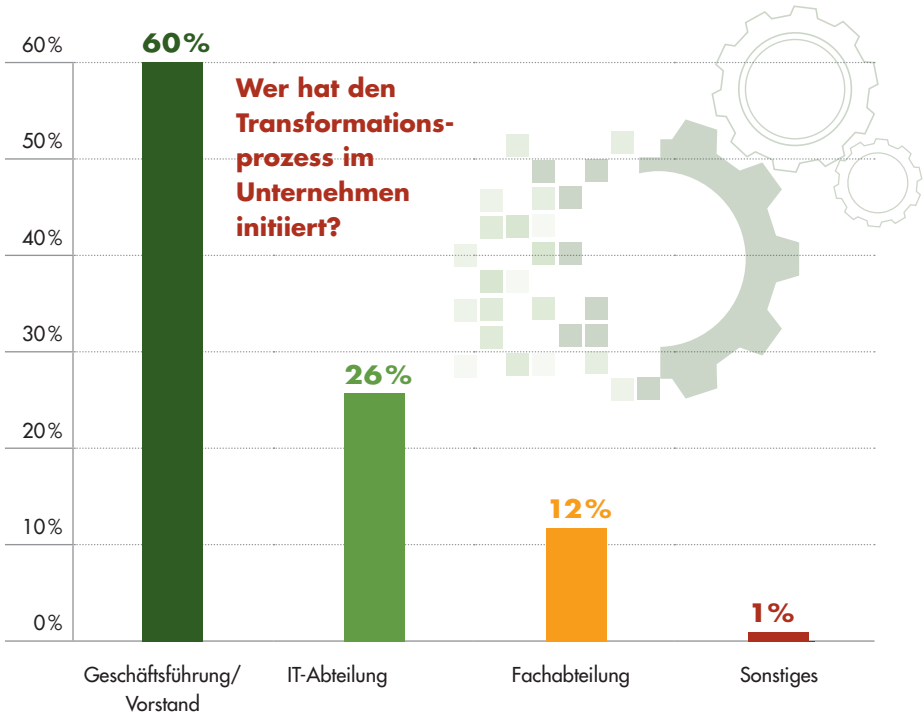
Erfolgreiche Unternehmen entwickeln sich dynamisch. Wichtige Voraussetzung: Ihre IT-Kernsysteme müssen schnell anpassbar sein. Dazu müssen Daten und Prozesse jederzeit auf modernsten Plattformen nutzbar sein. Natuvion hat in einer Studie untersucht, wie Unternehmen die dafür nötigen Transformationen planen und durchlaufen. Zwei Key-Learnings: Fast die Hälfte erreicht ihre angestrebten Transformationsziele nicht vollständig und digitale Umzüge erfordern Spezialisten mit viel Know-how und Erfahrung. Transformationsprojekte sind vor allem dann eine Challenge, wenn sie nicht gründlich geplant und umgesetzt werden. Doch leider existiert keine Blaupause, denn kein digitaler Umzug ist wie der andere.

### Digitaler Umzug nach Schema F?

Für digitale Umzüge oder Transformationen existieren zwei Grundprinzipien, an denen sich Unternehmen orientieren können. Diese Migrationskonzepte beschreiben, ob ein bestehendes Kernsystem mit allen existierenden Prozessen und Daten auf eine neue Plattform transformiert wird, oder ob bei der Transformation alle Prozesse und die Datenstruktur von Grund auf neu definiert werden. Diese beiden Varianten werden als Brownfield- (alles mitnehmen) oder Greenfield (alles neu)-Prinzipien bezeichnet. Soweit zur Theorie. In der Praxis haben die meisten Unternehmen teils erprobte Prozesse und Datensätze, die übernommen oder optimiert werden sollten. Kurz gesagt, Schema F ist bei einer digitalen Transformation keine realistische Option. Vielmehr ist eine Mischform aus „alles neu" und „alles mitnehmen" für viele Unternehmen der optimale Weg. Die Selective Data Transition (SDT) ist die individuelle Kombination aus Brownfield und Greenfield. Das bestehende System wird als funktionale Hülle beispielsweise auf SAP S/4HANA übertragen. Anschließend werden die benötigten Daten migriert sowie Altdaten archiviert oder gelöscht. SDT ist eine ideale Möglichkeit, etablierte Prozesse und Daten auf Aktualität und Qualität zu überprüfen und bei Bedarf mit Best Practices aufzufrischen. In der Natuvion Transformationsstudie 2022, die kostenlos zum Download zur Verfügung steht, gaben rund 50 Prozent der befragten mittelständischen und großen Unternehmen an, eine Selective Data Transition bei ihrer Transformation genutzt zu haben und nur vereinzelt dem eindimensionalen Pfad von Greenfield und Brownfield gefolgt zu sein.

### Herausforderungen, Wunsch und Wirklichkeit

Die Erwartungshaltung von Unternehmen an eine digitale Transformation ist hoch. Im Rahmen der Studie gab die Mehrheit (67 Prozent) der Befragten als Gründe für die Transformation neben einer strategischen Ausrichtung auch organisatorische Anpassungen, bessere und schnellere Geschäftsentscheidungen, die Kostensenkung oder die Einführung innovativer Geschäftsmodelle an. Das ist wenig überraschend, da – laut der Natuvion Studie – Digitalisierungsinitiativen mehrheitlich (60 Prozent) von der Geschäftsführung oder den Vorständen angeregt wurden.



Auch die Erwartungen an diese Projekte sind hoch. An erster Stelle stehen die Qualitätssteigerung und hohe Prozesssicherheit (knapp 65 Prozent), gefolgt vom Wunsch nach besserer Zukunftsfähigkeit (58 Prozent) und dem Senken der Kosten (48 Prozent).

Nun möchte man meinen, dass die Investitionen in einen digitalen Umzug meist von Erfolg gekrönt sind. Laut Studie sagen jedoch etwas über 49 Prozent der Unternehmen, dass sie die Ziele durch die Transformation nur teilweise oder nicht erreicht haben. Show-Stopper sind insbesondere die Ressourcenplanung sowie das fehlende Fachwissen und die entsprechende Projekterfahrung. Erschwerend kommen die Komplexität im Projektverlauf, die Einhaltung zeitlicher Vorgaben, der hohe Abstimmungsaufwand oder Probleme bei der Analyse der bestehenden IT- und Datenlandschaft hinzu.

## Mit Übersicht, Planung und Knowhow zum Erfolg

Die gute Nachricht: Gut 50 Prozent der Befragten berichten, dass sie ihre Ziele durch die Transformation vollständig erreicht haben. Das Erfolgsrezept beruht auf Erfahrung und Wissen sowie zu einem entscheidenden Teil auch aus einer guten Vorbereitung und Analyse.

Durch einen hohen Grad an Expertise können Fehler, die oftmals schon bei der Planung beginnen und sich dann durch das gesamte Projekt ziehen, vermieden werden. Das nötige Knowhow kann prinzipiell intern aufgebaut werden. Allerdings ist es mit spezialisierten externen Experten leichter und schneller zu realisieren – insbesondere da der Markt an hochqualifizierten Fachkräften leergefegt ist. Laut der Studie von Natuvion wollen über 32 Prozent der Unternehmen, zukünftig früher externe Berater hinzuziehen.

Unternehmen, die ihre Transformationen erfolgreich durchführen, durchlaufen die Vorbereitung und Analyse meist akribisch. Fast 31 Prozent der Studienteilnehmer nannten die Analyse der bestehenden IT-Landschaft als eine besondere Herausforderung in der Planung. Es ist daher kein Zufall, dass knapp 70 Prozent der Befragten die Analyse als eine der wichtigsten Maßnahmen bezeichnen. Bei der Bestandsaufnahme können geeignete Analyse-Tools wie Natuvion SOPHIA, welche die Standardanalysen von ERP-Lösungen wie von SAP weitreichend ergänzen, entscheidend helfen.

## Zeit und Verfügbarkeit sind kritische Faktoren

Digitale Transformationen der Kernsysteme, wie beispielsweise auf SAP S/4HANA, ermöglichen neue Perspektiven und Sicherheiten, die Unternehmen im zunehmend schnellen und digitalen Business benötigen. Allerdings darf der digitale Umzug den laufenden Betrieb nicht stören. Das Zeitfenster für die Migration wird immer kleiner und die Akzeptanz für Downtimes gehen gegen Null. Dies betrifft etwa international agierende Unternehmen, deren Systeme 7x24 im Einsatz sind oder Systeme in kritischen Infrastrukturen, wie bei Energieversorgern oder Krankenhäusern und Kliniken.

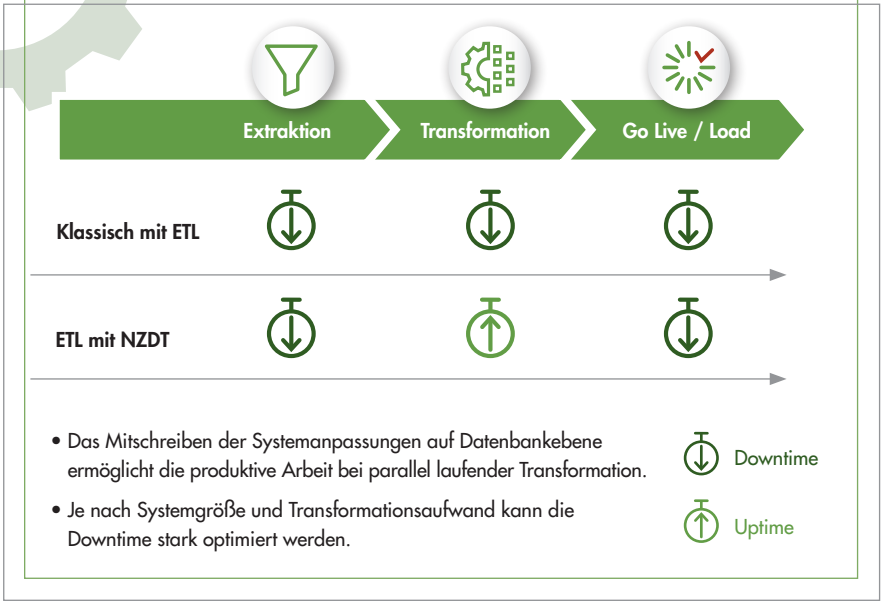
Laut der Studie von Natuvion gaben 16 Prozent der befragten Unternehmen an, derart kritische Systeme zu betreiben, dass bei einer Migration keinerlei Betriebsunterbrechung stattfinden darf. 62 Prozent gestehen einer potenziellen Betriebsunterbrechung nicht mehr als wenige Stunden, einen Arbeitstag oder ein Wochenende zu. Auch hier ist die Lösung das Migrationsprinzip der Selective Data Transition (STD) im Verbund mit der Near Zero Downtime (NZDT)-Methodik. Mit der Kombination aus SDT, NZDT und dem Transformations-Tool Natuvion Data Conversion Server (DCS) gelingt es, ein Transformationsprojekt in Wellen umzusetzen, so dass die Anzahl und Länge von Betriebsunterbrechungen gegen Null geht.

## Keine Transformation ist wie die andere

Digitale Transformationen oder Umzüge sind individuell an das Unternehmen angepasste Projekte. Mit guter Planung, hervorragender Expertise, einem realistischen Timing sowie mit dem richtigen Spezialisten ist eine gewinnbringende Investition sichergestellt. Dies bestätigt Sibylle Diederich, E.ON Program Manager: „Mit dem Know-how und der Spezialsoftware von Natuvion waren wir in der Lage, extrem große ERP- und CRM-Systeme zu transformieren – mit minimalen Auswirkungen auf das Geschäft bei sehr hoher Qualität.

***Philipp von der Brüggen***
***www.natuvion.com***

**Einer der Kostentreiber bei Datenmigrationen: Die Downtime**



# DMS, ECM UND EIM

## INNOVATIONEN IM ECM-UMFELD

Akronyme haben Konjunktur in der IT. DMS, ECM und EIM sind ein gutes Beispiel dafür. Viele Unternehmen verwenden die Begrifflichkeiten Dokumentenmanagement-System (DMS), Enterprise-Content-Management-System (ECM) und Enterprise-Information-Management-System (EIM) häufig als Synonyme.

Die Systemintegration ist eines der zentralen Themen bei der Einführung neuer Software. So unterschiedlich die verschiedenen DMS-Anwendungen und Einsatzfelder auch sind: Es gibt kein Projekt, in dem nicht die Anforderung zur Integration der DMS-Anwendung in andere Anwendungssoftware besteht. Warum also das Rad neu erfinden und nicht auf ein Vorgehensmodell setzen?

Silos aufbrechen, 360 Grad Sicht auf alle Dokumente, verbesserte Workflows, Wiederverwendung von Informationen, Beseitigung von Redundanz, Zugriffsrechte steuern, keine Datenverluste und compliant: Das sind die Highlights von Content-Management-Lösungen der nächsten Generation.


**Das eBook umfasst 35 Seiten und steht kostenlos zum Download bereit.**
**www.it-daily.net/download**

---


**Das eBook umfasst 46 Seiten und steht zum kostenlosen Download bereit.**
**www.it-daily.net/download**

# STORAGE

## WHAT`S NEW?

Daten entwickeln sich in der modernen digitalen Wirtschaft zur wichtigsten Währung. Gleichzeitig steigen Kosten, Komplexität und Bedrohungen für die Datensicherung. Ein effizienter Schutz der Daten tut Not, unabhängig davon soll der Nutz- und Mehrwert dieser „Assets" als Active Archive voll ausgeschöpft werden.

Das Backup hat sich zu einer existentiellen Anforderung für Unternehmen in der digitalen Transformation und angesichts der bekannten Cyber-Bedrohungen entwickelt. Doch wie sieht die Zukunft des Backups aus? Diese und weitere Fragen werden im eBook „Storage: What`s new?" beantwortet.

### Weitere Artikel aus dem eBook

- Storage-Strategie: Der richtige Mix macht`s
- PPR: Prevention, Protection & Recovery
- Zukunftssichere Speicherinfrastrukturen
- Always on: Unveränderbare Snapshots

Das E-3 Magazin

Information und Bildungsarbeit von und für die SAP-Community

# Wir leben alle unter dem gleichen Himmel, aber wir haben nicht alle den gleichen Horizont.

*Konrad Adenauer*


© Yevhenii_Chulovskyi, Shutterstock.com



e-3.de | e3zine.com


# RISIKO DURCH DIGITALISIERUNGSSCHEU

## UNTERNEHMEN VERSPIELEN ZUKUNFTSCHANCEN UND WETTBEWERBSFÄHIGKEIT

Nach über zwei Jahren Pandemie, die zunächst einen Investitionsschub in Cloud, KI und Co. ausgelöst hat, treten Unternehmen im DACH-Markt jetzt wieder auf die Digitalisierungsbremse. Mit diesem Befund sorgt eine aktuelle repräsentative Studie des Branchenverbands Bitkom für Aufsehen: Demnach plant ein Drittel aller befragten deutschen Unternehmen, ihre Investitionen in die Digitalisierung im Vergleich zu den letzten fünf Jahren bereits 2023 deutlich zu reduzieren. Ähnlich ist die Situation in Österreich, wo laut nationalem Digitalisierungsindex lediglich knapp ein Viertel weiterhin in digitale Modernisierung investieren will.

Gründe für die Ablehnung von DACH-Unternehmen gegenüber neuen Digitalisierungsprojekten halten sich dennoch hartnäckig. Neben der aktuell unsicheren Weltlage, Störungen in den Lieferketten und steigender Inflation gibt es drei Gründe, die mir in meinem Alltag immer wieder begegnen. Welche das sind und warum Unternehmen gerade wegen dieser Argumente ihre Digitalisierung unbedingt vorantreiben sollten:

### Grund 1: Für komplexe Digitalisierungsprojekte fehlen uns die Ressourcen

Ein zentraler Ablehnungsgrund ist der Fachkräftemangel. Insbesondere mittelständische Unternehmen haben häufig nicht die notwendigen In-House-Kapazitäten, um neben dem Alltagsgeschäft auch noch größere Digitalisierungsprojekte stemmen zu können. Laut der IDG-Studie „IT-Modernisierung 2021" verfügen in Deutschland weniger als ein Drittel der Unternehmen über eine ausreichend große IT-Abteilung. In der eingangs genannten Bitkom-Befragung klagt sogar die Hälfte aller befragten Unternehmen über fehlende Experten. Der Mangel von internen Fachkräften und verfügbaren Kapazitäten führt letztlich dazu, dass ohnehin häufig schon überlastete IT-Abteilungen eher Digitalisierungsbremse als Digitalisierungskraft sind.

Dieser Umstand spricht allerdings keineswegs gegen die Digitalisierung an sich. Zwar ist die hauseigene IT zentraler Dreh- und Angelpunkt für Digitalisierungsinitiativen. Doch sie muss nicht die Kraft sein, die ein solches Projekt strategisch plant und im Alleingang umsetzt. Mit der Unterstützung von externem Lösungs- und Umsetzungs-Know-How kann ein schneller und vor allem spürbarer Nutzen geschaffen werden. Es ist wichtig und von Vorteil, sich extern innovative Ideen und Lösungsansätze aufzeigen zu lassen und vor allem den Blick aus der Vogelperspektive zuzulassen. Denn um den eigenen Wettbewerbsvorteil zu erhalten, müssen Unternehmen ihre Komfortzone verlassen. Tun sie das nicht, lassen sie große Chancen liegen und riskieren die eigene Wettbewerbsfähigkeit.

### Grund 2: Digitalisierung dauert viel zu lange

Eine schnelle Markteinführungszeit zählt zu den wichtigsten Kriterien von Unternehmenserfolgen. So hat beispielsweise eine McKinsey Studie aus dem Jahr 2018 gezeigt, dass Wettbewerber, die frühzeitig und schnell han-

deln, ihre Konkurrenten in kürzester Zeit hinter sich lassen. Die Studie stellt weiter fest, dass die schnellsten Digitalisierer ein Umsatzwachstum über drei Jahre verzeichnen, das fast doppelt so hoch ist wie das von Spät-Digitalisierern. Dieser Trend hat durch die letzten beiden Pandemie-Jahre nochmal an Fahrt aufgenommen.

Demgegenüber steht die Befürchtung von Unternehmen, ihre Markteinführungszeit, die sie bereits ohne zusätzliche Digitalisierung erreichen, zugunsten von Mammutprojekten wie dem Umbau der hauseigenen IT opfern zu müssen. Doch das muss nicht sein, im Gegenteil. Digitalisierungsprojekte können zügig vorangetrieben werden und ebenso schnell erste spürbare Erfolge einbringen, und zwar mithilfe von Minimum Viable Products (MVP). Diese Prototypen, zum Beispiel eines Produkts oder Services, sind ausschließlich mit grundlegenden Funktionen oder Features ausgestattet. Während sie bereits genutzt werden können, durchlaufen sie weitere Entwicklungsphasen und erhalten nach und nach weitere Funktionen. Durch MVPs und mithilfe einer strategischen Roadmap können in Digitalisierungsprojekten Kleinstprozesse schrittweise implementiert werden. Die Vorteile:

- Unternehmen sind deutlich schneller am Markt,
- Innovationen werden gefördert,
- Wettbewerbsfähigkeit bleibt erhalten beziehungsweise wird gesteigert,
- Probleme werden frühzeitig erkannt und schnelle, kleinschrittige Lösungen können erarbeitet werden,
- Neue Produkte, Prozesse oder Lösungen können schnell getestet und flexibel angepasst werden,
- Nutzerdaten und -feedback kann kontinuierlich gesammelt und eingearbeitet werden.

## Grund 3: Die Digitalisierung schafft nur unnötige Sicherheitsrisiken

Ein weiteres häufiges Vorurteil ist, dass die Digitalisierung mehr Cybersicherheitsrisiken schafft, als sie löst. Die Bedenken sind nicht grundlos. Durch die voranschreitende Vernetzung bieten sich auch mehr potenzielle Einfallstore für Angriffe als bei analogen Prozessen. Was an dieser Stelle häufig vergessen wird, ist jedoch das enorme Risiko für Sicherheit und Unternehmenserfolg, das Altsysteme darstellen:

1. Veraltete Systeme sind deutlich anfälliger für Malware als moderne Systeme.
2. Der gesetzlich vorgegebene Datenschutz kann kaum gewährleistet werden.
3. Langsame IT behindert die Produktivität.
4. Moderne Software ist mit Altsystemen unter Umständen nicht mehr kompatibel.

Vor diesem Hintergrund ist es nicht verwunderlich, dass 21 Prozent von weltweit befragten 2.000 IT-Fachleuten dem Kaseya IT-Operations Report 2022 zufolge Altsysteme als Bremse von Innovation und Wachstum ansehen.

WER HEUTE DIE CHANCEN DER DIGITALISIERUNG LIEGEN LÄSST, RISKIERT SEINE WETTBEWERBSFÄHIGKEIT IN ZUKUNFT.

Marcel Kappestein, Geschäftsführer, Avenga Germany GmbH, www.avenga.com/de/

Nun hat man auf der einen Seite IT-Experten, die schon seit Jahren Alarm schlagen und auf die enormen Cybersicherheitsrisiken hinweisen. Auf der anderen Seite wägen sich jedoch der CyberDirekt-Studie „Risikolage 2022" zufolge fast 70 Prozent aller befragten mittelständischen Unternehmen selbst in Sicherheit vor einer Cyberattacke. Das zeigt deutlich, „dass das Thema trotz der hohen Gefahrenlage und Medienpräsenz noch nicht durchgängig in den Köpfen angekommen ist" , so Ole Sieverding, Geschäftsführer von CyberDirekt.

An diesem Punkt braucht es dringend ein Umdenken. Die Berufung auf die vermeintliche Sicherheit bestehender Systeme und die Verweigerung der Digitalisierung aufgrund von Cybersicherheitsbedenken begünstigt genau das, wovor Unternehmen sich eigentlich schützen wollen: erfolgreiche Cyberattacken, Datenschutzrisiken und mangelnde Wettbewerbsfähigkeit.

## Die Digitalisierung ist eine Frage des Mindsets

Die hier diskutierten Vorurteile gegenüber der Digitalisierung von Unternehmen müssen ernst genommen werden. Doch ohne Digitalisierung verspielen eben diese Unternehmen ihre Wettbewerbsfähigkeit. Deshalb gilt es umso mehr, die Chancen aufzuzeigen, die sich in innovativen Unternehmen eröffnen. Der Präsident des Branchenverbandes Bitkom Achim Berg bringt es auf den Punkt: „Digitalisierung ist die entscheidende Zukunftsfrage für die meisten Unternehmen und für die deutsche Wirtschaft insgesamt. Niemand sollte heute noch sagen, er habe keine Zeit für Digitalisierung." Wer sich heute Kooperationspartner sucht und innovative Wege geht, wird den Risiken der Zukunft vorbereitet entgegentreten. Letztlich sind Krisen oftmals auch ein Katalysator und so gilt derzeit noch stärker als sonst: Die Gewinner von morgen werden heute gemacht.

***Marcel Kappestein***

# METAVERSE

## SECHS TRENDS, DIE DIE TECHNOLOGIE VORANTREIBEN

Sechs Trends treiben den Einsatz von Metaverse-Technologien heute und in den nächsten drei bis fünf Jahren voran, so Gartner, Inc.

Gartner definiert ein Metaverse als „die nächste Stufe der Interaktion in der virtuellen und physischen Welt". Metaverse-Technologien ermöglichen es den Menschen, ihre physischen Aktivitäten zu replizieren oder zu verbessern, indem sie physische Aktivitäten in eine virtuelle Welt verlagern oder erweitern oder die physische Welt umgestalten.

Trotz des Hypes ist die Einführung von Metaverse-Technologien erst im Entstehen begriffen und fragmentiert. Gartner rät zur Vorsicht bei der Investition in ein bestimmtes Metaverse, da es noch zu früh ist, um festzustellen, welche Investitionen langfristig rentabel sein werden.

### 1. Spiele

Die Spieleindustrie, insbesondere Videospiele, ist seit vielen Jahren ein Innovator in Sachen Erfahrung und Technologie. Das Metaversum wird Spieltechnologien, Methoden, Entwicklungstools und sogar die Spieltheorie nutzen, um Erfahrungen sowohl für die Unterhaltung als auch für Trainingssimulationen zu schaffen. Unternehmen werden „Serious Games" einsetzen - Spieltechnologien, -erlebnisse und -erzählungen für die Schulung und Simulation bestimmter Arbeitsaufgaben und -funktionen. Gartner erwartet, dass der Markt aufgrund dessen um 25 Prozent wachsen wird.

### 2. Digitale Menschen

Digitale Menschen sind interaktive, KI-gesteuerte Repräsentationen, die einige der Eigenschaften, die Persönlichkeit, das Wissen und die Denkweise eines Menschen besitzen und in der Regel als digitale Zwillinge, digitale Avatare, humanoide Roboter oder dialogfähige Benutzeroberflächen dargestellt werden. Sie können Sprache, Gesten und Bilder interpretieren und ihre eigene Sprache, ihren Tonfall und ihre Körpersprache erzeugen.

### 3. Virtuelle Räume

Ein virtueller Raum - oder eine virtuelle Welt - ist eine computergenerierte Umgebung, in der Gruppen von Menschen mithilfe persönlicher Avatare oder Hologramme zusammenkommen können. Virtuelle Räume sprechen mehrere Sinne an und bieten den Teilnehmern die Möglichkeit, in den Raum einzutauchen und mit ihm zu interagieren.

### 4. Gemeinsame Erlebnisse

Ein gemeinsames Erlebnis bringt eine Gruppe von Menschen in einem virtuellen Raum zusammen. Das Metaversum wird gemeinsame Erlebnisse aus isolierten immersiven Anwendungen herausholen und mehr Möglichkeiten bieten, sich zu treffen, zusammenzuarbeiten, zu interagieren oder anderweitig Erfahrungen über Anwendungen, Verbraucherevents und Dienste hinweg zu teilen.

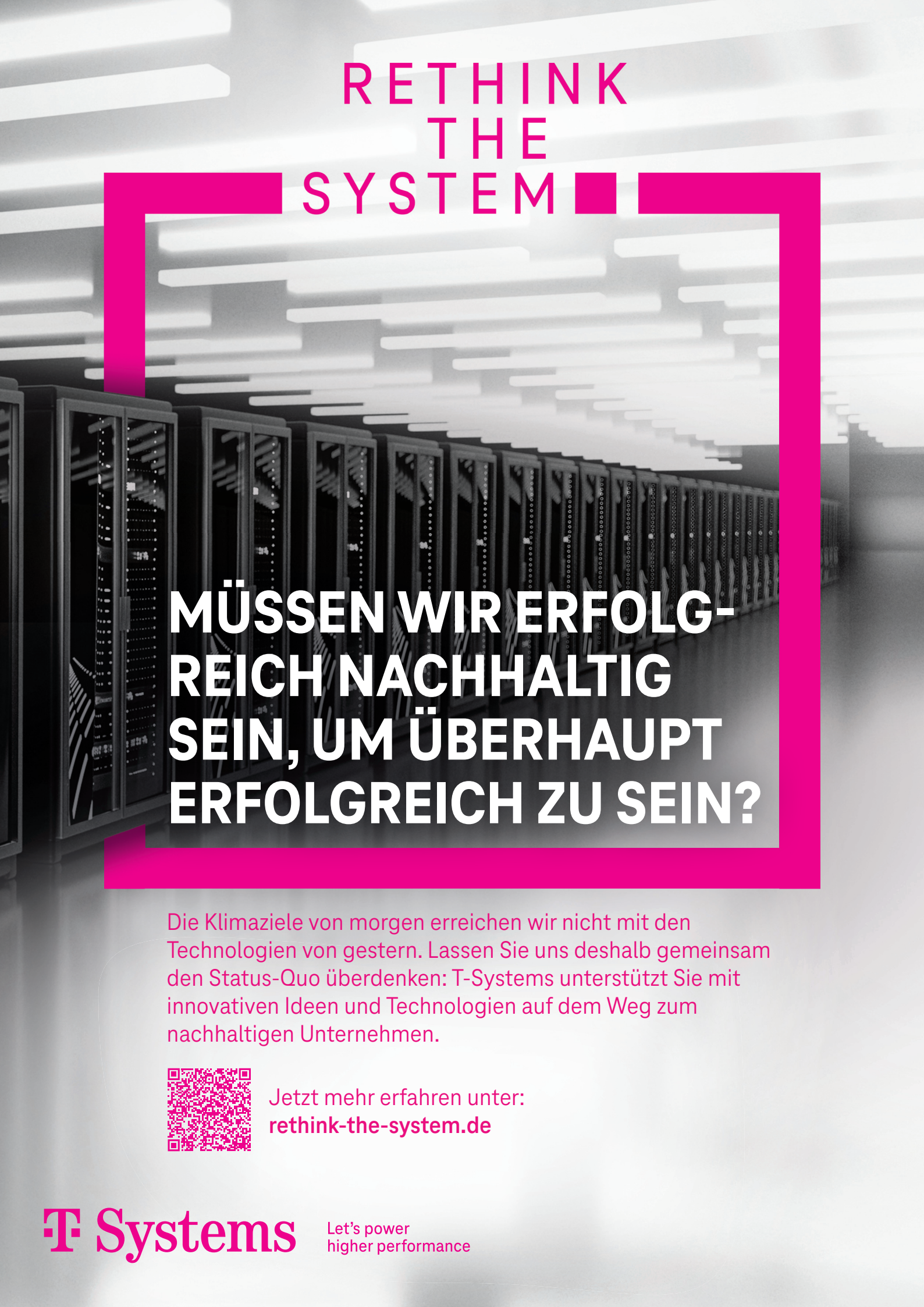
### 5. Tokenisierte Assets

Tokenisierte Assets bieten neue Geschäftsmodelle für Inhaltsersteller. In Metaverse-Erlebnissen werden die meisten tokenisierten Assets nicht-fungible Token-Technologien (NFTs) verwenden. NFTs unterstützen neue Wirtschaftsmodelle, bei denen die Urheber von Inhalten den Großteil der Einnahmen aus dem Verkauf ihrer Werke dauerhaft behalten. Die durch das Metaverse ermöglichten neuen Funktionen werden neue Wege eröffnen, um nicht nur virtuelle Produkte und Dienstleistungen zu monetarisieren, sondern auch physische Güter zu erwerben.

### 6. Räumliche Datenverarbeitung (Spatial Computing)

Spatial Computing kombiniert physische und digitale Objekte, um physische Räume digital aufzuwerten. Auf diese Weise können Unternehmen mehr aus ihren physischen und digitalen Ressourcen herausholen, indem sie verwandte „unsichtbare" digitale Informationen und Inhalte, die mit Menschen, Orten und Dingen verknüpft sind, sichtbar machen.

***www.gartner.com***


RETHINK
THE
SYSTEM
MÜSSEN WIR ERFOLG-
REICH NACHHALTIG
SEIN, UM ÜBERHAUPT
ERFOLGREICH ZU SEIN?
Die Klimaziele von morgen erreichen wir nicht mit den Technologien von gestern. Lassen Sie uns deshalb gemeinsam den Status-Quo überdenken: T-Systems unterstützt Sie mit innovativen Ideen und Technologien auf dem Weg zum nachhaltigen Unternehmen.
Jetzt mehr erfahren unter:
rethink-the-system.de
T Systems
Let's power
higher performance


# SCHNELLER, BESSER UND KOMFORTABLER

## CAWUM – DIE WSUS-ALTERNATIVE

Die Herausforderungen von Administratoren und IT-Managern nehmen zu – insbesondere im Zusammenhang mit neuen Risiken und Gefahren. Die mitunter starken Abhängigkeiten von den jeweils eingesetzten Betriebssystemen spielen hierbei eine wichtige Rolle. Denn in vielen Fällen sind die mitgelieferten Standard-Tools – die Windows Server Update Services (kurz: WSUS) – nicht die effizientesten. Aber es gibt eine Alternative: CAWUM von Aagon.

Innovationen in der Softwareentwicklung machen den Einsatz alternativer Lösungen möglich, die es Administratoren erlauben, Prozesse enorm zu vereinfachen und Kosten zu sparen. Denn bei der Auswahl und dem Einsatz einer Lösung sollten IT-Administratoren immer die drei Aspekte Sicherheit, Funktionalität und Wirtschaftlichkeit im Blick haben. Die Einführung einer speziellen Software für bestimmte, wiederkehrende Aufgaben etwa kann für einen Dominoeffekt sorgen, der die Performance von IT-Teams auf ein völlig neues Level hebt.

Die für Patches und Updates zuständige Softwarekomponente Windows Server Update Services (WSUS) von Microsoft ist ein Beispiel für einen solchen Fall. Im Folgenden finden Sie sieben Gründe, die dafür sprechen, WSUS mit einer fortschrittlichen Lösung abzulösen – und beim Windows-Updatemanagement in Zukunft auf das ACMP Complete Aagon Windows Update Management (CAWUM) zu bauen.

### Sieben Gründe für eine Ablösung von WSUS

#### 1. Punktgenaue und tagesaktuelle Update-Steuerung

Für eine reibungslose IT-Verwaltung ist es von zentraler Bedeutung immer tagesaktuell mit Patches auf Bedrohungen und Exploits reagieren zu können. Gewöhnliche und behelfsmäßige Lösungen sind in diesem Punkt von regelmäßig bereitgestellten Updatedateien von Microsoft abhängig.

Im Gegensatz dazu ist ACMP CAWUM zu jedem Zeitpunkt immer genau so aktuell wie der originale WSUS-Server. So sind IT-Administratoren in der Lage vollautomatisch und von ihnen gesteuert und kontrolliert zu reagieren. Bei der Verwaltung der Windows-Updates mit CAWUM lässt sich punktgenau steuern, welche File Repositories welche Patches in welchen Sprachen erhalten sollen. Außerdem wird nie die mehrere Gigabytes große Update-Datei heruntergeladen, sondern Clients erhalten allein diejenigen Patches, die sie jeweils tatsächlich benötigen. So wird wertvolle Bandbreite gespart und der zeitliche Installationsaufwand sinkt – ein enormer Gewinn für die Effizienz der IT.

#### 2. Mehr Effizienz und Übersichtlichkeit

Automatisierung unterstützt Admins dabei, IT-Prozesse im Unternehmen effizienter und übersichtlicher zu gestalten. Zudem kann sie zu mehr Übersichtlichkeit beitragen. Leider wird bei WSUS häufig manuelles Handeln vorausgesetzt. Darüber hinaus sind die Reporting-Fähigkeiten von WSUS limitiert.

CAWUM reagiert tagesaktuell auf die von Microsoft bereitgestellten Updates. Es funktioniert ganz automatisch – von Admins gesteuert und kontrolliert. So wird auch die Verwaltung von Lizenzgebühren und Serverlizenzen übersichtlicher und einfacher. Dank der umfassenden Reporting-Funktion von ACMP ist es außerdem möglich, lesbare Reports zu erzeugen – was auch bei Audits und Zertifizierungen notwendig wird.

### 3. Zeit und Ressourcen sparen

Grundsätzlich sollte das Windows-Updatemanagement Administratoren möglichst wenig Zeit kosten und Ressourcen einsparen. Obwohl WSUS für die Sicherheit von Unternehmens-PCs von Bedeutung ist, hat die Softwarekomponente schon seit mehreren Generationen keine Weiterentwicklung erfahren.

Mit der intuitiven Benutzeroberfläche von CAWUM geht die Verwaltung von Windows Updates schneller und sicherer als bei herkömmlichen Lösungen. Außerdem haben Administratoren Serverlizenzen und Lizenzgebühren immer im Blick.

### 4. Bessere Konfiguration der Verteilringe

Die Erfahrung vieler Admins zeigt, dass sich die Verwaltung von Verteilringen mit WSUS extrem unflexibel und umständlich gestaltet.

Für die Update-Verteilung in ACMP CAWUM besteht die größtmögliche Flexibilität. So können die Updates aus Wunsch in einzelne Verteilringe aufgesplittet werden, je nach Update-Art (Critical, Security, Feature usw.) beziehungsweise Geräteart (Clients, Server). Abhängig vom Verteilprozess lassen sich bis zu drei Verteilringe definieren – zwei Test- und ein Freigabering mit frei definierbarer Verweildauer. So können beispielsweise sicherheitsrelevante Updates schnellstmöglich verteilt werden.

### 5. Weniger Wartungsarbeiten

Immer wieder ist es bei WSUS nötig, manuelle Wartungsarbeiten vorzunehmen, etwa, um das wuchernde Datenvolumen zu beschneiden. Viele Wartungsarbeiten, die Admins bei WSUS selbst erledigen müssen, entfallen bei CAWUM. Darunter zählen unter anderem das regelmäßige Indizieren der Datenbank oder das Ablehnen und Löschen nicht benötigter Updates.

CAWUM REAGIERT TAGESAKTUELL AUF DIE VON MICROSOFT BEREITGESTELLTEN UPDATES.ES FUNKTIONIERT GANZ AUTOMATISCH.

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

### 6. Dynamische Rechnergruppierung

In WSUS fassen Nutzer Rechner, die sie einem Update-Server zugeordnet haben, entweder manuell auf der Konsole in Gruppen zusammen oder weisen sie per GPO einer bestimmten Sammlung zu.

CAWUM ist flexibler, da Administratoren PCs mit Hilfe von Abfragen dynamisch in Container einsortieren können. Mögliche Kriterien sind alle erdenklichen Merkmale eines Rechners, die der Agent erfassen kann. Über beliebige Filter können Container mit Computern befüllt werden.

### 7. Datengräber nicht benötigter Pakete vermeiden

Ein Punkt sind die unter WSUS berüchtigten „Datengräber" nicht benötigter Pakete. Eine Einstellung in CAWUM bedeutet in dieser Hinsicht einen großen Vorteil: Administratoren können genau einstellen, nach welchem Zeitraum die Annahme von Updates, die auf den Systemen nicht nötig sind, automatisch abgelehnt wird und diese danach gelöscht werden.

In der Vergangenheit hat sich die Arbeit mit WSUS als komplex und zeitaufwendig herausgestellt. Mit ACMP CAWUM können IT-Abteilungen auf ein zuverlässiges Tool zurückgreifen und in puncto Effizienz schnell Fortschritte machen. Damit wird das Windows-Updatemanagement – auch für Office 365 – einfach wie nie.

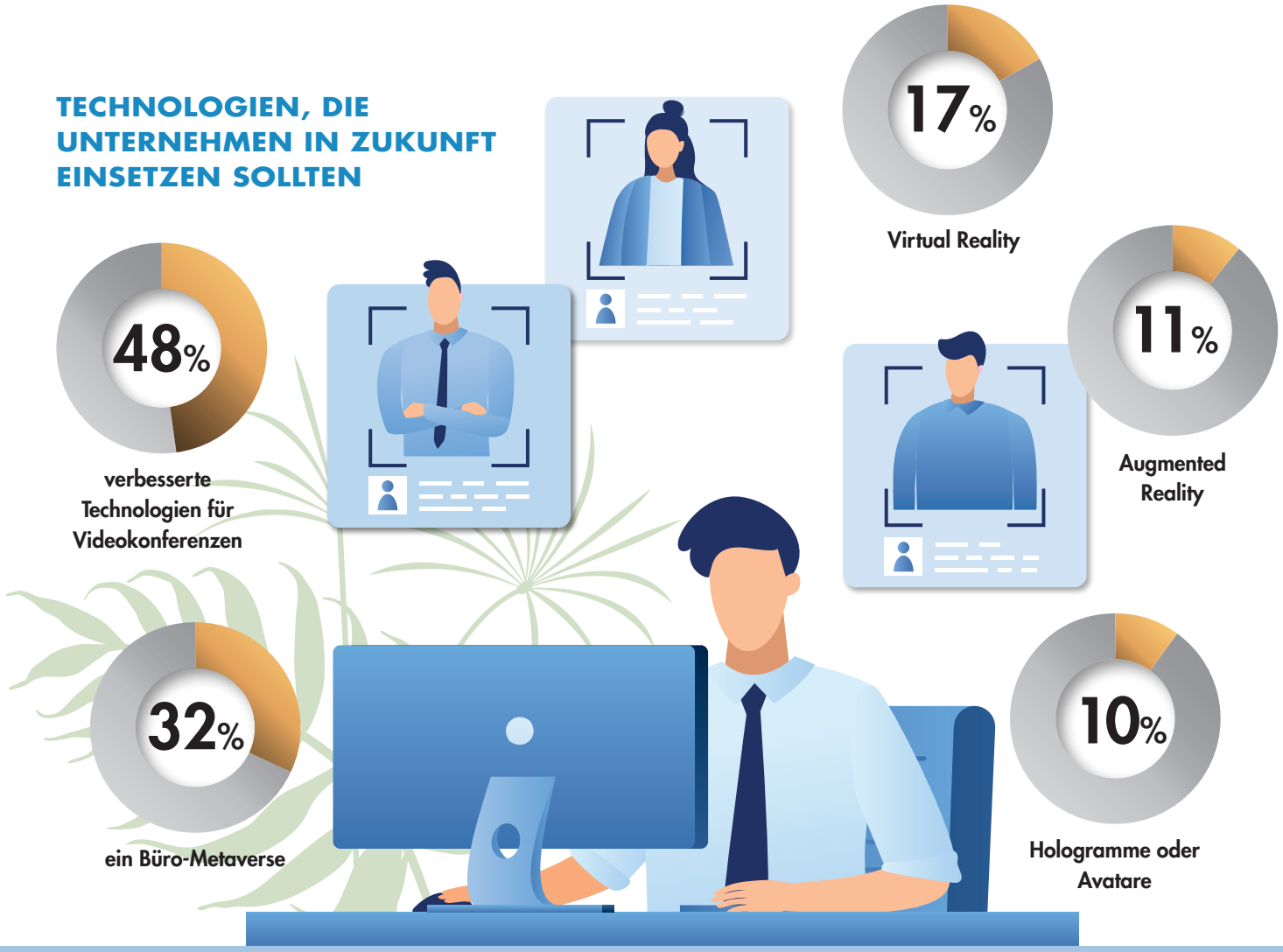
CAWUM ist unabhängig von WSUS. Alle Updates können bereits bei der Bereitstellung durch Microsoft freigegeben und verteilt werden.

***Sebastian Weber | www.aagon.com***

## VORTEILE DES WINDOWS-UPDATEMANAGEMENT MIT ACMP CAWUM

- Kompletter Verzicht auf WSUS
- Tagesaktuelle IT-Updates
- Autark und ohne ACMP Desktop Automation nutzbar
- Spart Zeit, Ressourcen und Bandbreite
- Ermittelt vorab, welche Patches ein Client benötigt und verschickt nur diese – nicht das komplette, mehrere Gigabytes umfassende Update-File
- Spart Serverlizenzen und Lizenzgebühren beim Updatemanagement
- Definieren einzelner Freigabeprozesse möglich
- Fein graduierbar, welche Patches in welchen Sprachen auf welchen File Repositories synchronisiert werden sollen
- Intuitive Benutzeroberfläche

## TECHNOLOGIEN, DIE UNTERNEHMEN IN ZUKUNFT EINSETZEN SOLLTEN




# HOMEOFFICE

## WIE VIEL IST ZU VIEL?

Wieviel Büro tut uns gut, und ab wann wird es im Homeoffice zu öde? Diese Frage hat sich auch Owl Labs, Anbieter für 360°-Videokonferenzlösungen, gestellt. Eine Umfrage unter deutschen Büroangestellten ergab: Mehr als die Hälfte der Arbeitszeit durchschnittlich im Homeoffice zu verbringen, gefällt der Mehrheit der deutschen Vollzeit-Büroangestellten gar nicht. Vor die Wahl gestellt, wären sie laut der Umfrage ziemlich genau je die Hälfte ihrer Arbeitswoche im Büro (2,6 Tage) und im Remote-Office (2,4 Tage). Männer bevorzugen das Büro dabei etwas stärker als Frauen: Sie tendieren zu knapp drei (2,8) Tagen im Büro und zu zwei (2,2) remote, während Frauen je genau 2,5 Tage im Büro und remote präferieren.

Frank Weishaupt, CEO bei Owl Labs, dazu: „Es ist auch 2022 bei Weitem nicht die Regel, dass sich Büroangestellte ihren Arbeitsort frei aussuchen dürfen, selbst wenn die Strukturen für hybrides Arbeiten in Unternehmen gegeben sind. Das sehen wir auch daran, dass es bei dem Verhältnis von tatsächlicher gegenüber präferierter Anzahl von Bürotagen aktuell Diskrepanzen gibt, und zwar unabhängig von Alter, Geschlecht, Joblevel oder Einkommen."

Er plädiert daher für mehr Selbstbestimmung und Autonomie, und sieht hier insbesondere Nachholbedarf bei KMU: „In kleineren bis mittleren Unternehmen ist die Diskrepanz stärker ausgeprägt, wie unsere Umfrage gezeigt hat. KMU können ihre Mitarbeitenden mehr dabei unterstützen, das individuell passendste Arbeitsmodell zu leben, anstatt starre Strukturen vorzugeben. Die hybride Arbeitswelt braucht mehr Recht auf Selbstbestimmung für Arbeitnehmende – Unternehmen laufen sonst Gefahr, ihre Angestellten nicht halten zu können und ihre Produktivität einzuschränken. Angesichts des akuten Fachkräftemangels ist das die falsche Taktik."

***www.owllabs.de***

# VON NULL AUF HUNDERT

## TELEKOM VERBINDET MOBILFUNK MIT MICROSOFT TEAMS

Innerhalb von nur fünf Jahren hat sich Microsoft Teams weltweit von Null auf Hundert zum erfolgreichsten digitalen Collaboration-Tool für Unternehmen etabliert. Die Zahl der monatlich aktiven Nutzer liegt inzwischen bei weit über 250 Millionen. Dazu hat auch beigetragen, dass durch Pandemie und Lockdown das hybride Arbeiten im Homeoffice und Büro zum Alltag in vielen Unternehmen geworden ist. Teams hat den Unternehmen dabei geholfen, das Konzept des flexiblen Arbeitens pragmatisch, einfach und schnell umsetzen zu können.

Hat sich durchgesetzt: Die Telefonie ist die meistgenutzte Funktion von Microsoft Teams. (Quelle: Telekom)

Sukzessive erweitert Microsoft die Features von Teams und hat auch die Sicherheit der Kommunikation weiter erhöht: ob Ende-zu-Ende-Verschlüsselung, Live-Transkription oder die automatische Zusammenfassung einer Besprechung, die den Chat-Text, Notizen, die während der Besprechung geteilten Dateien sowie eine Videoaufzeichnung enthält. Teams bietet inzwischen Funktionen, die das kollaborative Arbeiten deutlich vereinfachen.

### Telefonie meist genutzte Teams-Funktion

Die beliebteste Funktion aber ist – und damit hat Microsoft selbst nicht gerechnet – die Telefonie. Die Kosten sind kontrollierbar und die Mitarbeiter sind weltweit über die eigene Büronummer erreichbar. Dies ermöglicht die Kombination von Teams als Bestandteil von Office und Microsoft 365 mit einem Telefonanschluss samt Telefonie-Infrastruktur der Telekom. Die vorhandenen Festnetznummern lassen sich in Teams importieren, die Anrufe auf der Bürofestnetznummer kommen dann neben dem Desktop auch auf dem Smartphone, Tablet oder Laptop an – auch außerhalb des Büros im Homeoffice oder unterwegs bei Kunden. Und weitere Teilnehmer lassen sich mit einem Klick in einen bestehenden Anruf integrieren – auch externe Kunden, die keinen Zugang zu oder keine Lizenz für Teams besitzen.

Voraussichtlich im 4. Quartal 2022 geht die Telekom in Punkto Teams-Telefonie einen Schritt weiter. Exklusiv in Deutschland verbindet die Telekom dann auch das eigene Mobilfunknetz in Teams. Mit „Mobile für Microsoft Teams" können Telekom-Kunden dann auch Mobilfunknummern ihrer Beschäftigten in Teams integrieren, was die Nutzung von Teams als Telefonielösung noch attraktiver macht. Denn immer mehr Unternehmen verzichten inzwischen ganz auf eine Festnetznummer für ihre Mitarbeiter. Und da die Zahl der mobilen und hybriden Arbeitsplätze zunimmt, rufen Kunden und Kollegen meist die Mobilfunknummer an.

### Einfache Integration von Mobilfunknummern

Die Integration der Mobilfunknummer in Microsoft Teams ist genauso einfach wie bei der Festnetznummer und lässt sich ohne Unterstützung eines IT-Providers im Self Service umsetzen. Auch die bisherigen UCC-Funktionen von Teams, wie zum Beispiel Stellvertreter- oder Abwesenheitsregeln, sind mobil verfügbar. Ist in Outlook eine Abwesenheitsmeldung eingerichtet, wird ein entsprechender Text auf der Mobilbox abgespielt.

***www.geschaeftskunden.telekom.de***

# CLOUD-KOMPLEXITÄT

## ZUNEHMENDE HERAUSFORDERUNG FÜR UNTERNEHMEN

Dynatrace hat die Ergebnisse einer unabhängigen weltweiten Umfrage unter 1.303 CIOs und leitenden Cloud- und IT-Managern veröffentlicht. Die Ergebnisse zeigen, dass die Daten, die in solchen Umgebungen generiert werden, mit dem zunehmenden Trend zu Cloud-nativen Architekturen die Fähigkeit der aktuellen Lösungen übersteigen, aussagekräftige Analysen zu erstellen. Die CIOs stellen fest, dass ihre Teams auf mehrere unterschiedliche Monitoring- und Datenanalyselösungen angewiesen sind, um die Observability und Sicherheit aufrechtzuerhalten. Das erschwert es, schnell Antworten zu finden und die digitale Transformation voranzutreiben.

***www.dynatrace.com***

### KERNERGEBNISSE DER STUDIE

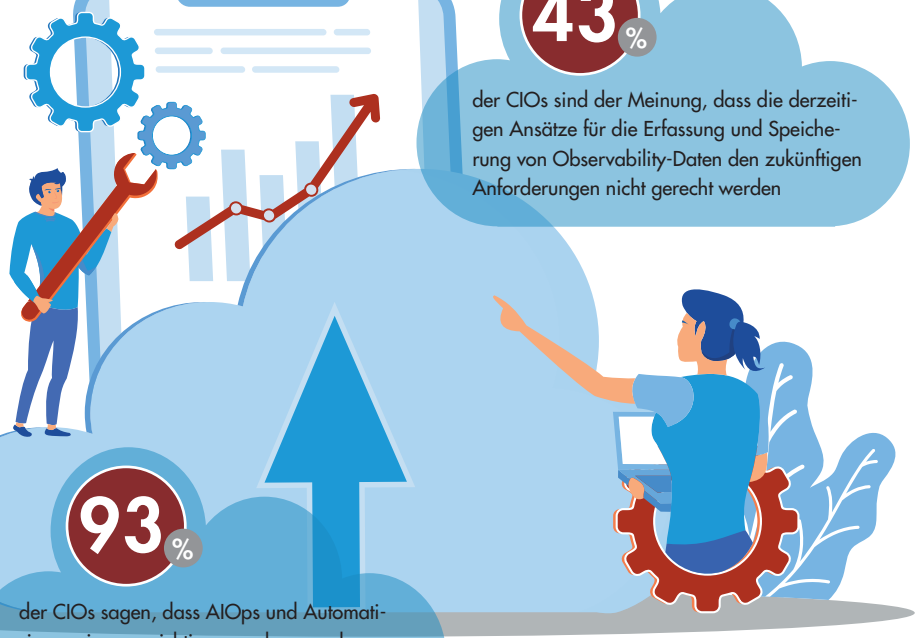
**71 %** der CIOs sind der Meinung, dass die Verwaltung der durch die Cloud-native Technologie-Stacks erzeugten Datenexplosion die menschlichen Fähigkeiten übersteigt

**64 %** der CIOs sagen, dass es schwieriger geworden ist, genügend qualifizierte IT-Ops- und DevOps-Experten für die Verwaltung und Wartung der Cloud-nativen Stacks zu gewinnen und zu halten

**77 %** geben an, dass sich ihre IT-Umgebung mindestens einmal pro Minute ändert

**43 %** der CIOs sind der Meinung, dass die derzeitigen Ansätze für die Erfassung und Speicherung von Observability-Daten den zukünftigen Anforderungen nicht gerecht werden

**59 %** der CIOs glauben, dass ihre Teams ohne einen stärker automatisierten Ansatz für den IT-Betrieb wegen der zunehmenden Komplexität ihres Technologie-Stacks bald überfordert und überlastet sind



**93 %** der CIOs sagen, dass AIOps und Automatisierung immer wichtiger werden, um den Mangel an qualifizierten IT-, Entwicklungs- und Sicherheitsexperten zu mindern

**45 %** der CIOs geben an, dass es zu kostspielig ist, die große Menge an Observability- und Sicherheitsdaten mit den bestehenden Analyselösungen zu verwalten. Deshalb bewahren sie nur die wichtigsten Daten auf.

Der kostenfreie Global CIO Report 2022 „How to Tame the Data Explosion and Overcome the Complexity of the Cloud" kann hier heruntergeladen werden: ***https://bit.ly/3elV4Q3***

# Leider fällt oft erst die Firewall, und dann erst der Groschen.

Cyber Incident Response Retainer:
Vertrauen Sie auf ein Team, das bei Cyberangriffen auf Ihr Unternehmen sofort reagiert und Ihnen auch vorab schon hilft, sich besser vor Hacker-Angriffen zu schützen. So schaffen wir gemeinsam mit Ihnen nachhaltige Werte und Vertrauen – heute und in Zukunft. www.pwc.de/incident-response

pwc

# IT-OPTIMIERUNG

## TURBULENTE ZEITEN MÜSSEN ALS CHANCE BEGRIFFEN WERDEN

Die Pandemie hat den Unternehmen gezeigt, dass sie flexibler werden müssen, um schneller auf die unvorhersehbaren Einflüsse von außen reagieren zu können. Das aktuelle Wirtschaftsklima ist ein weiteres Beispiel für solch ein unerwartetes Ereignis, das sogar größere Auswirkungen haben könnte als multiple Lockdown-Wellen. Anstelle zu agieren, neigen Unternehmen allerdings dazu in einer Phase des Abschwungs zu pausieren und legen IT-Projekte vielfach auf Eis, bis die Wolken vorüberziehen.

Oberflächlich betrachtet ist dieser Ansatz, der häufig von den Finanzabteilungen gesteuert wird, sinnvoll. Er geht mit dem Effekt einher, Ausgaben einzufrieren, denn warum sollte man angesichts einer unsicheren Wirtschaftslage etwas tun, was das Unternehmen ins Wanken bringen könnte? Vielfach ist die Ansicht vorherrschend, Aktivitäten so weit wie möglich herunterzufahren. Ein solches Vorgehen erschwert es Unternehmen allerdings zusätzlich, ihre Ziele zu erreichen und kann zu einer Abwärtsspirale führen. Stattdessen sollten Unternehmen eine Flaute als Chance sehen, um die Komplexität ihrer IT-Infrastruktur durch einen Umbau zu reduzieren, damit sie an Effizienz gewinnen.

### Optimierung und Automatisierung

Eine Neubewertung der Geschäftsabläufe kann zu erheblichen Verbesserungen führen. Wie die Pandemie bewiesen hat, kann die IT zu einem strategischen Geschäftsfaktor reifen, wenn sie strategisch für Veränderungsprozesse eingesetzt wird. In Zeiten der Knappheit siegt die Kreativität – das gilt auch für die Unternehmens-IT: Wird der Motor während eines Abschwungs besser eingestellt, wird dieser Wagen schneller durchstarten, wenn sich die Bedingungen ändern.

Übertragen auf die IT-Infrastruktur sollten Unternehmen die Zeit der wirtschaftlichen Instabilität nutzen, um folgende Faktoren zu überprüfen.

### 1. Berechnung der Kosten für den IT-Betrieb

Unternehmen sollten prüfen, wie viel Kosten im vergangenen Jahr für den Betrieb der IT-Infrastruktur angefallen sind. Können Kosten eingespart werden, wenn Hardware zugunsten von

Cloud First-Infrastrukturen ausgetauscht werden? Eine solche Transformation kann den Verwaltungsaufwand verringern und gleichzeitig zu einer flexibleren IT-Architektur führen.

Jetzt ist der Zeitpunkt gekommen, zudem die Infrastrukturkosten vor und nach der Pandemie zu vergleichen. Hybrides Arbeiten könnte bereits zu einer Verringerung der Bürofläche geführt haben. Verursacht ein Standort dennoch die gleichen Kosten, obwohl ein Teil der Belegschaft von zu Hause arbeitet, könnte es Zeit für ein Überdenken der Infrastruktur sein. Im Zusammenhang mit dem ortsunabhängigen Arbeiten sollten auch die Infrastrukturkosten für das virtuelle private Netzwerk (VPN) des Unternehmens überdacht werden, insbesondere wenn diese Technologie zur Erneuerung ansteht, aber die Budgets eingefroren wurden. Ein Cloud-basierter Ansatz auf Basis von Zero Trust für den Fernzugriff, kann nicht nur die Leistungsfähigkeit der Belegschaft erhöhen, sondern auch deren Sicherheit. Dabei wird nicht mehr der Netzwerkzugriff abgesichert, sondern jeder Zugriffsversuch auf Ebene der einzelnen Anwendung eines Mitarbeitenden verifiziert und authentifiziert. Außerdem unterstützt ein solcher moderner Sicherheitsansatz eine Cloud-First-Strategie als Basis für eine ganzheitliche digitale Transformation. Als Resultat entsteht eine schlankere Infrastruktur ohne die traditionelle Komplexität, die Unternehmen zu mehr Effizienz und größerem Wettbewerbsvorteil verhilft.

UNTERNEHMEN SOLLTEN EINE FLAUTE ALS CHANCE SEHEN, UM DIE KOMPLEXITÄT IHRER IT-INFRASTRUKTUR DURCH EINEN UMBAU ZU REDUZIEREN, DAMIT SIE AN EFFIZIENZ GEWINNEN.

James Tucker,
Sales Engineering Director, Zscaler,
www.zscaler.de

## 2. Umstellung auf die Cloud

Der Cloud-Ansatz reduziert wiederum auf anderer Ebene den Bedarf an Hardware und führt zur Reduktion des Wartungsaufwands, aber auch des Energieverbrauchs. Eine Cloud-First-Strategie ermöglicht den Mitarbeitenden einen nahtlosen Zugriff auf die Workloads von jedem Standort aus und entspricht damit den Vorstellungen für flexibles und dezentrales Arbeiten, die heute in vielen Unternehmen auf der Tagesordnung stehen. Wegen der Nutzung von IT-Services über die Cloud und verwalteter Dienste können sich die Unternehmen auf ihr Kerngeschäft konzentrieren. Darüber hinaus trägt die Partnerschaft mit Anbietern von Cloud-Diensten, die für den Betrieb der Cloud-Infrastruktur auf erneuerbare Energien setzen, zum Erreichen der eigenen Ziele für Klimaneutralität bei.

## 3. Manuelle Prozesse automatisieren

Die Untersuchung manueller IT- und IT-Sicherheitsaktivitäten wird wahrscheinlich eine Reihe von Möglichkeiten zur Automatisierung aufzeigen, unter anderem durch den Einsatz von künstlicher Intelligenz und maschinellem Lernen. Ein Beispiel: Ein Incident Responder in einem Security Operations Center (SOC), der einen Sicherheitsvorfall untersucht, kann Daten aus einer Anwendung oder einem System prüfen und dieses Wissen auf eine andere Anwendung oder ein anderes System übertragen, um eine Aktion durchzuführen. Ein solcher Prozess ist ineffizient. Jetzt ist es an der Zeit, neue Wege zu evaluieren, die diese Art von Aktivitäten automatisieren und gleichzeitig Geschwindigkeit und Genauigkeit erhöhen.

Unternehmen sollten sich fragen, ob die Bereitstellung von IT-Diensten automatisiert werden kann. Auf diese Weise könnte die Fluktuation von Mitarbeitenden durch das automatische Entfernen überflüssiger Benutzerprofile und das Hinzufügen von Profilen für neue User über eine Cloud-Sicherheitsplattform ausgeglichen werden. Auch die Aktualisierungen von Web-Proxy können automatisch erfolgen, anstatt von einem SOC durchgeführt zu werden.

## 4. Verbessern des Anwendererlebnisses

Ein Plattform-Ansatz für die IT bietet zahlreiche Vorteile und dazu zählt ebenfalls die Möglichkeit für die Belegschaft, von überall aus performanten Zugang zu Anwendungen und Systemen zu erhalten. Gerade bei den verbreiteten Online-Videokonferenzen aus dem Homeoffice kann beispielsweise Künstliche Intelligenz (KI) eingesetzt werden, um Probleme der Konnektivität zu erkennen, die zu einem eingeschränkten Anwendererlebnis mit Verbindungsabbruch führen. Anstelle der manuellen Bearbeitung von Tickets können IT- und Support-Teams von der aufwändigen Fehlersuche befreit werden, wenn die Störungen unter Einbeziehung verschiedener Parameter automatisch erkannt und behoben werden können. Dies kann helfen, verschiedene Störungen zu vermeiden, wie ein System, das bei einer bestimmten Aktion einfriert, oder eine Anwendung, die beim ersten Versuch keinen Zugriff gewährt. Tools zur Überwachung der digitalen Anwendererfahrung identifizieren Problemfälle in der Benutzererfahrung und erlangen zentrale Bedeutung, um die Ergebnisse der Fernarbeit zu optimieren.

## 5. Angriffsfläche verkleinern und Risikomanagement prüfen

Alle Unternehmen verfügen über redundante Domänen, Hardware und Systeme, die vielfach offen über das Internet erreichbar sind und die aus diesem Grund als Schwachstellen und Einfallstore für Angreifer in Betracht kommen. Dies vergrößert die Angriffsfläche des Unternehmens und damit das Potenzial für Sicherheitsverletzungen, auf das in Zeiten knapper Budgets und einem Mangel an Sicherheitsfachkräften reagiert werden sollte.

Es gibt Tools, die Unternehmen dabei helfen, den Angriffsvektor ihrer IT-Infrastruktur zu bewerten und Lücken im Risikomanagement aufzuzeigen, die geschlossen werden sollten. Die investierte Zeit zur Verringerung der Angriffsfläche und zur Optimierung der Sicherheitslage leitet einen Wandel hin zu aktiver Sicherheit ein, während reaktive Maßnahmen beibehalten werden können. Auf diese Weise minimieren Unternehmen das Risiko, Opfer eines kostspieligen Cyber-Angriffs zu werden.

## 6. Konnektivität automatisiert gewährleisten

Die Automatisierung der Kontrolle von Datenflüssen kann Geschwindigkeit, Genauigkeit und Effizienz verbessern. Wenn die Mitarbeitenden des Unternehmens weltweit verteilt sind und in hybriden Umgebungen arbeiten, ist es wichtig zu wissen, wer die User sind, welche Services und Anwendungen sie in Anspruch nehmen und wo sich die von ihnen benötigten Daten befinden. Oft sind die Daten in unterschiedlichen Systemen vorhanden, die kaum integriert sind, oder sie müssen im schlimmsten Fall manuell analysiert werden. Dadurch werden Geschäftsentscheidungen verlangsamt und es entsteht Zeit- und Arbeitsaufwand, den Unternehmen nicht stemmen müssen. Visibilität in die Datenströme aller Mitarbeitenden kann die Grundlage für Optimierungspotenzial bieten. Daher lohnt es sich, mithilfe von Tools und Konsolen den Fluss der Daten automatisch überwachen zu lassen, sodass stets die Konnektivität zwischen Nutzern, Daten und Anwendungen gegeben ist, aber auch Compliance-Vorgaben eingehalten werden.

## Fazit

Allzu oft gehen Unternehmen an ein IT-Upgrade mit einer lösungsorientierten Denkweise heran und konzentrieren ihre Bemühungen darauf, wie ein bestimmter Ansatz zu einem Unternehmen passt. Unternehmen sollten dabei nicht ausschließlich auf den Proof of Concept einer neuen Technologie achten, sondern sich den Vorteil für ihre spezielle Situation erläutern lassen und welchen Nutzen sie daraus realisieren können. Um diesen Nachweis zu erbringen und einen Aktionsplan für die Optimierung und Automatisierung erstellen zu können, müssen alle IT-Bereiche des Unternehmens – Sicherheit, Compliance, Betrieb, Verwaltung und so weiter – in die Planung einbezogen werden.

Dies führt zu einer vollständigen Sicht auf die Wertschöpfung der IT-Veränderungen und den Beitrag, der durch die IT für das Geschäftsmodell geleistet werden kann. Anstelle sich also derzeit Veränderungen zu verschließen, sollten Unternehmen die ruhigeren Zeiten nutzen, um ihre IT-Infrastruktur neu zu bewerten und sich zu fragen, wie sie ihren Betrieb optimieren können. Wird jetzt Zeit und Mühe in die Optimierung und Automatisierung investiert, können Unternehmen gestärkt aus dem Abschwung hervorgehen, wenn der wirtschaftliche Motor wieder anläuft und der Wettkampf erneut einsetzt.

***James Tucker***


itsa EXPO
CONGRESS
HOME OF IT SECURITY
HIT
HACKERS
HARD
LET'S TALK ABOUT IT SECURITY!
25. – 27. Oktober 2022
Nürnberg, Germany
Jetzt Gratis-Ticket sichern:
itsa365.de/hit-hackers-hard
NÜRNBERG MESSE

# DATA FIRST

## DAS SPANNUNGSVERHÄLTNIS ZWISCHEN SICHERHEIT & PRODUKTIVITÄT

**LIVE WEBINAR AM 12.10.2022 UM 11:00 UHR**

Yunus Karakaya, Presales Consultant, Consulting4IT GmbH

Daten sind die wichtigsten Ressourcen eines Unternehmens. Mit zunehmender Digitalisierung werden diese jedoch auch immer anfälliger für Angriffe. Die Erpressung im Zusammenhang mit Datendiebstahl stellt eine lukrative Möglichkeit für Cyber-Kriminelle dar und kann existenzbedrohend für Unternehmen sein.

Umso wichtiger ist es, über das eigene Sicherheitskonzept nachzudenken und dort anzusetzen, worauf Hacker abzielen: Daten.

Yunus Karakaya verrät Ihnen in diesem Webinar wie Sie den Schaden minimieren können ohne dass Ihre Produktivität eingeschränkt wird.

Nehmen Sie an unserer Sitzung teil und erfahren Sie:

- Risiken, die wir in der gesamten Branche beobachten
- Warum es so wichtig ist, mit der Security bei Ihren Daten anzufangen
- Wie Sie den Aktionsradius von Ransomware oder den Schaden, den ein kompromittierter Benutzer anrichten kann, reduzieren können, ohne an Ihrer Produktivität Abstriche machen zu müssen.

Interessenten können sich hier zu dem kostenlosen Webinar anmelden: ***www.it-daily.net/webinar***

# SICHERE GREMIENARBEIT

## ARBEITEN MIT VIRTUELLEN DATENRÄUMEN

**LIVE WEBINAR AM 20.10.2022 UM 11:00 UHR**

Andreas Glanz, Customer Success Manager, uniscon

Daniela Krause-Dettmann, Director Product Management, uniscon

Sensible Daten und vertrauliche Dokumente bestimmen die Arbeit von Vorständen, Geschäftsleitungen und Gremien. Diese Informationen sicher und compliance-konform zu bearbeiten, abzulegen und auszutauschen – intern wie extern, remote via PC oder iPad - , ist dabei die größte Herausforderung. Ein virtueller Datenraum bietet eine hochgeschützte Umgebung, um die Workflows gezielt zu unterstützen. Dabei lassen sich zum Beispiel Abstimmungen durchführen, Sitzungsmappen erstellen, Unterlagen annotieren, der unerwünschten Verbreitung von Dokumenten vorbeugen und Nutzeraktionen gezielt protokollieren.

Erfahren Sie alle Potenziale für die digitale Gremienarbeit und worauf Führungskräfte bei der Wahl des Datenraum-Anbieters achten sollten.

Warum Sie an diesem Webinar teilnehmen sollten:

- Profitieren Sie von über 10 Jahren Erfahrung des Anbieters
- Erfahren Sie, wie Sie den Herausforderungen beim Datenaustausch begegnen können
- Erleben Sie live, wie die Funktionen von idgard die Gremienarbeit erleichtern

Interessenten können sich hier zu dem kostenlosen Webinar anmelden: ***www.it-daily.net/webinar***

# MEHR TRANSPARENZ BEI PROJEKTAUFGABEN

## DURCHGÄNGIG DIGITAL ARBEITEN

Bei dem Förderanlagenbauer Schrage Conveying Systems sorgt eine neuentwickelte Kommunikationsplattform im Zusammenspiel mit dem ERP-System für Zeiteinsparungen und mehr Nachvollziehbarkeit bei der Erledigung von Aufgaben.

Um die selbstgesetzten hohen Qualitätsstandards jederzeit erbringen zu können, entschlossen sich die Verantwortlichen des ostfriesischen Familienunternehmens Schrage Conveying Systems vor einigen Jahren dazu, neben den bestehenden Wertschöpfungsbereichen Engineering, Konstruktion, Montage, Vertrieb und Kundendienst zusätzlich eine eigene Fertigung aufzubauen. Diese Firmenerweiterung, die mit einem entsprechenden Personalanstieg einherging, musste organisatorisch und technologisch abgesichert werden, weswegen seit 2019 das auf die Losgröße 1+ zugeschnittene Multiprojektmanagement-System ams.erp zum Einsatz kommt. Prozesstechnisch ergänzt wird die integrierte Business-Software durch das neuentwickelte Collaboration-Tool ams.taskmanager, dank dem viele vormals zeitaufwendige Routinetätigkeiten digitalisiert werden konnten. Papier sucht man beispielsweise in der Fertigung mittlerweile vergebens, wodurch sich die Effizienz und Transparenz der Abläufe deutlich erhöhte.

Die Kommunikationssoftware ergänzt das ERP-System, indem sie zusätzlich zu den übergreifenden Auftrags- und Geschäftskennzahlen aktuelle Informationen zum Status sowie zur Erledigung einzelner Projektschritte liefert. Es ist jederzeit für das gesamte Team ersichtlich, welche Aufgaben ab wann zur Bearbeitung anstehen. Ebenso ist nachvollziehbar, welche Mitarbeitenden welche Tasks zu welchem Zeitpunkt begonnen haben und wann diese beendet wurden.

### Eindämmung der E-Mail-Flut

Einen immensen Vorteil dieser Konstellation sieht IT-Leiter Helge Peters, der sämtliche Digitalisierungsbestrebungen bei Schrage Conveying Systems koordiniert, zudem in der Reduzierung der täglichen E-Mail-Flut. Denn obwohl digital, handelt es sich bei E-Mails doch größtenteils um unstrukturierte Informationen, für deren inhaltliche Bewertung, Ablage und Bearbeitung die Mitarbeiterinnen und Mitarbeiter in vielen Unternehmen selbst verantwortlich sind. „Die meisten kennen es wahrscheinlich aus eigener Erfahrung, dass Mails, die gerade nicht so wichtig erscheinen, in Unterordner verschoben werden und dann leicht in Vergessenheit geraten“, sagt er. Demgegenüber stellt die neue Kommunikationsplattform die Tasks zentral bereit, wodurch viele E-Mails schlichtweg obsolet werden.

DANK AMS.TASKMANAGER IST FÜR DAS GESAMTE TEAM JEDERZEIT ERSICHTLICH, WELCHE AUFGABEN AB WANN ZUR BEARBEITUNG ANSTEHEN.

Martin Gayer, Product Owner, ams.Solution AG, www.ams-erp.de

Das Kommunikations-Tool kommt bei den Norddeutschen abteilungsübergreifend und unternehmensweit zum Einsatz. Aktiv angebunden sind unter anderem das technische und das kaufmännische Büro sowie die Finanzbuchhaltung, die Konstruktion, die Arbeitsvorbereitung und die inzwischen komplett papierlose Fertigung.

Helge Peters zieht ein positives Resümee: „Unser Bestreben bestand von Beginn an darin, durchgängig digitaler zu werden, Papier und E-Mails durch eine strukturierte und nachvollziehbare Form der Kommunikation zu ersetzen und dabei kurze, schnelle Prozesse zu etablieren.“ Dabei hebt er neben der größeren Transparenz vor allem die minimierte Fehleranfälligkeit hervor.

***Martin Gayer***

# INFRASTRUKTUR-MONITORING

## DIE BESTE VERSICHERUNG FÜR RECHENZENTREN


Das Dätwyler Infrastruktur-Monitoring-System (DIMS) bietet einen Gesamtüberblick wie auch detaillierte Ansichten zum Status der IT-Infrastruktur in einem oder mehreren Racks, etwa in Micro- und Mini-Datacentern.

Mit der richtigen IT-Überwachungslösung lassen sich sensible und komplexe Infrastrukturen im Rechenzentrum gut kontrollieren. Eine einfache Bedienung und Skalierbarkeit sind dabei wichtige Auswahlkriterien.

Ohne Rechenzentren kommen unternehmenskritische digitale Prozesse zum Erliegen. Sowohl Systemfehler als auch der Faktor Mensch können zu Ausfällen und zu empfindlichen wirtschaftlichen Einbußen führen: Stehen Rechenzentrumsdienste nicht zur Verfügung, entstehen je Problemfall im Schnitt mehr als 1,5 Millionen US-Dollar Kosten, so Untersuchungen der Aberdeen Group. Gibt es keine ausreichende Notfallplanung, ist der Schaden noch höher, und pro Ausfall fallen 2,9 Millionen US-Dollar an. Dagegen müssen Unternehmen, die vorsorgen und ihre Infrastruktur konstant überwachen, durchschnittlich nur 72.000 US-Dollar aufwenden, um Störungen zu beheben.

### Grenzwerte im Blick

In Rechenzentren kann es neben ungeplanten Ausfällen auch zu kontrollierten Downtimes kommen, um Software zu aktualisieren, Hardware auszutauschen oder Wartungen durchzuführen. Mit geschickter Planung und der richtigen Überwachungstechnologie bleiben die Ausfallzeiten und damit auch die Kosten minimal. Überwacht werden beispielsweise die Klimasteuerung, Zutritt und Zugriffe, Temperatur und Luftfeuchtigkeit sowie die Stromversorgung. Das Monitoring prüft, ob sich alle zu beobachtenden Leistungskomponenten innerhalb der zuvor definierten Schwellwerte befinden. Sobald die Werte überschritten werden, schlägt das System Alarm, um Probleme frühzeitig beheben zu können.

Bei der Auswahl des passenden IT-Infrastruktur-Monitorings sollten IT-Manager das System eingehend auf einfache Bedienung und intuitive Konfiguration prüfen. Nützlich ist auch eine gute Kompatibilität für den Plattform-übergreifenden Einsatz: Idealerweise lässt sich das System über Schnittstellen wie SNMP einfach mit vorhandenen Management-Lösungen zusammenschließen, etwa solchen für Netzwerkkomponenten oder Server. Nicht zu vernachlässigen ist auch die Skalierbarkeit der Überwachungslösung für das Rechenzentrum. Denn für sich betrachtet ist ein Monitoring-System immer Teil eines übergeordneten IT-Managements, das mit den steigenden IT-Anforderungen über Erweiterungen und Updates ausbau- und zukunftsfähig sein muss.

Am besten eignen sich Infrastruktur-Monitoring-Systeme, die einen guten Gesamtüberblick sowie detaillierte Ansichten zum Status der IT-Infrastruktur in einem Rechenzentrum bieten. Die Überwachung sollte neben den Umgebungsbedingungen auch den Zutritt und den Energieverbrauch der IT-Komponenten einschließen sowie in Echtzeit aus der Ferne erfolgen können.

### Passgenaues Monitoring für Rechenzentren

Am Markt gibt es eine Reihe leistungsstarker Überwachungslösungen, die Hard- und Software kombinieren. Damit das Monitoring für unterschiedliche Rechenzentrumsdimensionierungen passt, sollten

Unternehmen darauf achten, dass die Racks über genügend Ports für den Anschluss von entsprechenden Tür-, Temperatur-, Luftfeuchtigkeits- oder Rauchsensoren verfügen. Bestimmte Produkte, wie das Dätwyler Infrastructure Monitoring System (DIMS) bieten die Option für zusätzliche Kameras, die sich nicht nur in den Racks, sondern auch in den IT-Räumen einsetzen lassen. Eine denkbare Variante für die Nutzung des Monitorings außerhalb des Rechenzentrums sind Etagenverteiler in Gebäuden. So erhalten Kunden einen ganzheitlichen Überblick über ihre IT-Infrastruktur und ihre Liegenschaft.

Gibt es zum Beispiel einen unbefugten Zutritt, laufen die vorab definierten Prozesse autark ab. Kunden oder IT-Verantwortliche können sich den Alarm per E-Mail schicken lassen. Auf Wunsch nimmt die Kamera ein Foto oder ein Video des Zwischenfalls auf und leitet auch dieses weiter. Zudem gibt es mehrere Eskalationsstufen: Meldet sich nach dem ersten Alarm niemand, kontaktiert das System eine definierte Kette von Verantwortlichen. Es ist möglich verschiedene Schwellenwerte festzulegen. IT-Verantwortliche können sich schon vor dem Erreichen kritischer Werte warnen lassen, damit sie genügend Reaktionszeit haben, um die Kühlung des Rechenzentrums rechtzeitig zu optimieren.

## Grafisches Dashboard, Reports und Schnittstellen prüfen

Vor der Entscheidung für ein Monitoring-System sollte die Benutzerfreundlichkeit überprüft werden. Mehrsprachige Web-GUIs mit integrierter Logik, die grafische Darstellung von Umweltdaten sowie eine Auswahl diverser Reports sind für die komfortable Verwaltung Pflicht. Wartungsmeldungen sollten sich bequem per E-Mail, SMS oder SNMP-Traps verschicken lassen. Damit sich die Überwachungslösung in die vorhandene IT-Landschaft integriert, braucht sie Schnittstellen wie Ethernet, USB, CAN, analog und digital. Von externen Geräten sollten sich Daten über SNMP GET lesen und visualisieren lassen. Um diese Fernüberwachungssysteme zusätzlich in führende SNMP-Tools integrieren zu können, unterstützen sie idealerweise SNMPv1, SNMPv2c und SNMPv3.

Fazit: Ein gut gewähltes Infrastruktur-Monitoring erlaubt eine automatisierte, übersichtliche Fernüberwachung in Echtzeit. Das sichert den IT-Betrieb und spart Zeit, die Unternehmen für geschäftskritische Prozesse nutzen können.

***Alexander Kölbel, Ralf Looks***
***https://itinfra.datwyler.com/de/***

# RECHENZENTREN SKALIEREN

## DATA CENTER DESIGN FÜR DIE ZUKUNFT

Bitrate, Bandbreite, Bereitstellung – Betreiber von Rechenzentren sehen sich im Zeitalter der Digitalisierung immer stärker wachsenden Anforderungen entgegen. Doch welche Basiskonzepte und Design-Elemente tragen zu einer gelungenen Skalierung für die Zukunft bei?

Der Anstieg des globalen Datenverkehrs und ressourcenintensiver Anwendungen wie Big Data, IoT, KI und maschinellem Lernen erfordern größere Kapazitäten und geringere Latenzzeiten im Rechenzentrum. Betreiber müssen mehr Ports mit höheren Datenraten und einer höheren Anzahl optischer Stränge bereitstellen. Dies erfordert unter anderem eine durchdachte Skalierung, deren Basis im nachhaltigen Management der „Basics" liegt – unter anderem im klassischen Fiber-Management.

### Nachhaltiges Kabel-Management statt Störfaktor Glasfaser

Rechenzentren nutzen vermehrt Mesh-Architekturen mit hohem Glasfaseranteil, die Anzahl an verbauter Glasfaser wird in Zukunft also weiterhin zunehmen. Dadurch wird das Kabelmanagement und das Management der steigenden Faserdichte zwangsläufig zeitintensiver und die Auswirkungen einer schlechten Verwaltung werden stärker spürbar: Neben dem Chaos ungeordneter Kabel, die auf die Flure wuchern, behindern übervolle Kabelschächte zudem die Belüftung und sorgen für Hitzeaufbau, was wiederum die Kühlsysteme unverhältnismäßig beansprucht.

Die Unordnung macht es zudem schwer bis unmöglich, einzelne Fasern zu identifizieren und zu managen. So steigt die Meantime-to-Resolution, der Turn-up-Speed sinkt und An- und Umbau werden kostenintensiv. Um das zu verhindern, wird das Kabel-Management zukünftig also mehr Zeit in Anspruch nehmen müssen. Viele Rechenzentrumsbetreiber sehen dieses Risiko und investieren in ein nachhaltiges Management um kostenintensive Fehlerbehebung zu vermeiden. Typische Ansätze reichen von Richtlinien für Kabelverlegung und Routing bis zu detaillierten Vorgaben zu Kabelkanal-Kapazitäten, Kabelgruppierungen nach Typ und Faserbestimmung (Labeling).

Eine weiterer Störfaktor sind fehlende Vorgaben zur Nutzung von Overhead-Kabeltrays. Best Practices zielen darauf ab, größere Trunk-Kabel von Patchkabeln zu trennen, etwa mit Ladder-Racks für Trunk-Kabel und Raceways für Patchkabel. Ebenso sollten Kupfer- und Glasfaserkabel getrennt geführt werden – ob in Gitterrinnen oder Unterflur-Kabelrinnen.

Kabel-Management-Strategien zielen nicht nur darauf ab, die Kabelführung jederzeit zugänglich zu gestalten und besser warten zu können, sondern haben auch einen spürbaren Effekt auf die optische Performance. Ein Negativbeispiel ist die Methode, Trunk-Kabel in Raceway zu führen, die für Patchkabel entwickelt wurden; wenn die größeren Kabel aus dem Raceway herausgeführt werden (Waterfall), passiert es häufig, dass die Kabel geknickt oder übermäßig gebogen werden, was die optische Leistung drosselt.

### Vier zukunftssichere Design-Prinzipien

Eine gute und nachhaltige Kabel-Management-Strategie garantiert die hürdenfreie Wartung und dient als Vorlage zur Skalierung oder für Upgrades im Rechenzentrum. Daher sollte direkt beim An- und Umbau von Rechenzentren das Kabel-Management von Anfang an priorisiert werden. Folgende vier Design-Prinzipien beispielsweise ermöglichen eine zukunftssichere und flexible Ausrichtung:

**1. Anwendungsbasierte Bausteine:**
Viele Rechenzentren steigen derzeit von Vier-Lane-Quad-Designs auf Oktal-Technologie um: Mit 16-Faser-Verkabelungen können Rechenzentren ihre Port-Effizienz maximieren und moderne Anwendungen ab 400G optimal bedienen. Doch ein Umstieg auf 16-Faser-Verkabelungen geschieht nicht immer direkt; daher ist es wichtig, parallel anwendungsbasierte Bausteine für 8-, 12- und 24-Faser-Konfigurationen vorzubereiten, um alte Implementierungen weiterhin zu betreiben ohne Fasern zu verschwenden oder Portzahlen zu verlieren.

> WENN DIE DIGITALISIERUNGSRATE ALS ANZEICHEN FÜR STEIGENDE TECHNISCHE ANFORDERUNGEN GESEHEN WERDEN KANN, STEHEN RECHENZENTREN VOR GROSSEN HERAUSFORDERUNGEN.
>
> Lewis White, Vice President Enterprise Infrastructure Europe, CommScope, www.commscope.com

## 2. Modulare Panels:

Wer die eigene Glasfaserkapazität schnell umverteilen kann, reagiert flexibler auf Anforderungen durch Kunden und Anwendungen. Die Crux liegt im Design der Patchpanels: Herkömmliche Panels sind fest konfiguriert – Kassetten und Adapterpakete können nicht einfach ausgetauscht werden. Modulare Panels erlauben eine schnelle Rekonfiguration einzelner Elemente und flexible Bereitstellung der geforderten Glasfaserkapazitäten, was Kosten und Zeit spart und Rechenzentrumsbetreiber besser auf Kundenbedürfnisse eingehen lässt.

## 3. Standardisierte Polarität:

Mit zunehmender Komplexität der Glasfaserinstallationen wird es immer schwieriger, die richtige Ausrichtung der Sende- und Empfangspfade über die gesamte Verbindung hinweg sicherzustellen. Im schlimmsten Fall müssen Installateure Module oder Kabelbaugruppen umdrehen, um die passende Polarität herzustellen. Fehler werden möglicherweise erst erkannt, wenn die Verbindung bereits eingerichtet ist, und die Behebung des Problems kostet Zeit. Es gibt bereits Glasfaserplattformen auf dem Markt, die sich diesem Problem annehmen. Sie besitzen eine standardisierte Polarität, die die Ausrichtung vereinfacht und dem Umdrehen der Kabelbaugruppen vorbeugt.

## 4. Reflexionsabsorption:

Um die Bitraten zu verdoppeln, ohne die Bandbreite zu erhöhen, werden neue Signal-Codierungen wie PAM4 verwendet. Die doppelte Bitrate beeinflusst allerdings die Signal-to-Noise Ratio, sodass die Verbindungen anfälliger für Rückreflexion oder Optical Return Loss (ORL) werden. Licht wird dabei zum Transmitter zurückreflektiert und kann als Störfaktor die Performance beeinflussen. APC-Stecker schaffen Abhilfe: Die Stirnfläche der Ferrule (Gehäuse der freiliegenden Faser) ist so poliert, dass das reflektierte Licht in den Mantel austritt, statt im Faserkern zu bleiben. Moderne Transceiver für Single- und Multimode MPO16 sind bereits auf APC ausgerichtet, ebenso wie Trunk- und Patchkabel.

### Weniger Platz, mehr Flexibilität

Wenn die Digitalisierungsrate als Anzeichen für steigende technische Anforderungen gesehen werden kann, stehen Rechenzentren vor großen Herausforderungen, vor allem auf der Ebene hyperskalierender Cloud Data Center. Die Nachfrage nach Bandbreite wächst, damit werden auch die Qualität der Service-Angebote und geringe Latenzzeiten für Endnutzer immer wichtiger.

Das Ergebnis: Glasfaser zieht immer tiefer ins Netzwerk ein – und mit seiner wachsenden Dominanz schrumpft der Platz im Rechenzentrum. Um erfolgreich zu skalieren, sollten Rechenzentrumsbetreiber bei den „Basics" beginnen: Gut durchdachten Strategien zum Routing, zur Kabelführung, zum modularen Aufbau, zu Polarität und Steckern. Mit diesen Design-Elementen können Betreiber auch den Anforderungen der Zukunft flexibel begegnen.

***Lewis White***

DAS NÄCHSTE

SPEZIAL

itsecurity

ERSCHEINT AM
30. NOVEMBER 2022

CLOUD COMPUTING: Vorteile nutzen

DAS SPEZIAL: Banking, Finance & Controlling

DIGITALE TRANSFORMATION: Zukunfts-Strategien

DIE AUSGABE 11/2022
VON IT MANAGEMENT
ERSCHEINT AM 28. OKTOBER 2022

## INSERENTENVERZEICHNIS





WIR WOLLEN IHR FEEDBACK

Mit Ihrer Hilfe wollen wir dieses Magazin weiter entwickeln. Was fehlt, was ist überflüssig? Schreiben sie an u.parthier@it-verlag.de

## IMPRESSUM


***Geschäftsführer und Herausgeber:***
Ulrich Parthier (-14)

***Chefredaktion:***
Silvia Parthier (-26)

***Redaktion:*** Carina Mitzschke

***Redaktionsassistenz und Sonderdrucke:***
Eva Neff (-15)

***Autoren:***
Philipp von der Brüggen, Martin Gayer, Thomas Herrmann, Michelle Janz, Marcel Kappestein, Alexander Kölbel, Ralf Looks, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, James Tucker, Sebastian Weber, Ralph Weiss, Lewis White

***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.





***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. 30. Preisliste gültig ab 1. Oktober 2022.

***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, 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

www.natuvion.com

Natuvion


## Studie kostenlos herunterladen:

Welche Erfahrungen haben mittelständische Unternehmen mit ihrer digitalen Transformation gemacht? Was hat sie überrascht? Was würden sie heute anders machen? Natuvion hat nach Antworten gesucht und über 200 Manager umfangreich befragt. Die ganze Studie gibt es gratis unter:
**https://www.natuvion.com/de/transformationsstudie-2022/**

# Transformationsstudie 2022

# “Tue, was du sagst und sage, was du tust – Kaspersky ist und bleibt transparent und sicher.”

Waldemar Bergstreiser,
Head of Channel Germany, Kaspersky

**Branchenweiter Vorreiter für Transparenz und Zuverlässigkeit**

Seit Jahren legen wir Quellcode, Updates, Threat Detection Rules, Daten, Engineering-Praktiken und mehr in unseren Transparenzzentren offen. Transparenzzentren bestehen aktuell in der Schweiz, Spanien, Malaysia, Singapur, Japan, den USA und Brasilien.

**kas.pr/vertrauen**

kaspersky 25 years YOUR PROTECTION IS OUR PRIORITY

itsecurity
OKTOBER 2022

DAS SPEZIAL

Threat Intelligence
ab Seite 20
kaspersky

Seppmail.Cloud
ab Seite 24
SEPPMAIL

DATA LOSS PREVENTION

# WIR SCHÜTZEN VOR DEM UNBEKANNTEN

DriveLock SE

THOUGHT LEADERSHIP

OT- UND IT-NETZWERKE
AB SEITE 10
macmon intelligent einfach

SICHERER LOGIN
AB SEITE 12
nevis

MODERNE SECURITY GESTALTEN
AB SEITE 16
SOPHOS

## IT-SECURITY TRENDS

Von Zero Trust bis Made in EU

## STIEFKIND IT-SECURITY

Sicherheitslücken minimieren

## SICHERE DATENRÄUME

Einfallstore für Cyberkriminelle

www.it-daily.net

Digital Security
**Progress. Protected.**

ESET 100% Made in EU IT-Security

# IT-Sicherheit ist Vertrauenssache

*„IT-Sicherheit ist Vertrauenssache. Hier sollten Sie und Ihre Kunden keine Kompromisse eingehen und bewusst auf IT-Security made in EU setzen."*

– Holger Suhl, Country Manger DACH, ESET Deutschland GmbH

www.eset.de/itsa

Stand 7-530

25.–27. Oktober in Nürnberg

itsa EXPO CONGRESS

# INHALT

## COVERSTORY



## THOUGHT LEADERSHIP



## IT-SA SPEZIAL



## IT SECURITY

# DATA LOSS PREVENTION

## „WIR SCHÜTZEN VOR DEM UNBEKANNTEN"

Jede Organisation hat sensible Daten. Ihrem Missbrauch oder Verlust systematisch vorzubeugen, ist das Ziel von Data Loss Prevention (DLP). Welche Maßnahmen und Lösungen sich dahinter verbergen, erläutert Anton Kreuzer, CEO bei DriveLock SE, im Interview.

**it security:** *Schön, dass Sie sich Zeit nehmen, Herr Kreuzer. Starten wir mit einer einfachen Frage: Wozu benötigt man Data Loss Prevention?*

**Anton Kreuzer:** Von der Unachtsamkeit eines Kollegen oder einer Kollegin über die kriminelle Hackerindustrie bis hin zu Aspekten der nationalen Sicherheit: Datenverlust verursacht auf verschiedene Arten Schäden. Der Verlust geschäftskritischer Daten oder geistigen Eigentums kann einen hart erarbeiteten Wettbewerbsvorteil zunichtemachen. Verstöße gegen Gesetze wie die DSGVO oder branchenspezifische Richtlinien ziehen Strafen und Reputationsschäden nach sich. Auch Personen können Schaden erleiden, wenn personenbezogene Daten verloren gehen oder missbraucht werden.

**it security:** *Welche Daten müssen besonders geschützt werden?*

**Anton Kreuzer:** Inhaltlich können das verschiedenste Daten sein, zum Beispiel sensible Kundendaten, Patientenakten, geschäftskritische Unternehmensdaten, Daten, die der Privatsphäre unterliegen aber auch politisch oder militärisch sensible Daten.

**it security:** *Wo fangen Unternehmen am besten an, Datenverlust vorzubeugen?*

**Anton Kreuzer:** Am Anfang steht die Discovery-Phase mit Inventarisierung und Klassifizierung. Das heißt, es gilt herauszufinden, welche Daten in einem Unternehmen überhaupt vorliegen und welche sensibel sind. Wichtig ist zudem, so früh wie möglich den Datenverkehr zu überwachen, um Transparenz herzustellen. Jeder Datenverlust, der präventiv vermieden wird, muss später nicht aufgedeckt und bekämpft werden. Durch mehr „Prevention" ist weniger „Detection" nötig.

**it security:** *Wo können sich sensible Daten befinden?*

**Anton Kreuzer:** Aus operativer Sicht unterscheiden wir zwischen drei „Aggregatzuständen", in denen sich Daten befinden können:

1. „Data at Rest" sind Daten im Ruhezustand, die etwa auf einem Speichermedium oder einem Server liegen.

2. „Data in Motion" sind Daten in Bewegung, die zum Beispiel gerade von einem Wechseldatenträger auf ein Gerät oder von einem Server zu einem Client unterwegs sind.

3. Als „Data in Use" werden Daten bezeichnet, die gerade live genutzt werden.

**it security:** *…und in allen Aggregatzuständen müssen die Daten geschützt werden.*

**Anton Kreuzer:** Richtig. DLP beschreibt hier ein Regelwerk, das alle Tools, Prozesse und Lösungen zum Schutz von sensiblen Daten vereint. Das umfasst alles, was vor unautorisiertem Zugriff, Datenverlust und -missbrauch schützt. Dabei spielt es keine Rolle, ob Daten irgendwo ungenutzt liegen oder in Bewegung oder Nutzung sind.

**it security:** *Was gehört neben dem konkreten Schutz von Daten zu DLP?*

**Anton Kreuzer:** Wie eingangs erwähnt gehört zu DLP auch die Einhaltung von Gesetzen und Compliance Richtlinien, zum Beispiel ISO 27001, DSGVO, oder branchenspezifische Standards wie PCI im Retail-Sektor oder HIPAA im Healthcare-Sektor.

Eine zentrale Anforderung ist hier die Nachweispflicht beziehungsweise Auditierung: Es muss überwacht werden, wer wann und wie auf welche Daten zugegriffen hat.

> DURCH MEHR „PREVENTION" IST WENIGER „DETECTION" NÖTIG.
>
> Anton Kreuzer, CEO, DriveLock SE, www.drivelock.com

**it security:** *Also werden auch aktiv Lücken aufgedeckt und behoben.*

**Anton Kreuzer:** Ja, das ist eminent wichtig. DLP sorgt dafür, dass Daten unter Umständen überhaupt erst sichtbar gemacht werden. Das heißt, dass ein Unternehmen einen Überblick bekommt, wo welche Daten liegen. Daraus lässt sich dann ableiten, wer Zugriff hat und ob dadurch potenzielle Schwachstellen entstehen. Cyber-Bedrohungen nehmen seit Jahren zu. Oft lässt sich durch das Sichtbarmachen von Daten und Zugriffsrechten sehr einfach eine unbeabsichtigte Datenexponierung aufzeigen und beseitigen. Kurz gesagt: Zuerst heißt es „Gain Insight", dann erst „Take Action".

**it security:** *Welche Rolle spielt der Trend hin zur Cloud?*

**Anton Kreuzer:** Die Nutzung von Kollaborationslösungen und virtuellen Datenspeichern wie AWS, Azure oder Google Cloud ist praktisch und ermöglicht produktives hybrides Arbeiten. Das bringt hinsichtlich Datensicherheit aber Herausforderungen mit sich. Sofern ein Unternehmen keine klaren Vorgaben und Lösungen bietet, werden häufig auf eigene Faust Workflows vereinfacht, Shortcuts genommen oder sogar Daten auf private Accounts synchronisiert. Es ist möglich, Lösungen anzubieten, die die Reibungspunkte während des Arbeitens verringern. Zu DLP zählt also auch die Vermeidung von Schatten-IT, also IT, die eingerichtet wurde unter unwissentlicher oder sogar wissentlicher Umgehung der IT-Abteilung.

**it security:** *Was bedeutet DLP vor dem Hintergrund dieser neuen Normalität hybriden Arbeitens?*

**Anton Kreuzer:** Wir sind mit DriveLock seit 20 Jahren als deutsches Unternehmen im Markt tätig. Wir haben die Entwicklung unserer Kunden hin zur Cloud von Anfang an begleitet und wissen daher sehr genau, was für DLP bei Cloud-Lösungen notwendig ist. Auch hier lautet der erste Schritt: Überblick verschaffen und Datenverkehr überwachen. Bei Data in Motion und Data in Use muss gewährleistet werden, dass nur die entsprechenden Nutzer Zugriff haben. Dieser Zugriff muss sicher sein, egal, von wo aus sie arbeiten. Die Cloud-basierte Endpoint Protection von DriveLock ermöglicht das und kann schnell eingerichtet werden, ganz gleich, ob ein großes Unternehmen 100.000 Endpoints hat oder ein mittelständisches Unternehmen nur einige wenige Clients.

**it security:** *Welche Rolle spielt das Thema Verschlüsselung?*

**Anton Kreuzer:** Verschlüsselung ist natürlich ein zentraler Bestandteil von DLP. Cloud-DLP-Lösungen verschlüsseln Daten entweder vor der Übertragung oder in der Cloud. Beim Thema Schlüsselmanagement lautet das zentrale Stichwort: „No Backdoor". Die Frage lautet: Überlassen Unternehmen die Verschlüsselung großen Anbietern oder verwalten sie die Schlüssel selbst? DriveLock bietet hier „Made in Germany" und „No Backdoor".

**it security:** *Wie genau schützt die DriveLock Lösung vor Datenverlust?*

**Anton Kreuzer:** Wir arbeiten hier nach dem Prinzip des sogenannten „Swiss-Cheese-Models" und legen mehrere Sicherheitsschichten übereinander. Stellen Sie sich einen Schweizer Käse vor: Jede Scheibe hat Löcher – so wie beispielsweise eine Firewall, die bestimmte Daten durchlassen muss, andernfalls könnte man nicht arbeiten oder eine Gerätekontrolle, die die Nutzung bestimmter Geräte erlaubt. Jede Sicherheitsbarriere weist gewisse Schwachstellen oder Löcher auf. Wenn Sie nun mehrere Käsescheiben übereinanderlegen, verdecken sich diese Löcher gegenseitig:

1. Device Control sorgt für Sicherheit an Geräten und Schnittstellen, etwa an USB-Eingängen.

2. Application Control definiert ganz spezifisch, welche Applikationen wo und mit welchen Services laufen dürfen. Das greift sowohl im Ökosystem des Unternehmens als auch im Homeoffice. Unsere Lösung hält auch Daten in Workloads oder Applikationen sicher, die in virtuellen Umgebungen laufen.

3. Mit Application Behaviour Control gibt es auch noch eine Art Verhaltenskodex für Anwendungen. Das sind bestimmte Regeln, die jede Anwendung beachten muss. Ein Verstoß wird sofort festgestellt und die nicht erlaubte Aktion – wie das Speichern in ein bestimmtes Verzeichnis oder Ausführen von Sub-Prozessen – die diese Anwendung vorhat, wird gestoppt.

**it security:** *Was ist der Vorteil einer Cloud-basierten Endpoint Protection?*

**Anton Kreuzer:** Der große Vorteil unserer Lösung: Im Gegensatz zum üblichen Antiviren-Scanner schützt DriveLock auch vor dem Unbekannten und Unternehmen müssen nicht in Infrastruktur investieren, um alle Sicherheitskriterien oder Compliance-Vorgaben zu erfüllen. Cloud-basierte Sicherheitslösungen können Schutz für Geräte gewährleisten, die nicht im Unternehmensnetzwerk arbeiten. Auch eine Aktualisierung dieser Lösungen ist einfach und schnell, ohne dass die Geräte mit dem Firmennetz verbunden sein müssen. Wir bringen auf diese Weise sehr schnell mehr Sicherheit zum Endgerät, ohne großen Aufwand und ohne hohe Investitionskosten.

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

# SICHERHEIT FÜR SENSIBLE DATEN

## PRÄVENTION IST IMMER BESSER ALS INTERVENTION

Wie viel Speicherplatz wird benötigt, um sensible Daten rund einer halben Million Menschen zu transportieren? Ein einziger USB-Stick reicht. Das erfuhren kürzlich die Einwohner der japanischen Stadt Amagasaki, als besagter USB-Stick mit persönlichen Daten verloren ging. Was war passiert? Ein Mitarbeiter eines IT-Dienstleisters der Stadtverwaltung hatte seine Tasche mit USB-Stick nach einem alkoholreichen Abend verloren

Das effiziente Mittel gegen derartige Datenlecks heißt: Data Loss Prevention (DLP). Vorfälle wie der in Amagasaki zeugen davon, dass Datenschutz nicht erst bei Datenverlust beginnt. Werden verschiedene Ebenen der Vorbeugung berücksichtigt, sind Daten vor nachlässigem Umgang oder auch mutwilligen Angriffen geschützt. Welche konkreten Maßnahmen und Lösungen verbergen sich hinter DLP? Ein zentrales Konzept hier ist Zero Trust, das auf dem Grundsatz basiert: „never trust, always verify".

### Transparenz schaffen und Daten klassifizieren

DLP beginnt mit dem Sichtbarmachen aller inaktiven Unternehmensdaten (Data at Rest) und ihrer Klassifizierung danach, wie sensibel und schützenswert sie sind. Die zweite zentrale Maßnahme ist die Überwachung aktiver Daten (Data in Use oder Data in Motion). Erst wenn ein Unternehmen vollständigen Überblick hat, kann unerwünschter Datenfluss verhindert werden.

### Geräte unter Kontrolle bringen

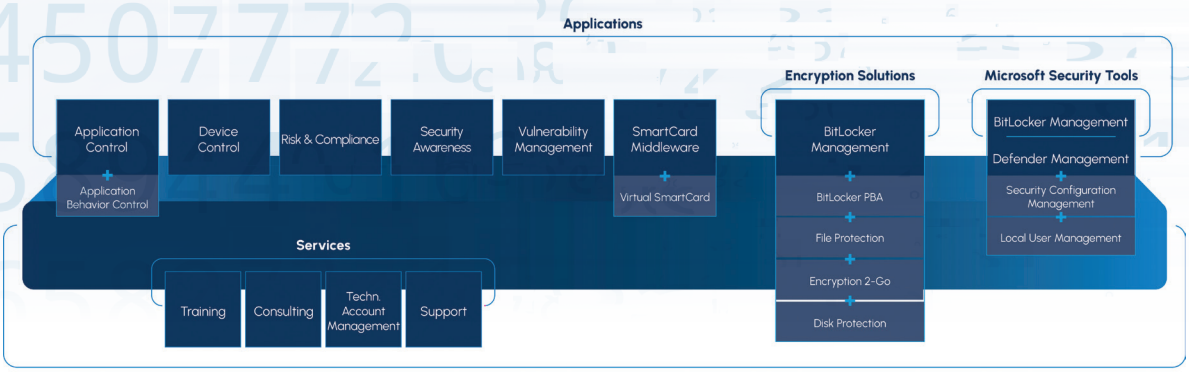
Häufig stellen Unternehmen beim Thema Identitäts- und Zugriffsmanagement eklatante Schwachstellen und exponierte Daten fest. Die gute Nachricht lautet: Auf Einsicht folgt Maßnahme. So kann eine umfassende Gerätekontrolle beispielsweise einem unautorisierten Abfluss von Daten vorbeugen und diesen vermeiden. Hier ist es wichtig, dass je nach Anwendungsfall granular abstimmbare Maßnahmen zur Verfügung stehen - von allgemeiner Gerätekonfiguration über die dezidierte Autorisierung bestimmter Personengruppen und Geräte bestimmter Hersteller bis hin zum spezifischen Management einzelner (oder bestimmter) USB-Wechseldatenträger. Darüber hinaus sollten Daten auf Wechseldatenträgern automatisch verschlüsselt werden, so dass sie auch im Falle eines Verlusts des Trägers vor unberechtigten Zugriffen geschützt sind.

Device Control ist allerdings nur ein Modul, das Lösungsanbieter für Endpoint Security im Rahmen einer Multi-Layered Defence ins Feld führen, um Datenverlust vorzubeugen. Der Trend zu Hybrid Work und die Nutzung von Cloud-Diensten bringt hinsichtlich Datensicherheit weitere Herausforderungen mit sich. Was passiert, wenn ein Unternehmen seiner Belegschaft keine klaren Vorgaben und technischen Lösungen für das Homeoffice anbietet? Häufig suchen sich Mitarbeitende dann eigenständig Lösungen. Das Resultat: Shortcuts, ungesicherte und unautorisierte Wechseldatenträger, Datensynchronisation auf privaten Accounts, kurz: eine anfällige und unkontrollierbare Schatten-IT.

> UNTERNEHMEN MÜSSEN MITARBEITENDEN EIN EFFIZIENTES UND SICHERES ARBEITEN ERMÖGLICHEN – EGAL VON WO.
>
> Andreas Fuchs, Head of Strategy and Vision, DriveLock SE, www.drivelock.com

### Anwendungen unter Kontrolle bringen

Mitarbeitende nutzen eine Vielzahl an Anwendungen, die weitere Angriffspunkte bieten können. Die aktive Kontrolle von Anwendungen, also Application Control, verhindert die Ausführung unbekannter Programme. Als anschauliches Beispiel eignet sich in diesem Kontext der Türsteher einer Party, die das gesamte Ökosystem eines Unternehmens verkörpert. Der Blacklisting-Ansatz von Antiviren-Scannern ist das Äquivalent zur „Hausverbotsliste" des Türstehers: Bekannte Störenfriede wer-




den geblockt. Aber was passiert mit den bis dato unbekannten Störenfrieden?

Der Zero Trust Security Ansatz geht daher noch weiter: Eine Whitelist definiert exakt – analog der Gästeliste des Türstehers – welche Anwendungen zugelassen werden. Was nicht explizit erlaubt ist, darf gar nicht erst im Ökosystem eines Unternehmens zur Ausführung kommen. Diese aktive Kontrolle von Applikationen, Skripten und Programmbibliotheken bietet dementsprechend nicht nur Schutz vor bekannten, sondern auch vor unbekannten Bedrohungen.

## Unerwünschtes Verhalten unterbinden

Nun kann es trotz Device Control und Application Control vorkommen, dass eine bereits zugelassene Anwendung missbraucht wird und in der Lage ist, Schaden anzurichten. Hier kommt als drittes Modul Application Behaviour Control (ABC) ins Spiel. So wie ein Verhaltenskodex auf einer Party festlegt, welches Verhalten erwünscht und welches unerwünscht ist, kontrolliert ABC das Verhalten zugelassener Anwendungen. Zum Beispiel ist es verdächtig, wenn plötzlich Unmengen von Daten wie im obigen Beispiel auf einen USB-Stick kopiert werden. ABC gewährleistet, dass nicht erlaubte Aktionen oder unerwünschte Skripte und Schadsoftware sofort erkannt und gestoppt werden.

Die sogenannte „Kill Chain" eines Angriffs wird damit frühzeitig unterbrochen, bevor der Worst Case eintritt, ein Dominostein den nächsten anstößt und eine unkontrollierbare Kaskade in Schwung kommt. So werden Unternehmen durch Application Behaviour Control frühzeitig auf potenzielle Gefahren aufmerksam und können entschärfend eingreifen.

## Verschlüsselung

Ein weiterer zentraler Bestandteil von Data Loss Prevention ist die Verschlüsselung. Cloud-DLP-Lösungen verschlüsseln Daten nicht nur lokal, sondern auch in virtuellen Storages und in der Cloud. DriveLock bietet diesbezüglich beispielsweise die nahtlose Integration von BitLocker Management, geht aber noch einen Schritt weiter: Eine eigene proprietäre Verschlüsselung ermöglicht Encryption at Rest, unabhängig davon, ob die Daten lokal, auf Servern oder auf Cloud Storages liegen.

## Schnelle Einrichtung und Integration

Die Cloud-basierte Endpoint Protection von DriveLock kann schnell eingerichtet werden, egal ob ein großes Unternehmen 100.000 Endpoints besitzt oder ein mittelständisches Unternehmen eine kleinere IT-Umgebung sichern muss.

Der große Vorteil: Die DriveLock Zero Trust Platform wird aus der Cloud bereitgestellt, schützt aber alle Typen von Endpoints: angefangen bei lokalen Workloads über virtuelle Umgebungen bis hin zu den Workloads in der Cloud. Nutzer können also reibungslos und sicher arbeiten, egal ob sie im Büro, im Homeoffice oder unterwegs sind. Unternehmen müssen dafür aber nicht in zusätzliche Infrastruktur investieren, um generelle Sicherheitskriterien oder branchenspezifische Anforderungen zu erfüllen.

Bereits bestehende Sicherheits-Tools, wie die BitLocker Festplattenverschlüsselung, das Microsoft Defender Antivirus Programm oder die Microsoft Defender Firewall bieten Unternehmen in der Regel guten Schutz. Allerdings ist es für Unternehmen und Sicherheitsbeauftragte häufig nicht leicht, diese Tools zentral zu managen und zu konfigurieren. Die DriveLock Zero Trust Platform vereint Device Control, Application Control und Application Behaviour Control mit diesen Microsoft Sicherheitsfunktionen in einer übersichtlichen Benutzeroberfläche. Dieser integrierte Ansatz vereinfacht die Verwaltung und Visualisierung enorm.

Unternehmen müssen Mitarbeitenden ein effizientes und sicheres Arbeiten ermöglichen – egal von wo. Mit der DriveLock Zero Trust Platform können Daten dort erhoben, verarbeitet und gespeichert werden, wo es notwendig und erlaubt ist. Unterbunden werden hingegen unautorisierter Datenabfluss – wie etwa das Speichern einer halben Million sensibler Personendaten auf einem USB-Stick –, unerwünschtes Eindringen in das System oder unerwünschte Aktivitäten innerhalb des Systems. Für den Fall, dass Daten bewusst und gewünscht gespeichert werden sollen, sorgt DriveLock für die erzwungene Verschlüsselung der Daten – nicht nur auf Wechseldatenträger, sondern auf jedem Speichermedium jenseits von lokalen Festplatten und USB-Sticks. Die Cloud-basierten Lösungen bieten auf diese Weise eine effektive, mehrschichtige Sicherheit für sensible Daten.

***Andreas Fuchs***

# RANSOMWARE

## WIE KÖNNEN SICH UNTERNEHMEN VOR SCHADSOFTWARE SCHÜTZEN?


Ransomware ist einer der schädlichsten Cyber-Angriffe und das Risikopotenzial nimmt stetig zu. Durch das Einschleusen von Schadsoftware wird der Zugriff auf Daten und Systeme verhindert. Die Daten des Opfers werden verschlüsselt, um ein Lösegeld zu fordern oder ausgeleitet, um sensible Informationen zu veröffentlichen.

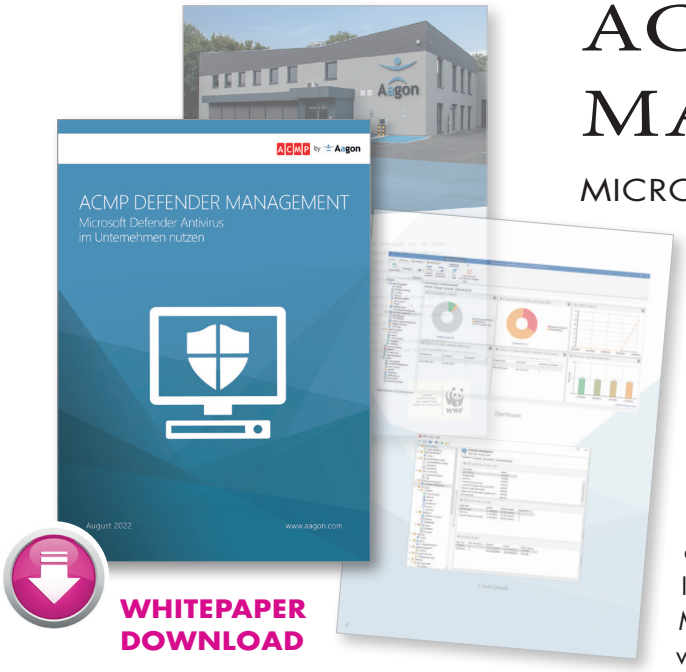
Durch Ransomware-Angriffe kann die IT-Infrastruktur eines Unternehmens für Wochen oder gar Monate lahmgelegt werden, wodurch der gesamte Geschäftsbetrieb zum Erliegen kommt.

Die Wahrscheinlichkeit, dass auch Ihr Unternehmen getroffen wird, ist hoch und realistisch. Prävention und Aufklärungsarbeit wird damit für Unternehmen immer wichtiger, um kein Opfer von Cyberkriminellen zu werden.

**WHITEPAPER DOWNLOAD**

Das Whitepaper umfasst 18 Seiten und steht kostenlos zum Download bereit.
***www.it-daily.net/Download***

---




**WHITEPAPER DOWNLOAD**

Das Whitepaper umfasst 11 Seiten und steht kostenlos zum Download bereit. ***www.it-daily.net/Download***

# ACMP DEFENDER MANAGEMENT

## MICROSOFT DEFENDER ANTIVIRUS IM UNTERNEHMEN NUTZEN

Die Nutzung von Microsoft Defender Antivirus kann ohne zentrale Verwaltung sehr zeitaufwendig sein. Die Konfiguration über Microsoft-Management-Lösungen wie Intune und SCCM erschweren zusätzlich eine übersichtliche Organisation.

Mit ACMP Defender Management können Administratoren Microsoft Defender Antivirus zentral verwalten und konfigurieren. In der ACMP-Console bietet die Lösung alle Funktionen, um den Microsoft Defender zu managen und dadurch den administrativen Aufwand zu vereinfachen.

In diesem Whitepaper erfahren Sie, welche Vorteile und Funktionen das ACMP Defender Management hat und welche Möglichkeiten die Lösung bei der Verwaltung von Microsoft Defender Antivirus bietet.

# SECURITY AUF ALLEN EBENEN

## WIE STEHT ES MIT DER OT UND IT-NETZWERK-SICHERHEIT, DER CYBERSECURITY UND DEM IDENTITY- UND ACCESS MANAGEMENT?

**OT- und IT-Netzwerke wachsen in der Industrie 4.0 zusammen, das erfordert neue Sicherheitskonzepte wie auch neue Expertisen. Schließlich sind die Netzwerke der Dreh- und Angelpunkt von Digitalisierungsprozessen.**
**Im Cybersecurity-Part werden konträre Aspekte diskutiert. Etwa, ob das menschliche Verständnis einer Umgebung und die Kreativität, Angriffswege zu identifizieren und Verteidigungsmaßnahmen zu entwickeln ausreicht und wo eine Maschine diese auch auf lange Sicht nicht ersetzen kann.**

**Beim Thema Identity Access Management zeigt unser Autor wie man von einer Insellösung über einen POC (Proof of Concept) zu einer zukunftsorientierten, ausbaufähigen Lösung kommt.**

# NEUE SICHERHEITSKONZEPTE UND EXPERTISE

## OT- UND IT-NETZWERKE WACHSEN IN DER INDUSTRIE 4.0 ZUSAMMEN

Im Alltag vieler Unternehmen, die sich der digitalen Transformation verschrieben haben, verschmilzt die klassische Informationstechnologie (IT) mit der OT. Die Abkürzung OT steht für Operational Technology und beschreibt Hardware und Software, die physische Endgeräte, industrielle Anlagen, Prozesse und Ereignisse steuert. Das OT-Netzwerk überwacht über Sensoren Umgebungsbedingungen, erkennt Objekte oder löst nach individuellen Vorgaben gezielte Aktionen aus. So lassen sich zum Beispiel Fertigungsumgebungen in der Automobilindustrie automatisieren oder der Energieverbrauch in Bürokomplexen reduzieren. Smarte Sensoren tauschen Daten aus und wenden sogar eigene Algorithmen an. So schaffen sie nicht nur eine deutlich effizientere Produktion, sondern sie verändern die Geschäftsmodelle und Jobanforderungen vieler Unternehmen von Grund auf.

Die Abkürzung IT steht für Informationstechnologie. Sie vereint als Oberbegriff Hardware, Software und IT-Services wie Cloud-Dienste. Darunter fallen Geräte wie Server, mobile Endgeräte, Drucker und Netzwerkkomponenten. Unter den Oberbegriff Software fallen neben den Betriebssystemen alle Anwendungsprogramme sowie mobile Apps. Die Kommunikation innerhalb der klassischen Fertigungs- und IT-Netzwerke erfolgte bisher in geschlossenen Systemen, im OT-Netzwerk mit herstellerabhängigen Protokollen. Diese stehen mittlerweile meist in Verbindung mit einem TCP/IP-Netzwerk. Unternehmen können die ermittelten Daten netzwerkweit analysieren, verarbeiten und nutzen. So lassen sich selbst hochkomplexe Vorgänge automatisieren oder zum Beispiel das Bestandsmanagement, die Nachverfolgung von Komponenten oder die Wartung von Maschinen einfacher, effizienter und sicherer gestalten. Ersatzteile, Waren oder Transportfahrzeuge werden per Mausklick über mobile Endgeräte in Echtzeit lokalisiert. Zusätzlich kommunizieren viele Sensoren per Funk, wie WLAN, Bluetooth oder RFID für den Nahbereich.

DREH- UND ANGELPUNKT VON DIGITALISIERUNGSPROZESSEN SIND IT- UND OT-SYSTEME UND DIE DARIN BEFINDLICHEN DATEN.

Brian Lieser,
Vice President and General Manager,
Industrial Network Solutions, Belden Inc,
www.belden.com

Brian Lieser, Vice President and General Manager, Industrial Network Solutions, Belden Inc: „Dreh- und Angelpunkt von Digitalisierungsprozessen sind IT- und OT-Systeme und die darin befindlichen Daten. Der Schutz der Netzwerke und die Datensicherheit spielen zukünftig eine noch exponiertere Rolle. In der Industrie 4.0 wandelt sich die Security zu einer Schlüsseltechnologie als unabdingbare Voraussetzung für beschleunigte Wertschöpfung."

### Sicheres Netzwerk ist nicht gleich sicheres Netzwerk

Der Anspruch an die Unternehmens-IT konzentriert sich auf die einfache Bedienbarkeit, Schnelligkeit und Zuverlässigkeit von Datenübertragung über eine gemeinsame Infrastruktur. Die Grundlage für einen sicheren Betrieb ist die allumfassende Cybersecurity mit Priorität auf der Vertraulichkeit unternehmenskritischer Daten und dem Schutz der Endgeräte vor unberechtigtem Zugriff oder Manipulation.

Dagegen fokussiert man sich beim Betrieb von OT-Netzwerken primär auf den sicheren Betrieb der Anlagen mit der zuverlässigen Datenübertragung bei für den Prozess zeitkritischen Applikationen – auch in anspruchsvollen Produktionsumgebungen (Hitze, Feuchtigkeit, Staub). Der Fokus liegt hier auf der dauerhaften Verfügbarkeit, dem störungsfreien Betrieb der Fertigungsanlagen, natürlich auch unter Beachtung von Sicherheitsanforderungen.

### Prozesse optimieren – mit der Lösungskompetenz von Belden

Die Komplexität vieler industrieller Prozesse führt zu einer Reihe von Ineffizienzen. Brüche im Prozess verhindern eine optimale Automatisierung. Manuelles Scannen und langsame Transportzeiten führen zu Differenzen beim Wareneingang, Lagerung und der Nachverfolgung. Fehler bei der Kommissionierung und beim Scannen sowie komplexe Verladevorgänge senken die Effizienz beim Versand. Die Belden-Lösungen zur Steigerung der Arbeitsproduktivität befassen sich genau mit diesen kritischsten Herausforderungen auf dem Weg zur Automatisierung und erhöhter Profitabilität.

### Zuverlässige Lösungen aus einer Hand

Mit seinem strategischen „ESD"-Ansatz (Enhanced Solution Delivery) bietet Belden einen kompletten Lösungsansatz für die Umsetzung industrieller Automatisierungsprojekte. Das Unternehmen hat ein umfassendes durchgängiges Lösungsportfolio und die erprobte Kompetenz – gemeinsam mit Partnern und Kunden – ein rundum sicheres Netzwerk – vom Kabel über die Switches bis hin zur Security-Lösung (Firewall+NAC) – zu realisieren. Erfahrene Experten gestalten gemeinsam mit den Partnern und Kunden eine maßgeschneiderte Roadmap für Optimierungsprozesse in der Industrie 4.0. Um den neuen Anforderungen in Punkto Netzwerksicherheit gerecht zu werden, fokussiert sich das Unternehmen gemeinsam mit macmon auf die Weiterentwicklung durchgängiger Lösungen für die Sicherheit in OT/IT-Umgebungen. Erste gemeinsame Projekte stammen aus der bereits langjährigen Zusammenarbeit mit Hirschmann – einer Marke von Belden – dem Technologie- und Marktführer für industrielle Netzwerke.

Entscheidend ist, dass bei der Kommunikation zwischen industriellen Netzwerken und Office-Umgebung die jeweiligen Datenschutzrichtlinien umfassend berücksichtigt sind. Die Einbindung von Produktionsanlagen mit langen Standzeiten in ein modernes, umfassendes Sicherheitskonzept ist eine große Herausforderung, da Hersteller, Alter, Kommunikationsfähigkeit und auch Maschinenintelligenz sich in einer gewachsenen, heterogenen Struktur stark voneinander unterscheiden.

Die Netzwerkzugangskontrolle von macmon ermöglicht nur anwendungsspezifische Zugriffe, für die überprüfte Berechtigungen auf Basis der Anwenderidentität und des Kontexts vorliegen. In Kombination mit den vorhandenen OT-Sicherheitsmechanismen, wie Hirschmann Firewalls, lässt sich so ein granulares Zugriffskonzept umsetzen. Dadurch werden die Anforderungen der Produktion nach Verfügbarkeit und Echtzeitfähigkeit erfüllt.

### Sicherheit für Produktion und Verwaltung

In Büronetzwerken gewinnt das Konzept des „Zero Trust" an Bedeutung, bei dem alle Teilnehmer, Benutzer und Geräte erst ihre Identität sowie Integrität nachweisen müssen, bevor eine Kommunikation mit einer Zielressource stattfinden kann. macmon secure dehnte bereits 2021 mit seiner Zero-Trust-Network-Access-Strategie seinen bewährten Schutz auf sämtliche Unternehmensressourcen in der Cloud aus.

***www.macmon.com***

#### MACMON SCHÜTZT PRODUKTIONSNETZWERKE:

- Einbinden aller Produktionstechniken ohne Gefahr für das bestehende Netzwerk oder die Produktion selbst
- Gewährleistung des spontanen Zugangs zu den Produktionssystemen für Wartungstechniker durch die Definition von gezielten Kommunikationswegen und der entsprechenden Absicherung
- Individuelle Festlegung von Richtlinien auf Benutzer- und Geräteebene
- Unterstützung bei der Zertifizierung nach ISO 27001
- Überwachung und Kontrolle aller im Netzwerk befindlichen Geräte (Live-Bestandsmanagement)
- Dokumentation aller Zugriffe auf das Netzwerk
- Definition von gezielten Datenrouten und Übergabeschnittstellen
- Exakte Netzwerksegmentierung
- Nahtlose Integration von Cloud-Ressourcen auch im Produktionsumfeld

# MODERNE SECURITY GESTALTEN

## OPTIMALER SCHUTZ GEGEN NEUE UND TRICKREICHE ANGRIFFSSTRATEGIEN

Die Cybergefahren werden zunehmend größer und Unternehmen müssen ihre Security immer schneller ausbauen und erweitern, um den Angriffsstrategien der Cyberkriminellen effektiv entgegenzuwirken. IT Security hat mit Michael Veit, Security-Experte von Sophos gesprochen, um die aktuelle Lage zu bestimmen und über Möglichkeiten zu sprechen, wie Unternehmen moderne Security gestalten können.

**it security:** *Ist das Cyber-Gefahrenpotenzial wirklich so hoch oder lassen uns die Beispiele von betroffenen bekannten Unternehmen etwas zu sehr fürchten?*

**Michael Veit:** Nichts wäre mir lieber, als Entwarnung zu geben. Wir sind in einer Situation, die keineswegs vergleichbar mit den Zeiten ist, als wir alle uns noch durch einen simplen Virenscanner und eine Firewall in Sicherheit wähnen konnten. Aus Viren-Programmier-Freaks sind professionelle Gruppierungen entstanden, die am Rad eines kriminellen Milliardengeschäfts drehen.

**it security:** *Wie ist denn die Lage konkret?*

**Michael Veit:** Neben vielen Studien von Organisationen wie beispielsweise dem BSI, haben wir unsere eigenen Studien, die sich weitgehend mit den Ergebnissen anderer decken. In unserem State of Ransomware Report 2022 haben wir festgestellt, dass 67 Prozent der in Deutschland befragten Unternehmen im Jahr 2021 von einem Ransomware-Angriff betroffen waren. Und von den angegriffenen Unternehmen hatten danach wiederum 65 Prozent verschlüsselte Daten – also wurden über 43 Prozent der befragten Unternehmen Opfer eines erfolgreichen Ransomware-Angriffs. Das durchschnittliche Lösegeld, das von deutschen Unternehmen gezahlt wurde, hat sich fast verdoppelt und beträgt über 250.000 EUR. Das Lösegeld ist aber fast vernachlässigbar im Verhältnis zum Gesamtschaden durch den Cyberangriff. Dieser Gesamtschaden betrug bei deutschen Unternehmen durchschnittlich etwa 1,7 Millionen Euro und ist vor allem durch Betriebsausfall entstanden. Im Durchschnitt benötigten die betroffenen Unternehmen einen Monat, um die IT und die Produktion wiederherzustellen. Für viele Unternehmen stellt ein Ausfall der IT und damit oft auch der Produktion für so einen langen Zeitraum eine Existenzbedrohung dar. Nach Umfragen von Cyber-Risikoversicherern liegen Cybervorfälle und Betriebsunterbrechungen deshalb zu Recht auf den ersten beiden Plätzen der Geschäftsrisiken für Unternehmen.

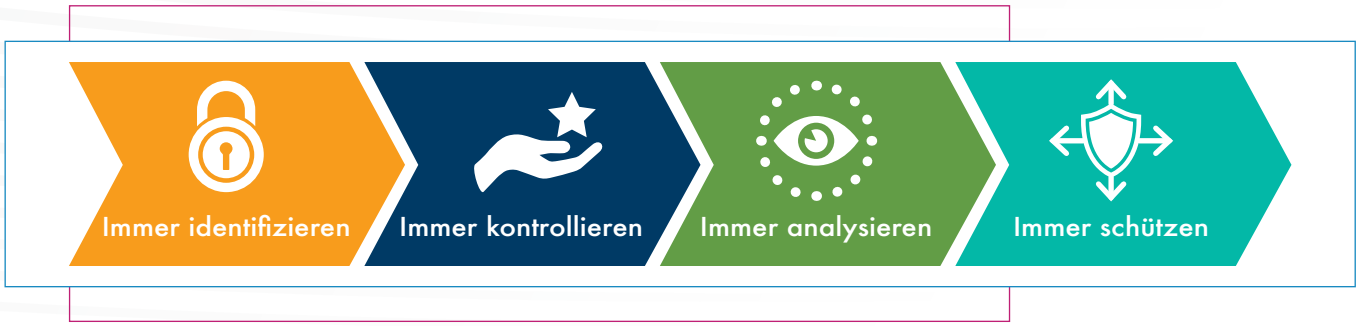
DAS MENSCHLICHE VERSTÄNDNIS EINER UMGEBUNG UND DIE KREATIVITÄT, ANGRIFFSWEGE ZU IDENTIFIZIEREN UND VERTEIDIGUNGSMASSNAHMEN ZU ENTWICKELN, KANN EINE MASCHINE AUCH AUF LANGE SICHT NICHT ERSETZEN.

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

**it security:** *Wie sieht denn eine optimale Vorbereitung aus, wie kann man sich optimal schützen?*

**Michael Veit:** Wir glauben, dass ein optimaler Schutz gegen neue und trickreiche Angriffsstrategien in einem integrierten Verbund von Security-Lösungen besteht. Einzelne und voneinander unabhängige Security-Inseln lassen zu viele Lücken offen, die es den Cyberkriminellen einfach machen, einen Weg ins Unternehmen zu finden. Darum haben wir letztes Jahr unser Adaptive Cybersecurity Ecosystem vorgestellt. Es ist eine SaaS-Sicherheitsplattform, die neben den Lösungen wie Endpoint-Schutz, Cloud-Schutz und Next Generation Firewalls auch unser Extended Detection and Response (XDR)-Produkt und unseren Managed Detection & Response (MDR)-Service einbezieht. Dies verbesserte unsere Fähigkeit, Echtzeit-Telemetrie von Endpoints, Servern, Firewalls und Cloud-Workloads zu erhalten, um Kunden und unseren Incident-Response-Teams einen Vorsprung vor Bedrohungsakteuren zu verschaffen.

**it security:** *Sie sprechen von einem Security Ökosystem, ist das die optimale Vorbereitung für Unternehmen?*




**Michael Veit:** Unser Adaptive Cybersecurity Ecosystem vereint jegliche Form der Security in einem zentral gesteuerten Verbund. Mit unserer Central Plattform verfolgen wir diese Strategie schon seit Jahren, indem einerseits alle Security-Bausteine über eine zentrale Konsole gesteuert und synchronisiert werden sowie dieselben Regeln und Vorgaben nutzen. Gleichzeitig haben wir mit unserem sogenannten „Security-Heartbeat" dafür gesorgt, dass alle unsere Lösungen ständig untereinander kommunizieren und Informationen austauschen. Dadurch erreichen wir eine wesentlich schnellere und höhere Informationsdichte und in Folge eine bessere Erkennung und Abwehr von Angriffen. Außerdem ist damit eine automatisierte und unternehmensübergreifende Reaktion auf Gefahren möglich.

Das Adaptive Cybersecurity Ecosystem geht noch einen entscheidenden Schritt weiter. Durch unsere forensische Arbeit wissen wir, dass wir zusätzlich menschliche Expertise benötigen, um den modernsten Angriffsstrategien entgegenzutreten. Wir haben diese Services deshalb mit unseren technischen und KI-basierten Lösungen kombiniert, um ein System zu etablieren, das den individuellen Anforderungen der Kunden anpassbar ist und einen hochwirksamen Schutz bietet.

**it security:** *Welche Rolle spielt das viel diskutierte Zero Trust in diesem Ökosystem*

**Michael Veit:** Zero Trust ist ein Konzept, das für viele Unternehmen zunehmend wichtig ist. Es geht es darum, von einer Kultur des Verbietens, zu einer Kultur des Erlaubens zu wechseln. Genauer gesagt, bis heute ist in vielen IT-Umgebungen alles erlaubt, was nicht explizit verboten ist. Bei Zero Trust verhält es sich anderes herum. Prinzipiell ist alles verboten und man erlaubt explizit bestimmten Usern den Zugriff auf bestimmte Ressourcen. Das ist gedanklich aber auch auf organisatorischer und technischer Ebene eine echte Umstellung.

Selbstverständlich haben wir Zero Trust in eine Security-Lösung einfließen lassen, das Zero Trust Network Access Gateway. Prinzipiell kann diese Lösung solitär genutzt werden, wie alle unsere anderen Lösungen auch. Im Verbund des Adaptive Cybersecurity Ecosystem kann es seine Vorteile noch besser ausspielen, weil alle Komponenten inklusive der menschlichen Expertise in diesem Ökosystem nahtlos ineinandergreifen.

**it security:** *Was sind heute die größten Treiber des Zero-Trust-Ansatzes, große Unternehmen?*

**Michael Veit:** Bei Zero-Trust sind große Unternehmen oder Organisationen, die einen besonderen Schutz bedürfen wie kritische Infrastrukturen, die Vorreiter. Wir haben allerdings durch die Pandemie einen weiteren Treiber. Es ist das Homeoffice, das sehr viele Unternehmen eingeführt haben und jetzt nach guten Erfahrungen beibehalten. Das Homeoffice ist aus Sicht der Security eine nicht zu unterschätzende Herausforderung. Denn die klassische Remote-Access-VPN-Verbindung für zuhause simuliert nichts anderes als ein langes Netzwerkkabel vom Homeoffice direkt in das Unternehmen – und zwar ohne die entsprechenden Schutzmaßnahmen, die man üblicherweise gegenüber Externem walten lassen würde. Die Schwierigkeit besteht darin, dass klassische Security-Konzepte alles nach außen abschirmen, prüfen und sichern, während sie alles, was sich innerhalb der Sicherheitsperimeter befindet, als vertrauenswürdig betrachten. Die Remote-Access-VPN-Verbindung führt dieses Prinzip ad absurdum, indem es das externe und aus Sicht der Security weitgehend unkontrollierte Homeoffice, als vertrauenswürdig innerhalb der Sicherheitsperimeters ansieht. Das bietet Cyberkriminellen große Chancen, sich über Homeoffice-Rechner ohne größere Hürden direkt in den Kern des Unternehmens einzuschleusen. Cyberkriminelle nutzen dies gezielt aus, wie beispielsweise der erfolgreiche Angriff auf die Colonial Pipeline in den USA im letzten Sommer gezeigt hat, bei dem die Angreifer in das Netzwerk genau über diesen Weg eingedrungen sind.

Mit dem ZTNA haben Unternehmen die Möglichkeit, den Schutz zwischen Homeoffice und der Kerninfrastruktur zu realisieren. Übrigens kann das ZTNA von externen Servicepartnern betrieben werden, womit die Unternehmen kein dedizierte Zero-Trust-Expertise aufbauen müssen.

**it security:** *Ist Zero Trust eine Security-Variante, die für das neue IT-Sicherheitsgesetz 2.0 hilfreich ist?*

**Michael Veit:** Sophos hat als offiziell vom BSI qualifizierter APT-Response-Dienst-

leister (Advanced Persistent Threat) für KRITIS einen Solution Brief erstellt, der Unternehmen und Organisationen hilft, ihre Security-Maßnahmen gemäß den neuen Anforderungen rechtzeitig anzupassen und dazu gehört auch Zero Trust. Im Solution Brief beschreibt Sophos, welche Themen aus dem Anforderungskatalog des BSI mit welchen Komponenten der Security adressiert werden können, um die geforderten Sicherheitsvorkehrungen umzusetzen – insbesondere im Zusammenhang mit dem neuen IT-Sicherheitsgesetz 2.0.

**it security:** *Könnten Sie bitte nochmals die Wichtigkeit von maschineller und menschlicher Security für uns unterscheiden?*

**Michael Veit:** Es geht eigentlich nicht um den Unterschied, sondern vielmehr um die Verzahnung beider Aspekte. Beispielsweise indem MDR-Services die Lücken durch menschliche Expertise schließen, die die beste Künstliche Intelligenz heute noch nicht finden und erkennen kann. KI ist eine hoch komplexe und weit fortgeschrittene Technologie. Sie ist aber noch meilenweit vom menschlichen Verstand entfernt. Und genau diese Schwäche versuchen Cyberkriminelle auszunutzen, indem sie selbst auf hochkarätige Technologie und trickreiches Verhalten, wie zum Beispiel die Nutzung legitimer Admin-Tools zum Einschleusen von Schadsoftware, setzen. Nur menschliche Expertise kann dem bis heute etwas entgegensetzen und final einschätzen, ob hier bestimmte Werkzeuge in legitimer oder schädlicher Absicht eingesetzt werden. Bei den Incident-Response-Services ist es ähnlich. Hier untersuchen Menschen die von der maschinellen Intelligenz vorsortierten und bewerteten Ereignisse und entscheiden über die beste Strategie, einen aktiven Angriff zu stoppen und zukünftige Angriffe zu verhindern. Das menschliche Verständnis einer Umgebung und die Kreativität, Angriffswege zu identifizieren und Verteidigungsmaßnahmen zu entwickeln, kann eine Maschine auch auf lange Sicht nicht ersetzen.

**it security:** *Wie viele Unternehmen nutzen heute diese zusätzliche menschliche Security-Komponente?*

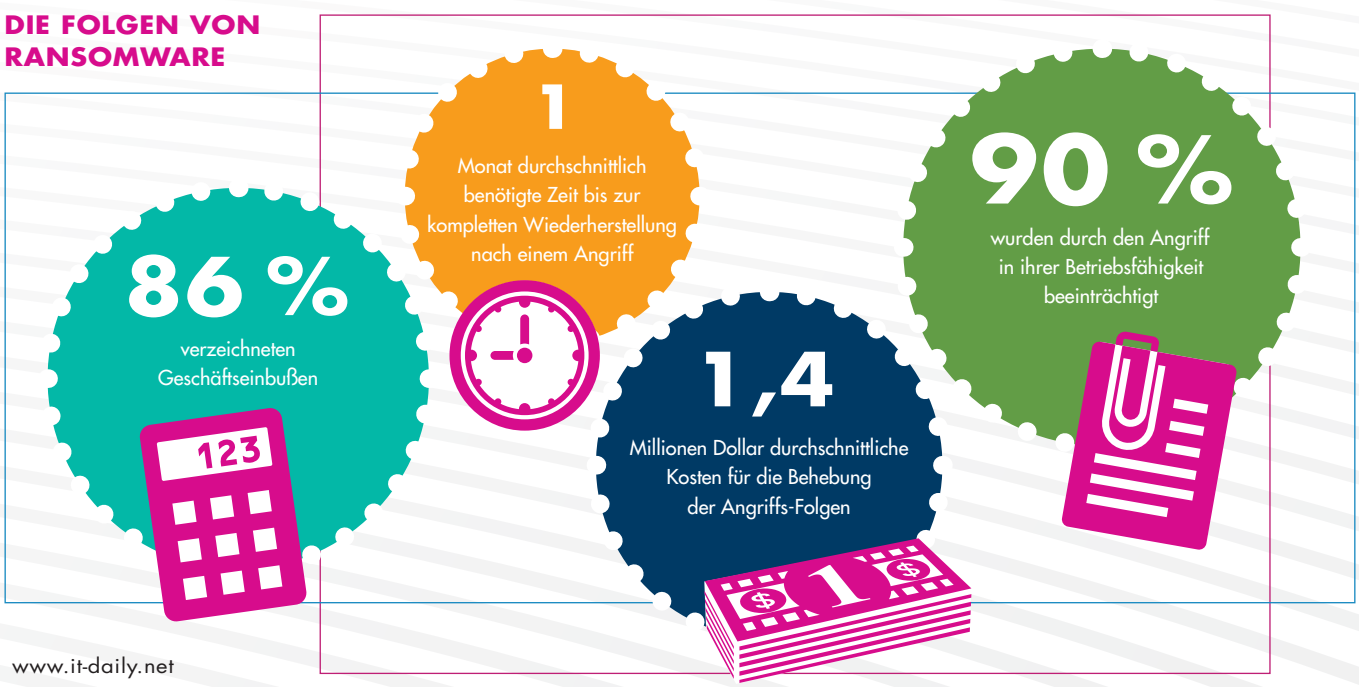
**Michael Veit:** Bei uns setzten bereits über 10.000 Unternehmen auf Sophos MDR – Tendenz stark steigend. Um dieser Nachfrage nachzukommen, haben wir große und weltweite Teams bei Sophos, die wir übrigens erst kürzlich zu einem integrierten X-Ops-Team vereint haben. Sophos X-Ops ist eine funktionsübergreifende Einheit aus SophosLabs, Sophos SecOps und Sophos AI und vereint die prädiktiven, realitätsnahen und detailliert recherchierten Bedrohungsdaten aller Teams in einem Pool.

**it security:** *Wohin geht die Reise der Security, was sind die nächsten Innovationen?*

**Michael Veit:** Der nächste entscheidende Schritt wird die prädikative Security sein. Mit Hilfe von Machine Learning und Künstlicher Intelligenz werden wir zunehmend in der Lage sein, potenzielle Cyberattacken vorauszusagen. Dafür ist noch eine ganze Strecke zu gehen, aber wir sind auf dem Weg.

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


## DIE FOLGEN VON RANSOMWARE



itsecurity

it-daily.net
Das Online-Portal von Itmanagement & itsecurity

# We secure IT

## 09.11.22 | Digitalevent

SAVE THE DATE

https://www.it-daily.net/wesecureit/


#WesecureIT2022

# INSELLÖSUNG ADE, WILLKOMMEN MODERNSTE SICHERHEITSTECHNIK

## VIESSMANN SETZT AUF SICHEREN LOGIN VON NEVIS

Seit der Gründung 1917 ist Viessmann mit Hauptsitz im hessischen Allendorf (Eder) stetig gewachsen: Das Familienunternehmen umfasst heute 22 Produktionsgesellschaften in zwölf Ländern sowie Vertriebsaktivitäten in 74 Ländern mit weltweit 120 Verkaufsniederlassungen. Diese starke internationale Vernetzung erfordert eine entsprechend leistungsfähige digitale Infrastruktur: 2017 entschied man sich bei Viessmann deshalb für die Etablierung einer unternehmensweiten Identity and Access Management (IAM)-Lösung.

Die Chancen der Digitalisierung hat die Viessmann Gruppe als international agierendes Unternehmen bereits frühzeitig erkannt: Um die Herausforderungen zu meistern, die aus neuen Marktanforderungen etwa im Bereich Internet of Things (IoT) erwachsen, wurde die Umstellung auf moderne IT-Systeme in allen Geschäftsbereichen konsequent vorangetrieben – sowohl unternehmensintern als auch im B2B- und B2C-Sektor. Als Grundvoraussetzung für das Gelingen der digitalen Transformation benötigte Viessmann zunächst ein Identity and Access Management für die gesamte Unternehmensgruppe.

Das 2017 erarbeitete Anforderungsprofil für das IAM sah vor, die IT-Profile von Endkunden, Partnern (zum Beispiel Händler, Heizungsbauer und Lieferanten) sowie Mitarbeitern zentral zu administrieren und diesen Nutzergruppen unkomplizierte Prozesse für Single Sign-on (Einmalanmeldung zur sicheren Authentifizierung an einem Arbeitsplatz für alle Rechner und Dienste) und Self-Service-Funktionalitäten (Online-Unterstüt-

zung für ein optimales webbasiertes Kundenerlebnis) bereitzustellen. Im Kern waren also folgende Ziele abzudecken:

1. Etablierung einer unternehmensweiten IAM-Lösung
2. Absicherung digitaler Kernprozesse über starke Authentifizierungsmechanismen
3. Anbindung zentraler Unternehmensanwendungen
4. Einbeziehung aller digitalen Identitäten

Nach der Zielfestlegung erfolgte im weiteren Verlauf des Jahres 2017 die Ausschreibung des Projekts. Auf die Ausschreibung reagierten auch die FSP GmbH Consulting & IT-Services mit Sitz in Köln und die mit ihr kooperierende Nevis AG – letztere damals noch unter dem Dach der AdNovum Informatik AG, aus der sie Anfang 2020 als eigenständiges Unternehmen hervorging.

## Partnerschaft für Sicherheit

Die Partnerschaft von FSP und Nevis war bereits ein Jahr zuvor zustande gekommen: 2016 hatte Nevis einen auf IAM spezialisierten Integrationspartner in Deutschland gesucht, um den Schwerpunktbereich Customer IAM & Authentifizierung im DACH-Raum weiter auszubauen. Gleichzeitig war FSP als Anbieter der webbasierten ORG Identity Governance and Administration Suite mit Schwerpunkt Autorisierung auf der Suche nach einem komplementären Lösungsanbieter. Beide Unternehmen trafen in einem Projekt bei einem gemeinsamen Kunden erstmals aufeinander. Schnell war klar, dass sich ihre Spezialisierungen gut ergänzten – es folgten die Vereinbarung einer Partnerschaft und die erste Integration von Nevis' Authentifizierungs-Lösungen durch die Consultants von FSP.

Diese gemeinsame Erfahrung kam FSP und Nevis ein Jahr darauf sehr zugute: Auch aufgrund der durchgehend positiven Resonanz ihres ersten gemeinsamen Kunden – vom Gelingen des Projekts konnten sich Vertreter von Viessmann während eines Referenzbesuchs persönlich überzeugen – gelang es den Partnern, sich in dem komplexen Ausschreibungsprozess gegen namhafte, international tätige Mitbewerber durchzusetzen und Viessmann als Kunden zu gewinnen.

Im Rahmen des von Nevis und FSP durchgeführten ausführlichen POC (Proof of Concept/Machbarkeitsnachweis) wiesen die Partnerunternehmen nach, dass die umfangreichen Anforderungen von Viessmann sowohl auf Produkt- als auch Projektseite abgedeckt werden konnten. Im Fokus stand die Kombination aus Produktfunktionalitäten (Nevis) und Kompetenz des Integrationspartners (FSP). Maßgeblich war die Fähigkeit, die Use Cases – also Anwendungsfälle, die alle denkbaren Szenarien bündeln – in der geforderten Zeit umzusetzen.

## Umfangreiche Planungen

Bereits bei der Ausarbeitung des Proof of Concept hatten die Partnerunternehmen zahlreiche Einflussfaktoren identifiziert, die bei der Umsetzung von Viessmanns Zielvorgaben Berücksichtigung finden mussten: Insbesondere waren dies die Vielzahl von Anwendungsfällen (Use Cases), Technologien, Anspruchsgruppen und speziellen Anforderungen; darüber hinaus aber auch der hohe Integrationsgrad bezüglich diverser Umsysteme – also derjenigen Anwendungen, die nicht zum eigentlichen IAM zählen, aber auf den Datenaustausch mit ihm angewiesen sind.

Hinsichtlich der Technologien standen Client-Server-Architekturen sowie web- und cloudbasierte Anwendungen im Vordergrund. Die eigentliche Herausforderung bildete hierbei die Integration der Standardsoftware und Eigenentwicklungen – bedingt durch die erhebliche Menge an Stakeholdern und die ausgeprägte Komplexität der Anforderung in den Bereichen B2B, B2C und B2E. So sollte etwa für Endkunden der Zugriff auf moderne appbasierte Anwendungen möglichst einfach erfolgen. Als Grundanforderung galt zudem Internationalität: Alle Anwendungen mussten in den jeweiligen Landessprachen der Viessmann-Niederlassungen verfügbar sein. Anhand dieses Kriterienkatalogs entwickelten FSP, Nevis und Viessmann gemeinsam einen priorisierten Projektplan.

## Erfolgreiche Umsetzung mit Zukunftspotenzial

Im Rahmen der Projektumsetzung waren zwischen drei und sieben Mitarbeiter in den Bereichen Consulting und Development im Einsatz. Hinzu kam das Integrations-Kernteam aus drei Personen, das ebenfalls fallweise flexibel auf bis zu sieben erweitert wurde. Die Integration der einzelnen Anwendungen erfolgte schrittweise entsprechend der Priorisierung im Projektplan.

SEIT DER EINFÜHRUNG UNSERES ZENTRALEN IAM-SYSTEMS ERLEBEN WIR EINE STARKE DYNAMIK AUFSEITEN DER FACHBEREICHE, DIE AUCH KURZFRISTIGE LÖSUNGEN FÜR DIE INTEGRATION IHRER ANWENDUNGEN ERWARTEN.

Sebastian Sassor,
TSO IdaaS (Technical Service Owner),
Viessmann IT Service GmbH

Aufgrund der zahlreichen unternehmensspezifischen Anforderungen von Viessmann war ein mittlerer bis hoher Grad an Customizing notwendig. Die Nevis-Architektur erlaubt ein hohes Maß solcher Anpassungen und ließ sich daher flexibel anpassen. Um die volle Bandbreite der IAM-Funktionalität auszuschöpfen, kommen nahezu alle Bestandteile der Zugriffsmanagement-Lösung Nevis Identity Suite zum Einsatz: NevisProxy, nevisAuth, nevisIDM, nevisLogrend, nevisMeta, nevisAdmin3 und nevisFido. Für die Zukunft eingeplant sind darüber hinaus nevisAdmin4 und nevisAdapt.

**IAM in der Praxis**

Wie läuft nun der Login via IAM konkret ab? Der erste Schritt zur Authentifizierung ist die sogenannte Authentisierung. Der Benutzer legt mit der Authentisierung einen Nachweis einer bestimmten Identität vor, die vom System zu verifizieren und zu bestätigen ist – bei Viessmann kommen hier neben Benutzername/Passwort auch Verfahren zur Zweifaktor-Authentisierung mittels mTAN, TAN oder Authenticator zum Einsatz.

DER STELLENWERT DES THEMAS IAM HINSICHTLICH INTEGRATION UND BETRIEB STEIGT STÄNDIG UND HAT ZU EINER ERHÖHUNG DER AKZEPTANZ BEI DEN STAKEHOLDERN GEFÜHRT.

Stephan Schweizer,
CEO, Nevis Security AG, www.nevis.net

Im Anschluss gleicht das Identity-Management der Nevis-Lösung die bei der Authentisierung vorgelegten Informationen mit den im System hinterlegten Identitätsdaten ab – dieser Prüfprozess wird als Authentifizierung bezeichnet. Ist die Identität des Users anhand der mitgeteilten Merkmale zweifelsfrei verifiziert, erfolgt im nächsten Schritt die Zuteilung der für den jeweiligen Nutzer freigegebenen Ressourcen.

Zu diesem Zweck gleicht das System die festgelegten Identitäten mit bestehenden Benutzerrechten und Einschränkungen ab und kontrolliert so den Zugriff auf die gewünschten Ressourcen. Im Zuge dieses Access Management wird den Benutzern also im Zusammenspiel mit dem Identity Management der Zugriff auf Daten, Dienste und Anwendungen erteilt oder entzogen. Ändert sich die Rolle eines Nutzers im Unternehmen, weil er beispielsweise einen neuen Verantwortungsbereich hinzugewonnen hat, lassen sich die Zugriffsberechtigungen im Access Management schnell und unkompliziert anpassen.

Hans-Christian Friedrich, Projektleiter IAM-Integration bei FSP, zieht eine positive Bilanz der IAM-Einführung: „Eine besondere Stärke von Nevis ist Flexibilität: Die Anforderungen wurden so umgesetzt, wie der Kunde sich das gewünscht hat. Es erfolgte eine Vereinfachung des gesamten Benutzermanagements, etwa bei Authentifizierung und Provisionierung. Der Benutzerkomfort wurde spürbar erhöht und die Sicherheit aller Benutzer deutlich gestärkt. Und: Die Nevis-Lösung gestattet eine flexible Weiterentwicklung, denn sie ist kein statisches Gebilde, sondern bereit für den weiteren Ausbau." Stephan Schweizer, CEO bei Nevis, ergänzt: „Der Stellenwert des Themas IAM hinsichtlich Integration und Betrieb steigt ständig und hat zu einer Erhöhung der Akzeptanz bei den Stakeholdern geführt. In der internen Anwendung wird es stärker wahrgenommen und ist inzwischen unternehmensweit bekannt. IAM gilt nunmehr als zentrale Drehscheibe für die Identitäten."

Auch für Sebastian Sassor, TSO IdaaS (Technical Service Owner) bei der Viessmann IT Service GmbH, ist das Fazit eindeutig: „Seit der Einführung unseres zentralen IAM-Systems erleben wir eine starke Dynamik aufseiten der Fachbereiche, die auch kurzfristige Lösungen für die Integration ihrer Anwendungen erwarten. Die zurückliegende Projektarbeit hat gezeigt, dass Viessmann mit der NEVIS Identity Suite als Plattform und FSP als Systemintegrator die richtige Entscheidung getroffen hat. Aufgrund der verlässlichen und zielführenden Zusammenarbeit haben wir die FSP GmbH nach der Einführungsphase mit dem Managed Service der IAM-Plattform betraut."

Die Zusammenarbeit von FSP, Nevis und Viessmann wird auch in Zukunft fortgesetzt: FSP ist seit 2020 als Managed Service Partner für den Betrieb der IAM-Plattform verantwortlich. Zuletzt wurden die weitergehenden Anforderungen im Berechtigungsmanagement – beginnend mit dem Viessmann Ordermanagementsystem – durch die Einführung und Integration des FSP-eigenen Produktes „ORG Identity Governance and Administration Suite" gelöst. Darüber hinaus ist bei der Viessmann-Unternehmensgruppe bereits ein weiteres IAM-System in China umgesetzt worden; weitere Projekte befinden sich derzeit in Planung.

***Stephan Schweizer***

# it-sa 2022

## WIEDER IM AUFWIND

**Wenn Sie sich im Vorfeld mit der it-sa beschäftigt haben, dann werden Sie festgestellt haben: mehr Aussteller, mehr Hallen. Und das wird sicher auch wieder mehr Besucher nach dem Restart im Vorjahr nach sich ziehen. Sowieso war die Bilanz 2021 schon ermutigend. Es kamen vor allem Besucher, die ein konkretes Interesse hatten, also Qualität vor Quantität. Und das überzeugte auch die Aussteller.**

**Für uns ist jedes Jahr die Verleihung der it security Awards das Highlight der it-sa. In diesem Jahr hat die Zahl der Bewerbungen für den Award stark zugenommen. Das freut uns natürlich. Schon im Vorfeld zeigt sich, es wird in den vier Kategorien Management Security, Web/Internet Security, Cloud Security und IAM ein enges Rennen. Am Ende werden kleine Details den Ausschlag geben. Über die innovativsten Produkte werden wir im Nachgang zur it-sa dann gesondert berichten, natürlich ebenso über die Gewinner der Awards.**

# THREAT INTELLIGENCE

## MEHR ALS NUR EIN BUZZWORD

Die Cyberbedrohungslandschaft verändert sich rasant und wird zunehmend komplexer. Technische Lösungen wie Endpoint-Security schützen vor unterschiedlichen Bedrohungen. Allerdings sollten diese dringend um die Komponente der menschlichen Expertise ergänzt werden. Das Buzzword der Stunde lautet Threat Intelligence (TI). Waldemar Bergstreiser, Head of Channel Germany bei Kaspersky, erklärt im Interview, welche Vorteile Threat Intelligence Unternehmen bietet und worauf sie bei der Auswahl eines Anbieters achten sollten.

**it security:** *Herr Bergstreiser, Cyberkriminelle entwickeln ihre Taktiken und Methoden stets weiter und passen sie unter anderem an aktuelle Ereignisse an. Sicherheitslösungen schaffen hier Abhilfe – oder sollten sie zumindest. Viele Anbieter bieten nun auch Threat Intelligence in ihrem Portfolio an. Worum handelt es sich dabei?*

**Waldemar Bergstreiser:** Gelegentlich wird der Begriff „Threat Intelligence" mit anderen Begriffen zusammengeworfen oder gleichgesetzt – zum Beispiel „Bedrohungsdaten". Dabei handelt es sich aber nicht um dasselbe, auch wenn es einen Zusammenhang gibt. Bedrohungsdaten sind quasi eine Liste möglicher Bedrohungen. Dagegen wird bei Threat Intelligence das Gesamtbild betrachtet: die Daten werden in einem breiteren Kontext analysiert. Auf dieser Grundlage lassen sich Entscheidungen zum weiteren Vorgehen treffen. So können Unternehmen mithilfe von Threat-Intelligence-Daten schnellere und fundiertere Sicherheitsentscheidungen fällen. Im Kampf gegen Cyberangriffe fördert TI vorausschauendes statt reaktives Verhalten, indem sie umfassende Einblicke in die Bedrohungslandschaft bietet. Das versetzt Unternehmen in die Lage, Risiken zu antizipieren. Heutzutage reicht ein reaktiver Ansatz für die Cybersicherheit einfach nicht mehr aus.

WIR HABEN ÜBER 20 JAHRE ERFAHRUNG MIT DER ENTDECKUNG UND ANALYSE VON CYBERBEDROHUNGEN UND UNSER TEAM AUS INTERNATIONALEN FORSCHERN UND ANALYSTEN IST WELTWEIT ANERKANNT.

Waldemar Bergstreiser,
Head of Channel Germany, Kaspersky,
www.kaspersky.de

**it security:** *Das klingt alles sehr technisch. Das heißt Threat Intelligence ist nur für große Unternehmen mit einer eigenen Sicherheitsabteilung geeignet?*

**Waldemar Bergstreiser:** Nein, Threat Intelligence kann jedes Unternehmen – unabhängig von der Größe – nutzen. Entweder verfügt das Unternehmen selbst über ein Sicherheitsteam, das weiß, wie es damit umgehen kann, oder man lagert Threat Intelligence über Managed-Detection-and-Response-Dienste aus. Diese Lösung bietet sich übrigens nicht nur für kleinere Unternehmen an. Threat Intelligence ist immer komplementär zur jeweiligen IT-Infrastruktur des Unternehmens. Es gibt jedoch zahlreiche unterschiedliche TI-Funktionen und eine große Vielfalt an verfügbaren Quellen und Diensten. Das macht es Unternehmen oft schwer zu verstehen, welche Lösung ihre Anforderungen abdeckt. Deshalb ist es wichtig, dass sich der Service individuell an die Bedürfnisse des Unternehmens anpassen lässt.

**it security:** *Nutzen denn Unternehmen Threat Intelligence bereits rege?*

**Waldemar Bergstreiser:** Wir haben dazu aktuelle Zahlen der Finanzbranche in

Weltweit anerkannte Bedrohungsjäger: das Global Research and Analysis Team (GReAT) von Kaspersky

Deutschland [1], die einen guten Überblick bieten. Diese Unternehmen setzen fast durchgängig auf Threat-Intelligence-Services: Insgesamt nutzen 99 Prozent mindestens einen entsprechenden Dienst. Allerdings haben nicht alle Unternehmen die Services, die sie gerne nutzen würden, auch wirklich im Einsatz. Mehr als die Hälfte gibt an, dass sich ihr Unternehmen mithilfe von Advanced Persistent Threat (APT)-Reports über die neuesten Untersuchungen, Bedrohungskampagnen und Techniken von APT-Akteuren auf dem Laufenden hält. Über ein Viertel wünscht sich den Einsatz solcher Reports. Nahezu die Hälfte greift auf Sicherheitsevaluierungen – etwa über das TIBER-Framework (Threat Intelligence-based Ethical Red Teaming) – sowie auf Tools zur Entdeckung zielgerichteter Attacken zurück. Mehr als ein Drittel (34 Prozent) ist der Auffassung, das eigene Unternehmen sollte solche technologischen Werkzeuge zukünftig einsetzen. Das Bewusstsein für die Bedeutung von Threat-Intelligence-Services scheint also in der Finanzbranche inzwischen recht hoch zu sein.

**it security:** *Was raten Sie Unternehmen, worauf sie bei der Auswahl eines Anbieters achten sollten?*

**Waldemar Bergstreiser:** Um gegen alle Bedrohungen gewappnet zu sein, müssen Unternehmen durchgehend alle Assets im Blick haben. Generell sollten sie sich für einen Anbieter entscheiden, der das System rund um die Uhr überwacht und analysiert, damit er jederzeit Schwachstellen finden und sofort entsprechende Sicherheitsmaßnahmen einleiten kann. Außerdem sollte der Anbieter stets topaktuelle Untersuchungsdaten nahezu in Echtzeit bereitstellen.

Eine qualitativ hochwertige Threat Intelligence muss sich auf ein anerkanntes Expertenteam mit nachgewiesener Erfahrung in der Aufdeckung komplexer Bedrohungen stützen und sich reibungslos in die bestehenden Sicherheitsabläufe des Unternehmens integrieren können. Denn eine gute Threat Intelligence entlastet interne Cybersecurity-Abteilungen durch umfassende Automatisierungsmöglichkeiten; so können sich diese auf vorrangigere Ziele konzentrieren.

**it security:** *Kaspersky bietet ja auch entsprechende Threat-Intelligence-Dienste an, die auf jahrelanger Erfahrung beruhen …*

**Waldemar Bergstreiser:** Genau, die Threat Intelligence von Kaspersky bietet Zugriff auf alle Informationen, die zur Abwehr von Cyberbedrohungen benötigt werden. Wir haben über 20 Jahre Erfahrung mit der Entdeckung und Analyse von Cyberbedrohungen und unser Team aus internationalen Forschern und Analysten ist weltweit anerkannt. Mit Kaspersky Threat Intelligence [2] erhalten Unternehmen einen direkten Zugang zu technischer, taktischer, operativer und strategischer Threat Intelligence. Zum Kaspersky-Portfolio gehören unter anderem Threat Data Feeds, die Threat-Intelligence-Plattform CyberTrace, Threat Lookup, Threat Analysis mit einer Cloud Sandbox und Cloud Threat Attribution Engine sowie eine Reihe an Threat-Intelligence-Berichtsoptionen. Besonders interessant für Spezialisten sind unsere APT & Crimeware Reportings. Zusätzlich bieten wir den Service „Ask the Analyst", sodass sie bei Bedarf Experten von Kaspersky direkt um Rat fragen können. Sehr stolz sind wir zudem auf die jüngste Kooperation zwischen Kaspersky und Microsoft, durch die unsere Threat Data Feeds jetzt in Microsoft Sentinel integriert sind.

**INFOBOX**

Derzeit bietet Kaspersky Unternehmen unter dem Shortlink **kas.pr/threat-intelligence** einen für sie kostenfreien Zugang zu den Threat-Intelligence-Services. Der Zugang wird zunächst für einen Monat gewährt.

**it security:** *… allerdings warnt das BSI vor dem Einsatz der Produkte. Was sagen Sie dazu?*

**Waldemar Bergstreiser:** Die BSI-Warnung bezieht sich „nur" auf unsere Virenschutzprodukte und nicht auf die Threat-Intelligence-Dienste von Kaspersky. Und: wie eine Recherche des Bayerischen Rundfunks und Spiegel zeigen, spielten technische Argumente und Fakten keine Rolle bei der Warnung durch das BSI. Kaspersky hat dem BSI seit Februar umfangreiche Informationsangebote gemacht und es zu Tests und Audits eingeladen. Es ist unser Ziel, den langjährigen konstruktiven Dialog mit dem BSI fortzusetzen, um gemeinsam auf der Basis faktenbasierter Bewertungen für ein Höchstmaß an Cybersicherheit für die deutschen und europäischen Bürger sowie Unternehmen einzutreten.

**it security:** *Herr Bergstreiser, wir danken für das Gespräch.*


Quellen:
[1] https://kas.pr/h2ia
[2] https://www.kaspersky.de/enterprise-security/threat-intelligence


# CYBER RESILIENCE ACT

## WICHTIGER SCHRITT FÜR MEHR CYBERSICHERHEIT

Mit dem Cyber Resilience Act geht die EU-Kommission die notwendige Aufgabe an, Produktanforderungen an Cybersicherheit zu vereinheitlichen und das Resilienzniveau in der EU anzuheben. „Diese Regulierung wird alle digitalen Produkte im europäischen Binnenmarkt betreffen. Auch wenn es unsere Unternehmen vor enorme Herausforderungen stellt, braucht der europäische Binnenmarkt ein solches harmonisiertes Level-Playing-Field in der Cybersicherheit", so Wolfgang Weber, Vorsitzender der ZVEI-Geschäftsführung. Der vorgelegte Entwurf sei ein wichtiger Schritt.

Kritisch sieht der ZVEI allerdings die weitgefasste Definition bei sogenannten „critical products" und „highly critical products", zu denen beispielsweise auch Mikrocontroller, industrielle Automatisierungs- und Steuerungssysteme oder Teile des Industrial Internet of Things gezählt werden, auch wenn sie in keinem kritischen Kontext verwendet werden. „Wenn Unternehmen solche oder darauf aufbauende Produkte auf Basis dieser Einteilung nur erschwert auf den Markt bringen können, wird es zu großen Verzögerungen in der EU beim Einsatz digitaler Produkte und Komponenten kommen", so Weber. Statt reine Hochrisikolisten zu führen, müsse deshalb das Konzept des vorgesehenen Verwendungszwecks im Vordergrund stehen. Zudem müssen Hersteller digitaler Produkte und Komponenten bei der Zuweisung der Kritikalität essenziell eingebunden werden, da sie potenzielle Sicherheitsrisiken am besten beurteilen und entsprechende Maßnahmen einleiten können.

Positiv bewertet der Verband der Elektro- und Digitalindustrie, dass der Regulierungsentwurf den Prinzipien des New Legislative Framework (NLF) folgt. Weber: „Diese Vorgehensweise knüpft unmittelbar an etablierte Prozesse in den Unternehmen, unter anderem zur Konformitätsbewertung, an und stärkt die Rolle der europäischen Normung." Allerdings ist die vorgesehene Übergangsfrist von 24 Monaten zur Umsetzung solcher Maßnahmen deutlich zu kurz und muss verlängert werden. Die akuten Schwierigkeiten bei der Anwendung der Medical Device Regulation zeigen, wie viel Zeit nötig ist, um alle Produkte bis zum Stichtag einer umfangreichen Konformitätsbewertung zu unterziehen. Die Europäische Kommission sollte hier deshalb längere Fristen setzen, damit harmonisierte Normen rechtzeitig gelistet und eine ausreichende Zahl an Drittstellen zur Konformitätsbewertung benannt werden kann.

Der ZVEI setzt sich bereits seit Jahren aktiv für eine horizontale Regulierung ein, die die Cybersicherheitsanforderungen für Produkte adressiert. Vom Hersteller bis zum Anwender müssen alle Beteiligten im Wertschöpfungsnetzwerk zusammenarbeiten und ihren Teil erfüllen, um ein hohes Niveau an Cyberresilienz zu erreichen. Dafür müssen die Anforderungen an die einzelnen Beteiligten, insbesondere für Hersteller von Hard- und Software, im Lebenszyklus auch künftig klar abgrenzbar bleiben.

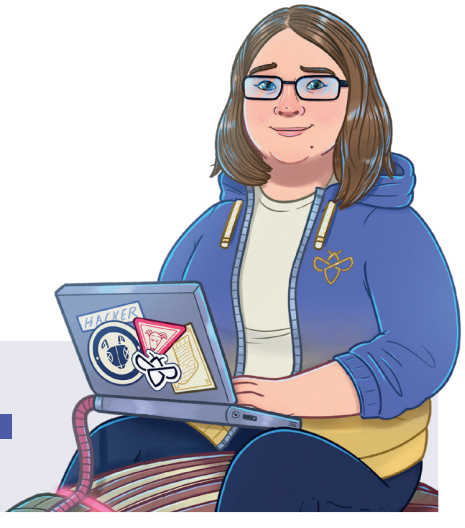
***www.zvei.org***

# Testen Sie Ihr Wissen über Hacker/-innen-Communities mit Intigriti

Bei Intigriti, Europas führender Plattform für ethisches Hacking und die Aufdeckung von Schwachstellen, sind mehr als 50.000 ethische Hacker/-innen registriert. Aber wer sind diese Menschen? Und wie können sie Unternehmen dabei helfen, ihre Cybersicherheitsvorkehrungen zu verbessern? Testen Sie Ihr Wissen mit dem folgenden Quiz.

Sie sind sich bei Ihren Antworten sicher? Scannen Sie für **kostenlose Geschenke** bei der **IT-SA 2022** einfach den QR-Code, reichen Sie Ihre Antworten ein und besuchen Sie unseren **Stand 6-111**. Außerdem nehmen alle Einsendungen an einer Verlosung eines **Rucksacks mit belgischen Leckereien teil!**

## Take the quiz


Brauchen Sie Hilfe bei der Beantwortung der Fragen?
Wir haben einen Hack dafür! Besuchen Sie den Stand **6-111** von Intigriti für die Antworten auf Ihre Fragen. **Viel Glück!**

INTIGRITI

Agile Sicherheitstests mit der Power der Community

# SEPPMAIL.CLOUD

## DIE LOGISCHE ANTWORT AUF DEN STEIGENDEN TREND ZUR E-MAIL-NUTZUNG

Nach wie vor sind E-Mails das Hauptkommunikationsmittel in Unternehmen. Aber nicht zuletzt deswegen war es für den E-Mail Security-Hersteller SEPPmail ein großes Anliegen, seine Services auch als Cloud-Lösung anbieten zu können. Günter Esch, Geschäftsführer der SEPPmail – Deutschland GmbH, erklärt im Interview die logische Entwicklung zur neuen SEPPmail.cloud und deren Merkmale.

**it security:** *SEPPmail hat vergangenes Jahr seinen 20. Geburtstag gefeiert. Erzählen Sie etwas über die Geschichte des Unternehmens!*

**Günter Esch:** Seit Beginn unserer Geschichte steht SEPPmail für eine sichere E-Mail-Kommunikation. Nachdem unser Gründer Stefan Klein im Jahr 2001 eine Software zur E-Mail-Verschlüsselung entwickelt hatte, wurde der elektronische Austausch verschlüsselter Daten zu einem wegweisenden Projekt für uns. Als kleines Start-up namens Onaras haben wir also damit begonnen, das Thema E-Mail-Verschlüsselung voranzutreiben. Nach der internationalen Patentierung unseres revolutionären GINA-Verfahrens, das eine spontane verschlüsselte E-Mail-Kommunikation ermöglicht, erhielten wir 2008 schließlich unseren heutigen Namen. Seitdem bauen wir unsere Aktivitäten in den Kernländern Schweiz, Deutschland und Österreich sowie darüber hinaus immer weiter aus. So wurde 2015 die SEPPmail – Deutschland GmbH gegründet, 2016 eröffneten wir ein Support- und Entwicklungsbüro in Leipzig, im Oktober 2021 folgte die neue Vertriebsniederlassung in Aschaffenburg. Seit Anbeginn agiert der Vertrieb aus dem eigenen Home-Office verteilt über Deutschland. So stehen wir unseren Kunden und Partnern im gesamten deutschen Raum direkt und unmittelbar zur Seite.

**it security:** *Welche Produkte hat SEPPmail neben der E-Mail-Verschlüsselung auf den Markt gebracht und was ist die neueste Entwicklung?*

**Günter Esch:** Das populärste Produkt dürfte unser Secure E-Mail Gateway sein. Dieses enthält zusätzlich zu den verschiedenen Verschlüsselungsfunktionen gleich auch digitale Signaturen. Diese dienen als ein elektronisches Siegel, mit dem der Absender beweisen kann, dass die versendete Nachricht auch wirklich von ihm stammt. Um solche Signaturen zu erhalten, müssen Zertifikate bei akkreditierten Zertifizierungsstellen beantragt werden. Dieser Prozess wird von dem Gateway automatisch übernommen.

Darüber hinaus gewährleistet unser Produkt Large File Transfer auch ein sicheres Versenden übergroßer Dateien. Mit dem Central Disclaimer Management sorgen wir für ein einheitliches, unternehmensspezifisches Erscheinungsbild der Mails unserer Kunden.

Was wir im Moment aber am stärksten fokussieren, ist unsere neueste Entwicklung: die SEPPmail.cloud. Nicht nur, dass wir unser bekanntes Lösungsportfolio aus der Cloud heraus anbieten, sondern wir erweitern dieses um einen wesentlichen Teil: den E-Mail-Filter! Ein Meilenstein in unserer über 20-jährigen Firmengeschichte.

**it security:** *Wie kam es dazu, dass Sie gerade jetzt die SEPPmail.cloud entwickelt haben?*

**Günter Esch:** Das war ein logischer Schritt. Derzeit herrscht in vielen Firmen ein allgemeiner Ressourcenmangel. Zum einen fehlen Mitarbeiter, zum anderen hat das vorhandene Personal kaum noch freie Kapazitäten übrig.

Darum werden von den Unternehmen verstärkt Standardlösungen in die Cloud verschoben. Die Vorteile liegen auf der Hand: Es werden keine physischen Ressourcen wie Hardware oder virtuelle Kapazitäten benötigt. Das Management dieser fällt also auch weg. Eine hohe Verfügbarkeit ist durch den Cloud-Betrieb gegeben. Das verbleibende Management wird über ein zentrales Dashboard, über das sich alle Services zentral und einfach verwalten lassen, gewährleistet. Und weil Cloud-Lösungen zusätzlich auch noch relativ kostengünstig und viel flexibler sind,

> WEIL CLOUD-LÖSUNGEN AUCH RELATIV KOSTENGÜNSTIG UND VIEL FLEXIBLER SIND, WERDEN SIE IMMER BELIEBTER UND SIND AUCH FÜR KLEINERE UNTERNEHMEN GEEIGNET.
>
> Günter Esch, Geschäftsführer, SEPPmail – Deutschland GmbH, www.seppmail.com/de

werden sie immer beliebter und sind auch für kleinere Unternehmen geeignet.

Umfragen haben gezeigt, dass sich deutsche Systemintegratoren heutzutage bis zu 80 Prozent mit Cloud-Beratung im Tagesgeschäft beschäftigen.

**it security:** *Warum nun auch noch E-Mail-Filter? Was zeichnet diesen Service im Vergleich zu anderen aus?*

**Günter Esch:** Wir hatten letztes Jahr das Glück, eine Gruppe von sehr erfahrenen Cloud-Spezialisten an Board nehmen zu können. Diese haben seit zehn Jahren einen Premiumservice für E-Mail-Filter entwickelt und betreut. Da haben wir die Gelegenheit beim Schopf gepackt und nun, ein Jahr später, können wir mit beeindruckenden Zahlen belegen, dass wir von Null an in der Premier League gelandet sind.

Die SEPPmail.cloud bietet zusätzlich zu den bekannten Signatur- und Verschlüsselungsfunktionalitäten Filterfunktionen gegen Spam, Phishing sowie Malware aller Art und überzeugt dabei mit einer maximalen Erkennungsrate. Zur zielgenauen Abwehr fortgeschrittener Angriffe wie Spear-Phishing oder CEO-Fraud können die Filterregeln ganz nach den eigenen Wünschen eingestellt werden. Die hohe Leistung der Erkennungsrate wurde durch den VBSpam-Test im Juni 2022 bestätigt: bei 400.000 Mails keine falsch-negativen Ergebnisse im Malware-Set, nur zwei übersehene Phishing-Samples und eine fast 100-prozentige Spam-Erkennungsrate mit nur 18 übersehenen Spam-Samples.

Unsere SEPPmail.cloud wird in hochverfügbaren Rechenzentren in der Schweiz und in Deutschland betrieben. Somit stellen wir eine gefordert hohe Verfügbarkeit der Services sicher. Gleichzeitig ist die Lösung zu 100 Prozent mit allen europäischen Datenschutz- sowie Sicherheitsstandards konform.

Die Installation und Verwaltung der SEPPmail.cloud ist über ein einziges Portal sehr intuitiv und einfach. Unsere Kunden erhalten mit SEPPmail.cloud eine umfassende E-Mail-Sicherheit – alles aus einer Hand, mit der gewohnten Qualität bei Funktionalität, Service und Support.

**it security:** *Ändert SEPPmail durch die Cloud seine Go-to-Market-Strategie?*

**Günter Esch:** Uns liegen die Beziehungen zu unseren Partnern weiterhin sehr am Herzen, und wir wollen mit der SEPPmail.cloud unseren Partnern nur ein zusätzliches Produkt an die Hand geben. Daher ändert sich also an unserer Go-to-Market-Strategie nichts. Unsere Partner und Kunden können je nach Bedürfnis zwischen on premises Hardware oder VM, Kauf oder Miete, vom Partner angebotenem Managed Service (MSP) oder eben nun neu auch aus der Cloud wählen.

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

# CYBERSICHERHEIT IN ZAHLEN

## IT-SICHERHEITSGEFÜHL IN DEUTSCHLAND HAT ABGENOMMEN

Die aktuelle Studie „Cybersicherheit in Zahlen" von G DATA CyberDefense und Statista belegt: Die Corona-Pandemie und der Ukraine-Konflikt haben auch bei der IT-Sicherheit Spuren hinterlassen. Der G DATA Index Cybersicherheit ist innerhalb eines Jahres um zwei Prozent zurückgegangen. Das heißt: Die gefühlte IT-Sicherheit in Deutschland hat abgenommen. Insbesondere beim Fachwissen und dem Sicherheitsgefühl sind die Indexwerte gesunken. Gleichzeitig ist das Risikoempfinden zurückgegangen.

Im beruflichen Umfeld schätzt ein Drittel der Befragten das Risiko als hoch oder sehr hoch ein, Cyberkriminalität zum Opfer zu fallen. Im privaten Umfeld liegt der Anteil sogar noch höher – bei 38 Prozent. Ein möglicher Grund: Es fehlt vielen Menschen an den Kompetenzen, um sich und ihre digitalen Geräte entsprechend zu schützen.

„Über viele Jahre war Cybersicherheit vor allem ein Thema für die IT-Abteilung, mit dem das Management sich höchstens punktuell beschäftigen wollte. Das war und ist eine Fehleinschätzung", sagt Andreas Lüning, Mitgründer und Vorstand von G DATA CyberDefense. „IT-Sicherheit mag mit der Technik beginnen. Aber dort ist lange noch nicht Schluss. Gerade Führungskräfte müssen eine gute Fehlerkultur vorleben und Mitarbeitende ermutigen auch Fehler, welche die Sicherheit gefährden können, zu melden."

### Große Personalnot bei IT-Sicherheit

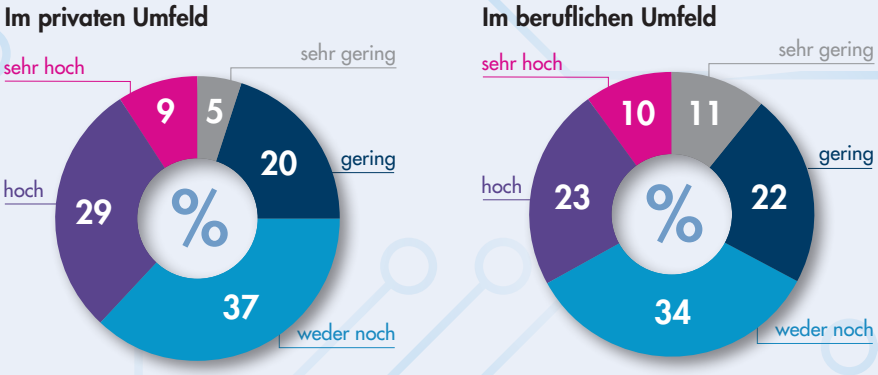
Bereits zum zweiten Mal hat Statista im Auftrag von G DATA eine repräsentative Studie zum Stand der IT-Sicherheit in Deutschland geführt. Mehr als 5.000 Arbeitnehmer wurden im beruflichen und privaten Kontext befragt.

Die Umfrage zeigt, wie groß der Personalmangel in der IT ist: Insgesamt klagen 36 Prozent der Befragten über fehlende Mitarbeitende im IT-Bereich. Weitaus dramatischer ist die Lage bei kleinen Firmen. In Unternehmen mit weniger als 50 Angestellten sprechen mehr als zwei Drittel der Umfrageteilnehmer von fehlendem Personal. Daher überrascht es auch nicht, dass Mitarbeitende für IT generell händeringend gesucht werden – gerade für den Bereich der IT-Sicherheit. Mehr als 44 Prozent der Befragten aus großen Unternehmen haben hier den größten Handlungsbedarf.

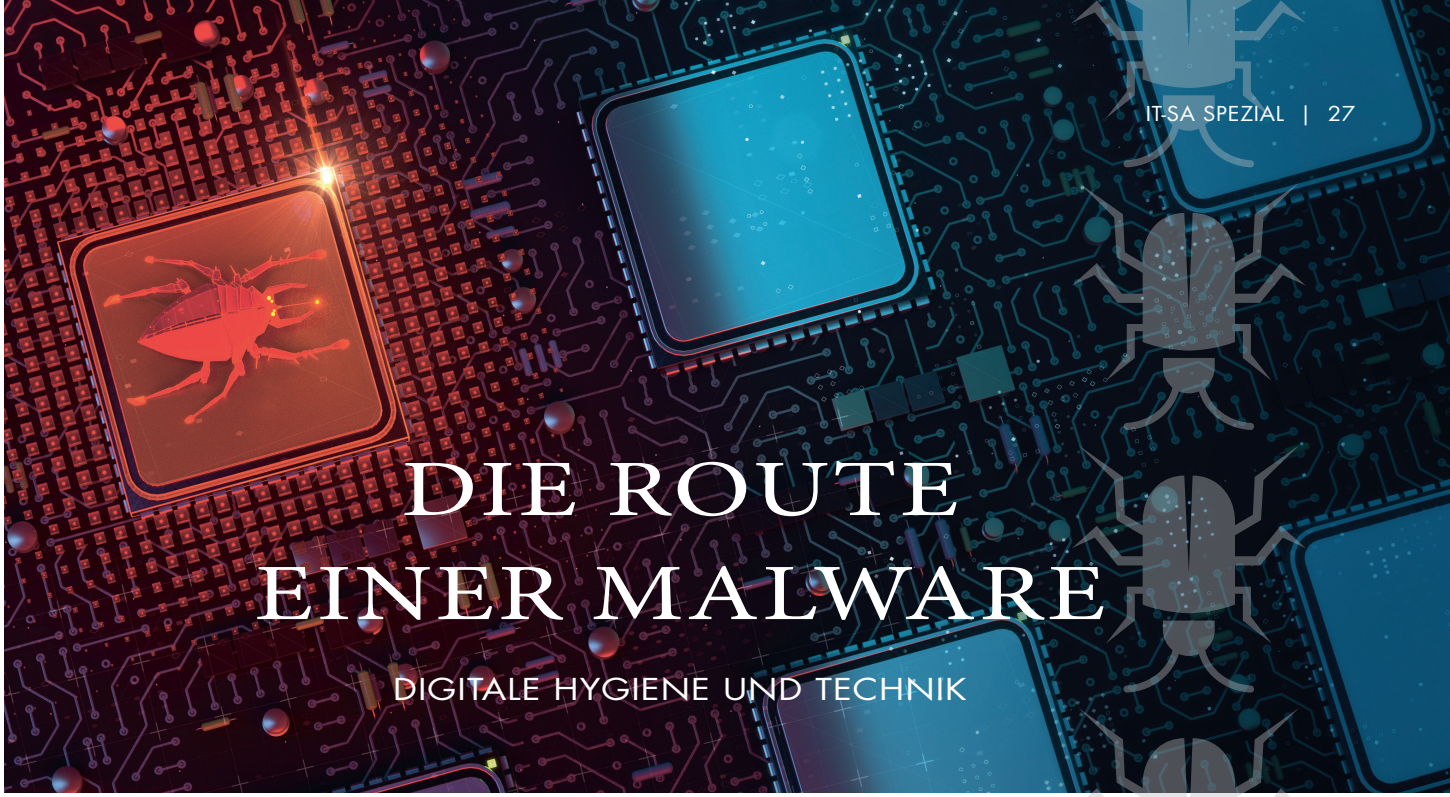
„Die Studie von G DATA und Statista zeigt, dass es keine hundertprozentige IT-Sicherheit gibt. Wir sollten den Angreifern nicht mehr Angriffsflächen bieten als unbedingt nötig", sagt Robin Rehfeldt, Senior Analyst bei Statista. „In der zweiten Ausgabe von ‚Cybersicherheit in Zahlen' nehmen wir Unternehmen und Organisationen in den Fokus, schauen auf Systeme, Strukturen oder auf Prozesse. Und fragen: Wie können und müssen sich Firmen in einer gefährlicher werdenden Welt aufstellen? Wie funktioniert Sicherheit – für die Institution, die Führung, die Mitarbeitenden?"

***www.gdata.de***

**WIE HOCH SCHÄTZEN SIE DAS RISIKO EIN, OPFER VON CYBERKRIMINALITÄT ODER DATENKLAU ZU WERDEN?**




(Quelle: G Data CyberDefense 2022)



# DIE ROUTE EINER MALWARE

## DIGITALE HYGIENE UND TECHNIK

Malware nutzt zahlreiche Vektoren, um ihr Ziel zu erreichen. Die Gesamtheit dieser Faktoren wird öfter als Angriffsfläche bezeichnet, deren tatsächliche Breite den Cyberkriminellen einen gewissen Spielraum eröffnet.

Unter den zahlreichen Methoden einer Malware stechen einige Hauptinfektionsvektoren hervor, darunter E-Mails, gefälschte Websites oder in legitime Play- und App-Stores oder gar Update-Server von Softwareherstellern hinterlegte manipulierte Anwendungen (Beispiel SolarWinds' Sunburst). Doch die Bedrohung geht nicht nur von der reinen Software-Dimension aus, auch physische Datenträger können zu Infektionsvektoren werden. Faxgeräte, Drucker, Computermäuse, USB-Sticks oder auch USB- und Lightning-Kabel werden regelmäßig als Vektoren ausgenutzt. Anfang 2022 wurde sogar ein Rootkit entdeckt, das im SPI-Flash-Chip eines Computer-Mainboards versteckt war.

Nach dem Herunterladen installiert sich die klassische Malware in temporäre Ordner, die von Anwendungsdaten bis hin zu Browser-Caches reichen. Anschließend wird der bösartige Code ausgelesen und das Skript ausgeführt. Spuren der Installation von Malware sind manchmal auch in der Windows-Registrierung zu finden. Bei der „dateilosen" Malware hingegen wird gar keine Datei gespeichert, demnach gibt es keine feststellbare Spur: Der Schadcode wird direkt aus dem RAM ausgeführt. Einmal infiziert, gibt es auch nur zum Teil offensichtliche Hinweise auf eine Infektion (langsameres Betriebssystem, plötzlich auftretende Bluescreens). Viele Signale sind eher am verdächtigen Verhalten des Systems einer Arbeitsstation mittels EPP- und EDR-Lösungen zu erkennen.

### Die Mischung macht's

Noch bevor man an den Schutz des Endgerätes denkt, sind den Anwendern Basiskenntnisse in digitaler Hygiene zu übermitteln. Denn die Unachtsamkeit des Benutzers erleichtert leider in den meisten Fällen die Arbeit der Cyberkriminellen. Zusätzlich zu einem guten Grad an Wachsamkeit sind die regelmäßige Aktualisierung des Betriebssystems und des Browsers sowie die Änderung der Passwörter eine erste Stufe des Schutzes gegen Malware und Angriffe.

Parallel dazu gibt es technische Lösungen, die vor Malware schützen. Auf der Datenfluss-Ebene im Netzwerk sind Lösungen zur Erkennung von Eindringlingen und E-Mail-Filter bewährte Verfahren. Sie analysieren und entfernen Links und gefährliche Anhänge. Was Desktops, Notebooks und Server betrifft, sorgen EPP- und EDR-Lösungen (idealerweise HIPS – „Host Intrusion Prevention Systems") für Verhaltensschutz und/oder Gerätekontrolle: Das Verschließen von USB-Ports an Computern ist keine Notwendigkeit mehr, um Malware abzuwehren, die über physische Vektoren übertragen wird. Dafür sind EPP-Funktionen da, die raffinierteste Angriffe abwehren, noch bevor EDR-Lösungen Elemente für weitere Analysen liefern.

Wenn die Infektion dennoch erfolgreich ausbricht, ist es sinnvoll, die Verbindung des befallenen Rechners zum Unternehmensnetzwerk und zum Internet zu trennen, um die Beseitigung der Malware vorzunehmen. Dabei sollte man darauf achten, nicht nur die bösartige Datei, sondern auch temporäre Dateien sowie Persistenz-Mechanismen wie Register-Schlüssel zu löschen. Herkömmliche Antivirenprogramme können zudem bestimmte Schadprogramme unter Quarantäne stellen oder löschen – vorausgesetzt, sie werden als solche erkannt. Nur in den komplizierteren Fällen muss eine komplette Neuinstallation des Systems durchgeführt werden. Die Änderung von Kennwörtern sowie die Aktualisierung von Software und Betriebssystem sind ebenfalls unumgängliche Maßnahmen, um eine sofortige Neuinfektion zu vermeiden.

***www.stormshield.com***

# VERLUST KRITISCHER DATEN

## PROBLEM FÜR VIELE UNTERNEHMEN

Arcserve gibt die wichtigsten Ergebnisse seiner jährlichen unabhängigen globalen Forschungsstudie bekannt. Die Studie bestätigt, dass der Verlust kritischer Daten weiterhin ein Problem für Unternehmen darstellt. In der Studie bei IT-Entscheidungsträgern (ITDMs) berichteten 75 Prozent der Befragten in Deutschland, dass sie in ihrem Unternehmen kritische Daten nach einem schwerwiegenden Verlust wiederherstellen mussten. Davon erlitten 52 Prozent der deutschen Unternehmen einen dauerhaften Verlust entweder von Teilen oder von allen Daten. Daten sind ein unbezahlbares Gut. Diese Ergebnisse unterstreichen, wie wichtig es ist, mit einem robusten Datensicherungs- und Wiederherstellungsplan, bei dem die Datenintegrität im Mittelpunkt steht, die Widerstandsfähigkeit der Datenverfügbarkeit zu steigern, um schwerwiegende Geschäftsunterbrechungen zu verhindern.

**Problem Business Continuity**

Die Studie ergab auch, dass viele Unternehmen nicht in der Lage sind, die Geschäftskontinuität aufrechtzuerhalten, wenn Daten verloren gehen oder gefährdet sind. Die schnelle Wiederherstellung von Daten ist für Unternehmen von entscheidender Bedeutung, insbesondere in einem Business, in dem Daten immer zur Verfügung stehen müssen.

79 Prozent der in Deutschland befragten Unternehmen finden, dass eine Ausfallzeit von 12 Stunden oder weniger für kritische Systeme akzeptabel ist – erst dann kommt es zu messbaren negativen Auswirkungen auf das Business. Dennoch wären nur 52 Prozent in der Lage, einen schwerwiegenden Datenverlust innerhalb von 12 Stunden oder weniger zu beheben.

25 Prozent der in Deutschland befragten Unternehmen konnten ihre Daten erst nach einem Tag oder länger wiederherstellen.

**Disaster Recovery**

Die Ergebnisse der Studie zeigen auch, dass ein neuer Ansatz für die Notfallwiederherstellung erforderlich ist. Unternehmen sind angehalten, ihren Disaster-Recovery-Plan kontinuierlich zu aktualisieren, zu testen und zu dokumentieren, um die Widerstandsfähigkeit ihrer Datenverfügbarkeit zu erhöhen. Die Bedeutung des Schutzes und der Wiederherstellung von Daten sollten auch auf allen Unternehmensebenen mit spezifischen Zielen priorisiert werden.

In Deutschland gaben 90 Prozent der Befragten an, dass ihr Unternehmen über einen Notfallwiederherstellungsplan verfügt. Allerdings haben nur 20 Prozent einen ausgereiften Plan, der gut dokumentiert, getestet und aktualisiert wird.

87 Prozent der in Deutschland Befragten gaben an, dass ihr Unternehmen die Ausfallsicherheit von Daten in die Strategie einbezieht. Dennoch haben nur 22 Prozent einen ausgereiften Ansatz mit entsprechenden Zielen, um den Fortschritt zu verfolgen.

**Strategien implementieren**

„Unsere jährliche Umfrage unterstreicht die geschäftliche Notwendigkeit für Unternehmen, eine Strategie zur Datensicherheit zu implementieren, die ausgereifte Pläne zur Datensicherung und -wiederherstellung beinhaltet. Wir leben in einer Welt mit zunehmenden Ransomware-Angriffen und häufigen Naturkatastrophen. Jede Ausfallzeit aufgrund von Datenverlusten kann für ein Unternehmen verheerende Folgen haben – von Umsatzeinbußen bis hin zum Verlust von Kunden“, sagt Florian Malecki, Executive Vice President, Marketing bei Arcserve.

***www.arcserve.com***

STORMSHIELD

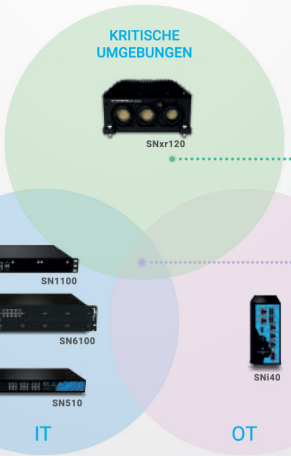
Die europäische Wahl für Cybersicherheit

# Absicherung von **kritischen** und **operativen Infrastrukturen**

SNxr**1200**
**Gehärteter Schutz** für kritische Umgebungen

SN**1100**
Leistungsfähigkeit und Resilienz für **komplexe Infrastrukturen**

**STORMSHIELD DATA SECURITY** (SDS)
Schutz **sensibler Daten**




**STORMSHIELD ENDPOINT SECURITY** (SES)
Schutz von **Endgeräten** und **Servern**

SN**i40**
SN**i20**
Angepasster Schutz für **industrielle Umgebungen**

**www.stormshield.com**

# TRENDS DER IT-SECURITY

## VON ZERO TRUST BIS MADE IN EU



Auf der Sicherheitsmesse it-sa stehen für gewöhnlich die technischen Neuentwicklungen im Kampf gegen Cyberkriminalität im Vordergrund. Doch in diesem Jahr bestimmen andere Faktoren den Takt. Die Auswahl der passenden Security-Philosophie steht ebenso im Vordergrund wie die Herkunft der Hersteller. Mehr denn je ist IT-Security Vertrauenssache. Thorsten Urbanski vom IT-Sicherheitsspezialisten ESET erläutert, was sich im Detail dahinter verbirgt.

**Trend 1:**

**Endpoint Detection and Response rückt immer mehr ins Rampenlicht – was steckt eigentlich dahinter?**

Erfolgreiche Cyberangriffe auf Unternehmen erfolgen in den seltensten Fällen „Knall auf Fall", sondern sind das Resultat längerer und vor allem aufwendiger Vorbereitungen auf Seiten der Angreifer. Je besser das anzugreifende Netzwerk jedoch abgesichert ist, desto intensiver müssen Cyberkriminelle nach Schwachstellen suchen. Das bedeutet für sie, vorab geeignete Wege finden zu müssen, um in der Zielorganisation eine Basis für einen Angriff schaffen zu können. Insbesondere, wenn Advanced Persistent Threats und Zero-Day-Exploits ins Spiel kommen, stoßen jedoch klassische Sicherheitsprodukte an ihre Grenzen. Diese Gefahren können selten direkt, wie beispielsweise Malware, erkannt werden, verraten sich aber über ihre spätere Arbeitsweise im Netzwerk.

Abhilfe schaffen Endpoint Detection and Response Lösungen, die das Schutzniveau deutlich erhöhen und IT-Security-Verantwortlichen eine umfassende Innenansicht ihres Netzwerkes ermöglichen. Aber was bedeutet Detection und Response eigentlich in der Praxis? Zum einen soll damit der Endpoint geschützt werden („Detection"), auf dem die meisten Hacker-Aktivitäten stattfinden. Dort liegt ein Großteil der schutzwürdigen Daten vor bzw. werden am Gerät zum Beispiel Passwörter oder Bankdaten eingegeben. Zum anderen beschreibt „Response", dass auf Anomalien sofort reagiert werden kann. Je nachdem kann das eine manuelle Reaktion eines IT-Sicherheitsexperten oder eine automatische, zuvor definierte Verhaltensweise sein.

Und genau auf diese Veränderungen an Dateien, Protokollen und ausgeführten Diensten springen die EDR-Lösungen beinahe in Echtzeit an – und können sofort überprüft werden. Zudem bieten sie eine weitere wichtige Einsatzmöglichkeit: Anhand von EDR können nach einer Cyberattacke forensische Untersuchungen eingeleitet werden. Ähnlich einem Mordfall in bekannten Krimis werden möglichst viele Informationen gesammelt und „Alibis", in diesen Fällen die ordnungsgemäßen Arbeitsweisen, überprüft. Administratoren erkennen dann zuverlässig, wie der Angriff ablief, welche Schwachstellen konkret ausgenutzt und welche Veränderungen im Netzwerk vorgenommen wurden. Dazu kann der Verantwortliche auf Informationen des Reputationssystems (wie etwa ESET LiveGrid) zurückgreifen und/ oder anhand des MITRE ATT&CK Frameworks die Attacke nachvollziehen.

**Trend 2:**

**EDR und Zero Trust werden oft in einem Atemzug genannt. Was verbindet die beiden Trendthemen?**

Hinter Zero Trust steht die Idee einer konzeptionellen Leitlinie für alle IT-Security-Maßnahmen, die auf Vorsicht und Skepsis beruht. Es handelt sich also nicht um eine Blaupause für ein IT-Sicherheitssystem oder eine technisch ausgefeilte Security-Lösung. Laut Forrester beruht die Prämisse von Zero Trust darauf, keiner Entität zu vertrauen, weder intern noch extern. Mit anderen Worten: „Vertraue nie, überprüfe immer". Experten beschreiben Zero Trust als ein perimeterloses Modell. Dieses muss ständig aktualisiert werden, um Daten, Software und andere Anwendungen unabhängig von Nutzern, Standort oder Geräteart zu schützen. Ein wichtiger Bestandteil von Zero Trust ist dabei die kritische Sicht nach innen. Also, wer macht was und darf er das. Womit wir dann wieder beim Thema EDR wären.

Wir haben ein Reifegradmodell entwickelt, das die unterschiedlichen Stufen und Maßnahmen von Zero Trust an-

schaulich darstellt. Unser Ansatz besteht aus einer dreistufigen Pyramide. Je höher die Stufe ist, desto sicherer ist die Schutzwirkung – also „reifer". Das Modell startet mit der Basisstufe „Grundschutz Plus", die dem Prinzip des „Multi Secured Endpoint" folgt. Diese eignet sich unabhängig vom individuellen Schutzbedarf für jede Organisation und sollte die Mindestanforderung jeder IT-Abteilung abbilden. Daran schließen sich zwei Zero Trust-Stufen mit weiter steigenden Security-Maßnahmen und -Diensten an.

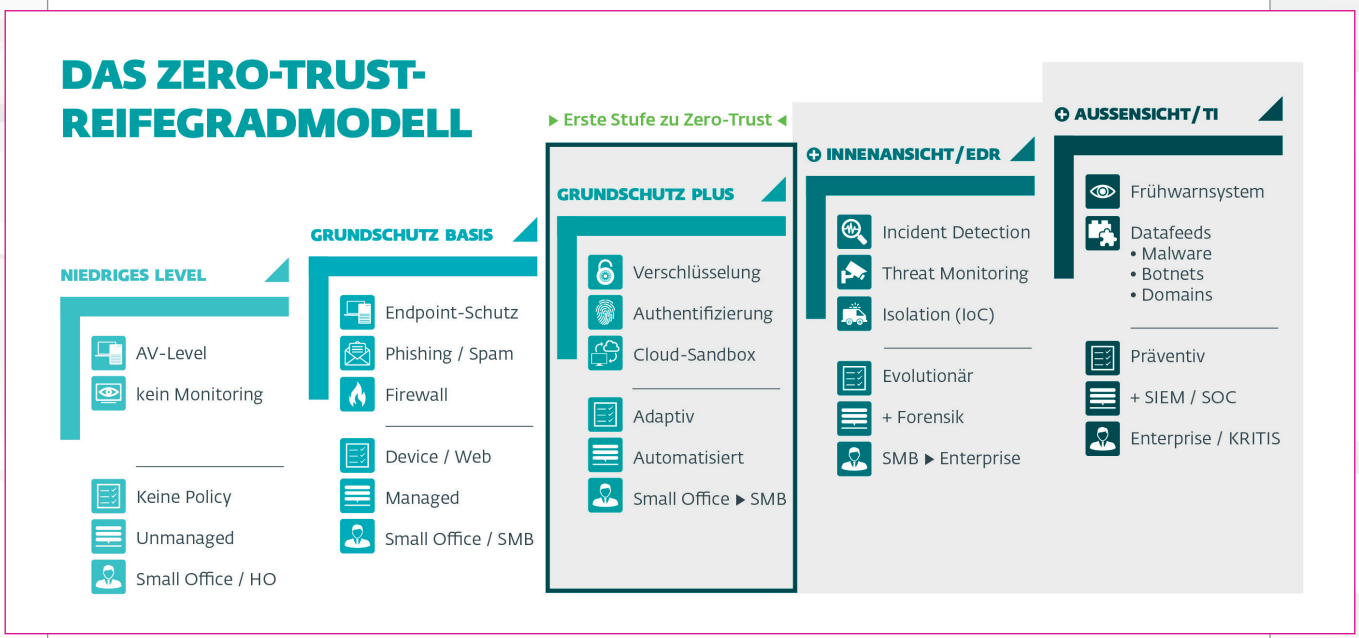
## Trend 3:
## Kunden bevorzugen „Made in EU"

Aufgrund der Ereignisse rund um die Ukraine hat definitiv ein Umdenken eingesetzt – und ein regelrechter „Run" auf Security-Unternehmen wie ESET begonnen. Natürlich sind die Qualität der IT-Sicherheitslösungen sowie die begleitenden Services immer noch die wichtigsten Faktoren bei der Auswahl des Herstellers. Aber: Immer mehr Unternehmen oder Verwaltungen hinterfragen die Herkunft der Sicherheitslösungen und schauen verstärkt auf das Label „Made in EU". Ihnen stellt sich zwangsläufig die Frage: Ist der Hersteller des Malwareschutzes, den meine Organisation einsetzt, auch wirklich vollumfänglich vertrauenswürdig und vor allem für meine Sicherheit verlässlich? Wer garantiert mir, dass jeder Schadcode gefunden, Updates vollständig bereitgestellt und keine Hintertüren durch die Software geöffnet werden? Oder gar Regierungen im Hintergrund Druck ausüben und Backdoors einbauen lassen?

Die Herkunftsbezeichnung „Made in EU" steht für eine Top-Qualität und die Einhaltung strikter Vorgaben. Insbesondere im Bereich der IT-Security sind Unternehmen aus der Europäischen Union weltweit führend und bestechen zudem durch eines: Vertrauen der Kunden in die Technologie und den Schutz der Kundendaten. Mit diesem Vertrauenssiegel können sich europäische Hersteller von IT-Security-Lösungen von ausländischen Mitbewerbern abheben und zeigen, dass ihre Lösungen den strengen europäischen Datenschutzbestimmungen entsprechen. Das Siegel signalisiert nicht nur Vertrauen, sondern bringt Produkte und Technologien aus der EU in den Fokus von Wirtschaft und Government. So können beispielsweise Behörden bei Ausschreibungen davon ausgehen, dass eine mit dem Siegel „IT-Security made in EU" ausgezeichnete Lösung höchsten Anforderungen genügt. Organisationen und Anwender stellen damit sicher, dass sie auf die Leistungsfähigkeit und Zuverlässigkeit der gekennzeichneten Technologien und Lösungen ebenso vertrauen können wie auf deren bedingungslose Gesetzeskonformität. Denn mit diesem Siegel verpflichten sich Hersteller mit Hauptsitz in der EU freiwillig dazu, dass ihre Security-Lösungen vertrauenswürdig sind, strengsten Datenschutzauflagen entsprechen und keinerlei versteckte Backdoors enthalten.

Einen Punkt möchte ich explizit hervorheben: Egal, ob beim Kampf gegen Malware staatlicher Behörden oder bei den Forderungen danach, bei der Entwicklung der Sicherheitssoftware „Hintertürchen" offenzulassen – unverändert gilt: Die Sicherheit der Nutzer steht an erster Stelle. Diese sogenannte „No backdoor guarantee" gibt ESET als europäischer Hersteller all seinen Kunden. Auch dies sucht außerhalb der Europäischen Union seinesgleichen.

***Thorsten Urbanski***



# SICHERER FERNZUGRIFF PER VPN

## IN 6 SCHRITTEN ZUR LANGFRISTIG FLEXIBLEN REMOTE-WORK-UMGEBUNG

Die Corona-Krise hat zu einem Boom bei VPN-Diensten in Unternehmen geführt. Viele Umsetzungen mussten überstürzt und unter großem Zeitdruck vorgenommen werden. Mit der erneuten massenhaften Rückkehr ins Homeoffice im Januar 2021 zeigte sich, dass bei vielen Unternehmen die bestehende Remote-Access-Infrastruktur dringende Anpassungen benötigt. Um künftig flexibel auf zu erwartende Schwankungen reagieren zu können, müssen bestehende Strukturen überdacht werden. Der nahtlose Übergang zwischen Homeoffice und Büroarbeitsplatz ist ein entscheidender Faktor für die Produktivität und Business Continuity von Unternehmen.

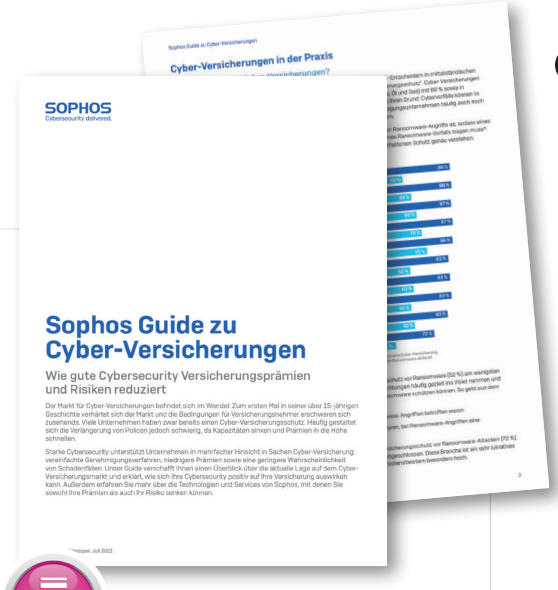
Wir zeigen Ihnen in diesem Whitepaper in sechs Schritten, wie Sie mithilfe einer durchdachten Remote-Access-Lösung zur langfristig flexiblen Remote-Work-Umgebung kommen.


**WHITEPAPER DOWNLOAD**

Das Whitepaper umfasst 19 Seiten und steht kostenlos zum Download bereit.

***www.it-daily.net/Download***

---




**WHITEPAPER DOWNLOAD**

Das Whitepaper umfasst 10 Seiten und steht kostenlos zum Download bereit.

***www.it-daily.net/Download***

# GUIDE ZU CYBER-VERSICHERUNGEN

## WIE GUTE CYBERSECURITY VERSICHERUNGSPRÄMIEN UND RISIKEN REDUZIERT

Der Markt für Cyber-Versicherungen befindet sich im Wandel: Zum ersten Mal in seiner über 15-jährigen Geschichte verhärtet sich der Markt und die Bedingungen für Versicherungsnehmer erschweren sich zusehends. Viele Unternehmen haben zwar bereits einen Cyber-Versicherungsschutz. Häufig gestaltet sich die Verlängerung von Policen jedoch schwierig, da Kapazitäten sinken und Prämien in die Höhe schnellen.

Der Guide verschafft Ihnen einen Überblick über die aktuelle Lage auf dem Cyber-Versicherungsmarkt und erklärt, wie sich Ihre Cybersecurity positiv auf Ihre Versicherung auswirken kann. Außerdem erfahren Sie mehr über die Technologien und Services von Sophos, mit denen Sie sowohl Ihre Prämien als auch Ihr Risiko senken können.

# (R)EVOLUTION DES SERVICE DESK

## MIT INNOVATIVEM ANSATZ HELPDESK-IMPLEMENTIERUNGEN ERFOLGREICH DURCHFÜHREN

Schnellere Reaktionszeiten, Kosteneinsparungen und glückliche Anwender - Die Mär vom neuen, heilbringenden Service Desk Tool ist immer noch weit verbreitet. Dabei ist die Intention dahinter kaum zu verübeln. Doch die Praxis zeigt, dass der Ansatz, einfach ein neues Service Desk Tool zur Erreichung der benannten Ziele zu implementieren, in der Regel trotz all der glorreichen Versprechungen scheitert. Die berechtigterweise hohen Erwartungen werden allzu schnell enttäuscht, wenn statt der erhofften Mehrwerte Frust und noch mehr Komplexität in den Arbeitsalltag insbesondere der First-Level-Mitarbeiter einziehen.

Doch warum ist das so? Und was könnte wirklich funktionieren? Diese Fragen stellte sich der Systemintegrator Consulting4IT aus Waldbronn. Mit aktuell 125 Mitarbeitern und über 15 Jahren Projekterfahrung mit Service Management Projekten hatte er genügend Kenntnisse und Ressourcen, um gründlich in die Ursachenforschung gehen zu können.

### F4SD – Innovatives Tool mit besonderem Fokus

Die Lösung ergab sich aus einem Perspektivenwechsel und einem ganz neuen Denkansatz. Denn, Hand aufs Herz, im Grunde wird immer wieder die gleiche, heilversprechende Madonna verkauft, neu sind meistens lediglich Name und Gewand. Und wenn auf dieser Grundlage auch immer wieder nur die veralteten, standardisierten Pflichtenhefte für Ausschreibungen verwendet werden, ist das Schicksal des Projekts in den meisten Fällen besiegelt.

Das Pferd einmal von hinten aufzäumen und da anfangen, wo gehobelt wird: Am Arbeitsplatz der First-Level-Mitarbeiter, die tagtäglich mit den hochheiligen Tools arbeiten dürfen. Ihre Grundbedürfnisse sind in aller Kürze schnell beschrieben: Gebraucht wird eine Oberfläche, die alle relevanten Informationen zu Usern und Clients bündelt, übersichtlich darstellt und direkte Lösungsmöglichkeiten bietet.

Beispielansicht des F4SD Cockpits – für die sofortige Übersicht an relevanten Informationen für den First-Level-Support

Nach dieser Erkenntnis überlegte die Consulting4IT nicht lange. Heraus kam die erste eigene Software: F4SD – First Aid Service Desk. Ein Tool, das in Echtzeit Informationen kumuliert mittels übersichtlichem Ampelsystem in einer Art Cockpit darstellt und mit Quick Actions sofortige Lösungsmöglichkeiten gängiger Problemfälle anbietet. Wo sonst dutzende verschiedener Tools parallel geöffnet werden müssen, um zumindest im Ansatz eine Problemursache beim User ausfindig zu machen, ist diese nun auf einen Blick erkennbar. Und kann darüber hinaus in 80 Prozent aller Fälle auch direkt mit einem Klick gelöst werden.

### Der Gamechanger, der Kunden zu Helden macht

F4SD ist damit beileibe kein neues Service Desk Tool im herkömmlichen Sinne. Denn das Tool ist so konzipiert, dass es mit allen gängigen Helpdesks kombiniert werden kann. Der Mehrwert ist dabei stets der Gleiche. Es versetzt die Support-Mitarbeiter in die Lage, endlich effektiv handeln zu können. Aus ihrem oftmals hilflosen Blindflug wird eine gesteuerte Punktlandung. Aus den Leidtragenden, die den Frust der Anwender tagtäglich zu spüren bekommen, werden echte Helden, die das Steuerrad fest in der Hand haben. Wenn diese Erkenntnisse dann auch noch in Prozesse und neue Ansätze in der Erstellung von Ausschreibungsunterlagen miteinfließen, steht einer Evolution des Service Desks auf den nächsten Level nichts mehr im Wege. Das Ergebnis: Hochmotivierte First-Level-Mitarbeiter, schnellere Reaktionszeiten, Kosteneinsparungen, glückliche Anwender.

***Linda Schmittner | www.consulting4it.de***

# CYBERWAR

## SIND UNTERNEHMEN VORBEREITET?

Seit bereits vielen Jahren ist ein weltweiter Cyberwar zu beobachten. Der Ansicht einiger nach handelt es sich hierbei lediglich um eine Fortsetzung des bestehenden „stillen Cyberkriegs": jüngste geopolitische Instabilitäten, Malware und Kampagnen zum Diebstahl geistigen Eigentums, die von Russland, China, Iran und Nordkorea ausgehen und sich gegen viele westliche und NATO-Staaten richten (und umgekehrt). Mit anderen Worten: Es habe sich nicht viel geändert und Organisationen hätten wenig zu befürchten, solange sie nicht zu eng mit den Zielstaaten zusammenarbeiten, auf die die Angriffe abzielen.

Vertreter dieser Ansicht unterliegen damit jedoch einem Irrglauben – denn es hat sich viel verändert. Der Cyberwar zielt weit über staatliche Einrichtungen hinaus und betrifft mittlerweile alle Arten von Organisationen auf der ganzen Welt. Tatsächlich haben sich kriminelle Akteure, die es auf Staaten abgesehen haben, und solche, die auf finanziellen Profit aus sind, zusammengeschlossen. Sie tauschen untereinander das Wissen über Angriffstechniken aus und nutzen Bedrohungsvektoren gegen jede Art von Ziel. Alle Organisationen sind nun potenzielle Ziele, wobei kritische Infrastrukturen, hochwertige Betriebstechnologie in der Fertigung und Ziele aus dem Technikbereich ganz oben auf der Liste stehen.

Cyberangriffe auf kritische Infrastrukturen, Hersteller und Technologieunternehmen sind so häufig geworden, dass die CISA die „Shields Up"-Initiative eingeführt hat, die aktuelle Informationen darüber liefert, wie sich Russlands laufende Aktionen auf Organisationen jenseits des unmittelbaren Kriegsgebiets auswirken, sowie Hinweise zur Verhinderung von Cyberangriffen. Wenn Unternehmen der CISA Cyber-Vorfälle schnell melden, kann die CISA diese Informationen zur Hilfeleistung nutzen. Außerdem kann sie rechtzeitig Warnungen aussprechen, um andere Organisationen und Einrichtungen davor zu bewahren, Opfer eines ähnlichen Angriffs zu werden.

### Industrie und Fertigung sind nicht mehr sicher

In jüngster Zeit nehmen Cyberangriffe immer mehr die Betriebstechnik (OT) und die industriellen Kontrollsysteme (ICS) in Produktionsbetrieben aller Branchen ins Visier.

Zwei bemerkenswerte Beispiele aus jüngster Zeit sind die Ransomware-Attacke auf einen japanischen Reifenhersteller und ein mutmaßlicher Cyberangriff auf japanische Toyota-Werke. Letzterer Angriff war womöglich politisch orientiert, denn er ereignete sich am selben Tag, an dem Japan sich dem Westen anschloss und Transaktionen mit der Zentralbank der Russischen Föderation einschränkte. Die meisten kriminellen

## AUSWIRKUNGEN VON CYBERSECURITY-EREIGNISSEN

### KURZFRISTIGE AUSWIRKUNGEN:

**Betriebsstillstand**

**Verlust des Überblicks über die Produktion und die Sicherheitssysteme**

**Finanzielle Verluste aufgrund von Ausfällen**

**Diebstahl von geistigem Eigentum**

Hacker wollen sich jedoch finanziell bereichern und werden nicht nur von geopolitischen Erwägungen geleitet.

Gartner postulierte im Juni, dass Bedrohungsakteure bis 2025 in der Lage sein werden, operative Technologieumgebungen erfolgreich als Waffe einzusetzen, um menschliche Verluste zu verursachen. Das bedeutet, dass sich die Situation für Unternehmen, die sich nicht angemessen geschützt haben, noch verschärfen wird. Angriffe auf kritische Infrastrukturen haben von 2013 bis 2020 um 3.900 Prozent zugenommen (Gartner), und 55 Prozent der OT-Sicherheitsexperten stufen Ransomware als Bedrohung Nr. 1 für OT-Systeme ein (SANS) – noch im Jahr 2019 war dieser Prozentsatz nur halb so hoch. Doch was ist der Grund für diesen Anstieg?

Ein Grund ist das Aufkommen von Ransomware-Banden wie Conti, die im Jahr 2021 mindestens 180 Millionen Dollar von ihren Opfern erpresst haben. Das ist etwa doppelt so viel wie die Erpressung durch DarkSide/BlackMatter, die für den bekannten Angriff auf Colonial Pipeline verantwortlich waren. Ransomware erweist sich also als sehr profitabel für kriminelle Akteure.

Während Angreifer im Cyberraum früher oft den Anschein machten, derartige Angriffe auf die Öffentlichkeit zu vermeiden, scheinen heute viele einen Cyberkrieg ohne Rücksicht auf Verluste zu führen – und zwar auch gegen Verbraucherdienste, kritische Infrastrukturen, Krankenhäuser und dergleichen. Sie konzentrieren sich nicht mehr nur auf staatliche Einrichtungen.

**Auf Cyber-Resilienz kommt es an**

Unternehmen sind auf eine funktionierende IT-Infrastruktur angewiesen, um ihre Geschäftsaktivitäten voranzutreiben. In den letzten Jahren hat sich jedoch ein grundlegender Wandel vollzogen. Die fortschreitende Migration in die Cloud, die Umstellung auf mobile Geräte und BYOD (Bring Your Own Device), die Konvergenz von IT/OT/IoT und die starke Zunahme der Fernarbeit haben unsere Herangehensweise an die Cybersicherheit verändert. Da die Zahl der vernetzten Geräte am Arbeitsplatz und in den Produktionsstätten zunimmt, werden die IT/OT- und Sicherheitstools, auf die sich Organisationen bisher verlassen haben, zu großen Teilen unwirksam.

Unternehmen im Bereich Kritischer Infrastrukturen und OT-Organisationen stellen sich zwei grundlegende Fragen: „Wie hoch ist das Sicherheitsrisiko, dem unsere Organisation ausgesetzt ist?" und „Wie sicher sind unsere Infrastruktur und Geräte?". Angesichts der aktuellen geopolitischen Lage sollte jede Organisation zumindest in der Lage sein, diese konkreten Fragen zu beantworten:

ES IST UNABDINGBAR, DASS UNTERNEHMEN FÜR IHRE KÜNFTIGE SICHERHEIT UND ZUM SCHUTZ IHRER RENTABILITÄT BESONDERES AUGENMERK AUF DIE SICHTBARKEIT IHRER ASSETS LEGEN.

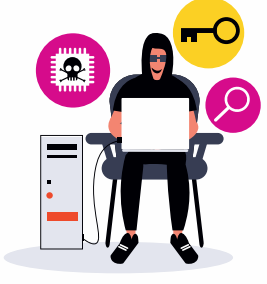
Conor Coughlan,
CMO and Advocacy Officer, Armis,
www.armis.com

**LANGFRISTIGE AUSWIRKUNGEN:**

**Risiken für Gesundheit und persönliche Sicherheit**

**Kontrollverlust**

**Erhebliche ungeplante Kosten für Arbeit, Überstunden und Ausrüstung**



**Erhöhte oder verweigerte Versicherungsleistungen**

- Welche Geräte sind an mein Netzwerk angeschlossen?
- Was machen diese Geräte, während sie verbunden sind?
- Gibt es aktive Angriffe auf mein Unternehmen?
- Wie ist die Risikolage unserer Geräte und unserer Organisation?

**Welche Assets habe ich im Netzwerk?**

Aufgrund der sprunghaften Zunahme von Endgeräten haben viele Unternehmen eine „Sichtbarkeitslücke", was bedeutet, dass IT- und Sicherheitsverantwortliche nicht alle gefährdeten Ressourcen in ihren Umgebungen sehen können. Viele Unternehmen haben weder den erforderlichen Einblick in ihre Infrastruktur noch sind ihre Systeme im Einklang mit den notwendigen Richtlinien und Prozessen, um effektiv auf einen Angriff zu reagieren. Wenn hier keine ausreichende Sichtbarkeit gewährleistet werden kann, dann ist es wahrscheinlicher, Ziel eines schweren Angriffs zu werden.

Im Idealfall sollten über ein Mapping alle im Unternehmen ablaufenden Prozesse bekannt sein. Dazu gehören alle angeschlossenen IT- und OT-Assets – verwaltete und nicht verwaltete – in und um das Unternehmen herum, aber auch Netzwerk-Assets und zugehörige Assets, die mit dem Netzwerk verbunden sind. Sobald das Mapping abgeschlossen ist, kann die Erkennung von Bedrohungen durch Verhaltensmuster Anomalien in Echtzeit aufdecken und ein schnelles Handeln ermöglichen.

Viele Anbieter bieten auch eine Erweiterung für das Schwachstellenmanagement an. Der Schlüssel dazu ist, sicherzustellen, dass die Lösung eine Single Source of Truth, also eine einzige, maßgebliche Wahrheit über die Unternehmensressourcen nutzt – denn eine einzige übersehene Ressource im Unternehmen kann ausreichen, um von einem Cyberangriff betroffen zu sein. Wenn Organisationen dagegen einen umfassenden Überblick über alle Assets haben, können sie viel schneller und effektiver reagieren. Jedes Mal, wenn eine neue schwerwiegende Sicherheitslücke/CVE veröffentlicht wird, können die Schwachstellenanalysten das Gesamtrisiko für das Unternehmen auf der Grundlage aller betroffenen Assets schnell ermitteln. Auf der Grundlage der Risikostufen für das Unternehmen kann dann festgelegt werden, welche Assets zuerst abgesichert, unter Quarantäne gestellt oder vielleicht sogar offline genommen werden sollen.

Die Erfassung aller Prozesse und Assets ist auch der Schlüssel zur Wiederherstellung im Falle eines Cyberangriffs. Nach einem Angriff kann der Betrieb in Organisationen manchmal für ein oder zwei Tage ausfallen, in besonderen Fällen kann es Monate dauern, bis die Arbeit wieder aufgenommen wird. Unternehmen sollten sich zudem von unabhängigen Prüfern versichern lassen, dass ihre Infrastruktur nach einem Cyberangriff schnell wiederhergestellt werden kann.

Es ist unabdingbar, dass Unternehmen für ihre künftige Sicherheit und zum Schutz ihrer Rentabilität besonderes Augenmerk auf die Sichtbarkeit ihrer Assets legen.

***Conor Coughlan***


**Verschlechterung der Leistung und Qualität des Equipments**


**Gebühren und Gerichtsverfahren aufgrund von Fahrlässigkeit oder Nichteinhaltung**

**Kundenverlust**

**Umlenkung von Unternehmensausgaben auf Wiederherstellung**

# SECURITY STRATEGISCH DENKEN

## RÜSTZEUG GEGEN CYBERATTACKEN

Cyberangriffe und kein Ende in Sicht: Nahezu jedes zweite der befragten Unternehmen (46 Prozent) in Deutschland hat in den letzten zwölf Monaten mindestens eine Cyberattacke erlebt. Das geht aus einer aktuellen Statista-Erhebung hervor. Die Gesamtbedrohungslage ist angespannt und hat sich laut Bundesamt für Sicherheit in der Informationstechnik (BSI) seit dem russischen Angriffskrieg auf die Ukraine noch einmal verschärft. Cyberattacken durch Ransomware oder Phishing-Mails und andere digitale Bedrohungen legen im schlimmsten Fall den Unternehmensbetrieb lahm, ziehen Daten ab und verursachen Gesamtschäden in Milliardenhöhe.

### In 4 Schritten zum integrierten Security-Konzept

Wie lassen sich Cyberangriffe erfolgreich abwehren und Risiken für eine Attacke generell minimieren? „Eine rein Checklisten-gepflegte Security reicht nicht aus. Vielmehr kommt es darauf an, die IT-Sicherheit als organisatorisches Thema systematisch zu betrachten“, sagt Edgar Reinke, Security-Experte und Strategic Technology Officer (STO) bei Damovo. Der ICT-Dienstleister Damovo unterstützt Unternehmen dabei, Bedrohungen und Risiken strukturiert zu beleuchten und ein ganzheitliches, individuelles Sicherheitskonzept zu designen.

**▶ 1. SCHRITT:**

#### Einschätzung der Ausgangslage

Mit strategischen Security-Ansätzen wie etwa dem Security Quick Check stellt Damovo den Security-Reifegrad eines Unternehmens auf den Prüfstand.

**▶ 2. SCHRITT:**

#### Angriffssimulation und Awareness

Anhand initiierter Phishing-Aktivitäten, Penetrationstests und weiterer Angriffssimulationen testen die Sicherheitsexperten das Security- und Risikomanagement auf seine Widerstandsfähigkeit. Mit den aufgedeckten Sicherheitslücken schafft Damovo Awareness für Risiken und Angriffsziele bei den Nutzern.

**▶ 3. SCHRITT:**

#### Evaluierung und Security-Architektur

Aus den Schwachstellen leitet Damovo konkrete Handlungsempfehlungen ab und bietet als Cisco Gold Partner darüber hinaus weitere Services für das Cisco Secure Portfolio. Als Sparringspartner ist der ICT-Dienstleister fester Bestandteil des Security-Betriebs der Kunden und unterstützt bei der zielgerichteten und schnellen Behebung von Sicherheitsrisiken.

**▶ 4. SCHRITT:**

#### Umsetzung und Managed Security Services

Darüber hinaus begleitet Damovo die Umsetzung der empfohlenen Maßnahmen. Den laufenden Betrieb sichern die Experten durch Instandhaltung der IT-Landschaft, aktuelle Release-Stände und eingespielte Patches der Security-Infrastruktur.

Dabei gilt es, die Security Services über den kompletten Lebenszyklus hinaus im Blick zu behalten – im Kontext von Infrastruktur, Applikationen und Nutzungsverhalten.

### Security-Know-how kontinuierlich abrufen

Mit dem virtuellen Chief Information Security Officer (vCISO) stellt Damovo seinen Kunden ein erfahrenes Expertenteam an die Seite. Als Sparringspartner verstärkt es die strategische Unternehmenskompetenz in der Informationssicherheit. Gerade in Zeiten des Fachkräftemangels bietet der vCISO-Service eine flexible und individuelle Lösung, IT-Security-Strategien konzeptionell aufzubauen, weiterzuentwickeln, kontinuierlich zu verbessern und nachhaltig im Unternehmen zu verankern.

Edgar Reinke: „Der virtuelle CISO ist der Lotse, der Unternehmen beim Aufbau eines standhaften Mauerwerks an integrierten IT-Sicherheitsmaßnahmen begleitet, das Cyberangriffe und andere digitale Bedrohungen erfolgreich abwehrt.“

DAMOVO

**Besuchen Sie Damovo auf der it-sa**
25.-27. Oktober 2022
Messe Nürnberg: **Halle 7A**
Stand A-418 (Cisco-Stand)

# ENDNUTZER STÄRKEN

## SICHERHEITSARCHITEKTUREN PRAGMATISCH UMSETZEN

Zero-Trust-Konzepte beruhen auf der Erkenntnis, dass die Sicherheit auf Endnutzerebene gestärkt werden muss, da es keine grundsätzliche Vertrauensstellung mehr gibt. Mit der Verlagerung der Endgeräte heraus aus dem vermeintlich geschützten Unternehmensnetzwerk entsteht ein mehr oder weniger blinder Fleck. Hier gilt es, sich die Automatisierungs- und Analytics-Funktionen von Digital Employee Experience Management zunutze zu machen, um Produktivität, Akzeptanz und Sicherheit gleichzeitig sicherzustellen.

Zero Trust-Konzepte können auf unterschiedliche Weise um- und durchgesetzt werden, je nach bestehenden Infrastrukturen und Organisation der IT. Klar ist in jedem Fall, dass sie hochgradig automatisiert werden müssen.

Typischerweise definiert ein Sicherheitsteam das Zero-Trust-Framework und stellt dessen Umsetzung sicher. Netzwerkteams kümmern sich um die Bereitstellung, Konfiguration und das Management der einzelnen Security-Komponenten. Das IT Service Management steht letztlich vor der Anforderung, insbesondere das Geschehen bis zu den Endgeräten beziehungsweise Endanwendern im Blick zu behalten. Hier treffen vielschichtige Risikofaktoren aufeinander.

- Konsolidierte Sicht auf alle Endgeräte
- Automatisiertes Patch-Management
- Echtzeit-Telemetriedaten in der Gesamtsicht
- Korrelation von möglichen Risikofaktoren
- Hinterlegte Lösungsverfahren
- Endanwender-Support

In der Konsequenz dieser Anforderungen sind Zero-Trust-Umgebungen nicht umsetzbar, wenn das IT Service Management Team mit der häufig üblichen verteilten Sicht auf das Unternehmensnetz konfrontiert ist, die teils noch überlappende Verantwortlichkeiten aufweist:

1. Das Client-Management kümmert sich um Endgeräte und gemeinsam mit dem Network Monitoring um die Navigation im Unternehmensnetz.

2. Das Network Monitoring hat in der Regel noch Public und Private Networks im Blick, teilweise auch lokale Infrastrukturen.

3. Anbieter aus den Bereichen Application Performance Management (APM) und Software-as-a-Service (SaaS) liefern ihrerseits Daten zum Geschehen auf Netz- und Endanwenderebene.

Diese vielschichtigen, teils isolierten Sichten, gepaart mit sporadischen E-Mail-Umfragen bei Endanwendern zu ihren Erfahrungen mit dem digitalen Arbeitsplatz, bergen mehrere Risikofaktoren:

- Es bleibt zu viel Raum für Interpretationen in der Sicherheit.
- Compliance-Probleme werden übersehen, wenn Monitoring- und Performancedaten nicht übergreifend korreliert werden können.
- Sicherheitsmaßnahmen können nicht lückenlos automatisiert ausgerollt und überprüft werden.
- Fehlkonfigurierte Schutzmechanismen können die Produktivität des Arbeitsplatzes beeinträchtigen.

Um Zero-Trust mithilfe von Plattformen für das End-User Experience Management (EUEM) oder Digital Employee Experience (DEX) zu unterstützen, sind folgende Kriterien relevant:

- Konsolidierte Sicht auf Endgeräte
- Zustandsanalyse der Endgeräte – Client Health
- Netzwerkanalyse mit Kontext
- Vorausschauendes Sicherheitsmanagement mit intelligenter Mustererkennung
- Kontext-bezogener Endanwender-Support

**Fazit**

Zero Trust und DEX haben das gleiche Ziel: Endanwendern eine produktive und gleichzeitig sichere digitale Arbeitsumgebung zu gewährleisten. Worauf es dabei ankommt, sind drei Dinge: Client- und Netzwerkteams müssen eng verzahnt zusammenarbeiten können mithilfe der Integration von geeigneten DEX- und Netzwerkmonitoring-Plattformen. Das Client-Management muss aufholen im Hinblick auf Automatisierung und Analytics – Dinge, die im Netzwerkmanagement seit langem Standard sind. Und drittens, nicht weniger wichtig, brauchen Endanwender mehr und bessere Unterstützung.

***www.nexthink.com***

# REZERTIFIZIERUNGEN

## SCHNELL UND UNKOMPLIZIERT DURCHFÜHREN

Die aktuell geltenden Regularien der Finanzaufsichtsbehörden BaFin (DE), FINMA (CH) und FMA (AT) verlangen insbesondere von Banken und Finanzinstituten, aber auch von Industrieunternehmen Nachweise der ordentlichen Berechtigungsvergabe. Die Einführung eines umfassenden Rezertifizierungssystems geht mit hohem Aufwand für Unternehmen einher. Die technologieführende Identity and Access Governance (IAG) Plattform NEXIS 4 bietet durch einen No-Code-Ansatz die entsprechenden Werkzeuge zur ressourcenschonenden Lösung.

**Weniger Technik, mehr Konzeption:**
NEXIS 4 kann sich an bestehende IAM Systeme anschließen und zusätzlich weitere Berechtigungsstrukturen schnell und unkompliziert per Datei- oder Datenbankanbindung darstellen. So sind Unternehmen nicht gezwungen, die zu prüfenden Systeme aufwändig zentral bereitzustellen und können sich auf die Konzeption der Rezertifizierung fokussieren.

**Workflow-Konfiguration durch Best-Practices:**
Nach dem Anschluss der relevanten Daten, können vom Hersteller mitgelieferte Workflow- und Delegations-Templates ohne aufwändige Skripte oder Code verwendet werden, um die Prüfprozesse entsprechend anerkannter Best-Practices aufzusetzen.

**Individuelles UX-Design:**
Die Endanwender-Sichten werden direkt in den jeweiligen Workflow-Schritten nutzergruppenspezifisch gestaltet. Das Content-Management von NEXIS 4 erlaubt hierbei das Zusammenstellen der Sichten auf Basis von Vorlagen, die mit wenigen Klicks individualisiert werden können.

**Pilotierung & Produktivsetzung:**
Mit Hilfe einer initialen Rezertifizierung für Pilotbereiche kann die Konfiguration weiter verfeinert werden. Nach Einarbeitung möglichen Feedbacks kann dann so eine optimal abgestimmte Rezertifizierung gestartet werden.

NEXIS

Mehr Informationen zu NEXIS 4 auf ***https://www.nexis-secure.com.***

# DIGITALE FORENSIK

## DIE ZUKUNFT DER VERBRECHENSAUFKLÄRUNG

Bundesinnenministerin Nancy Faeser hat eine Grundgesetzänderung vorgeschlagen. Das Bundesamt für Sicherheit in der Informationstechnik soll eine Zentralstelle werden. Zurzeit liegt die Verantwortung für Cybersicherheit noch bei den Bundesländern, das BSI könne nur Amtshilfe leisten. Das sei angesichts der gewachsenen Bedrohung nicht mehr zeitgemäß, sagte die Ministerin in Berlin. Die Länder seien mit dieser Aufgabe langfristig „überfordert".

Dirk Labudde schildert in seinem Buch „Digitale Forensik" anhand verschiedener Beispiele die Problematik bei der Cybersicherheit durch die unterschiedlichen Herangehensweisen der Bundesländer und zeigt auf, was sich ändern muss:

„Damit wir zu einer solchen Form von Ermittlungsarbeit kommen, muss sich die Ausbildung von Polizistinnen und Polizisten, aber auch von IT-Forensikerinnen und -Forensikern im Polizeidienst drastisch ändern. Zwar ist inzwischen in allen Bundesländern die Vermittlung von IT-Fähigkeiten in der Polizeiausbildung verankert – allerdings mit großen Unterschieden in Quantität und Qualität."


**Digitale Forensik. Die Zukunft der Verbrechensaufklärung, Dirk Labudde, Lübbe Sachbuch, 04-2022**

# VPN UND DIE CLOUD

## VEREINEN SIE MAXIMALE FLEXIBILITÄT MIT HÖCHSTER SICHERHEIT!

Im Zuge des weiter voranschreitenden Cloud-Booms scheinen Schlagwörter wie „Zero Trust", „Single Sign On" oder „SD-WAN" den klassischen VPN-Tunnel immer weiter abzulösen. Doch wieso eigentlich? Weil sich virtuelle private Netzwerke und Cloudanbindung von vornherein ausschließen? Mitnichten! Entscheidet man sich für die richtige, moderne Lösung, lassen sich zeitgemäße VPN-Strukturen und digitale Cloud-Technik zu einem mächtigen IT-Security-Instrument kombinieren.

### Security auf einer neuen Stufe

Damit dies gelingt, müssen vor allem zwei Punkte erfüllt sein: Hochsichere IPsec-Datenkommunikation und vollständige Kompatibilität mit allen gängigen Cloud-Technologien. Das entsprechende Sicherheitslevel kommt bei einer cloud-integrierten VPN-Lösung durch das Gateway in Verbindung mit einem Management-System zustande. Dies kann z.B. der NCP Virtual Secure Enterprise VPN Server (vSES) in Kombination mit dem NCP Secure Enterprise Management (SEM) sein. Dieser Zusammenschluss hat den Vorteil, dass alle Verbindungen IPsec-basiert und somit hochsicher übertragen werden. Außerdem liegt das Gateway nicht direkt in der Cloud, sondern bildet hinter der Firewall eine abgesicherte Umgebung direkt auf dem Server, welcher im Hinblick auf Ihre digitale Souveränität in einem deutschen Rechenzentrum beheimatet sein sollte.

### VPN kann auch Cloud!

Um die Kompatibilität zu allen etablierten Cloud-Services zu garantieren, setzen Unternehmen am besten auf Lösungen wie das Enterprise-VPN von NCP, die z.B. mühelos als Teil einer SASE- oder SD-WAN-Infrastruktur eingesetzt werden können. Die VPN-Komponenten sind hier bereits von Natur aus „cloudfähig" und fügen sich auch in komplexe SD-WAN-Verbünde ein. Die Integration in ein SAML-System ist ebenfalls kein Problem. Hier gilt die Authentisierung des Nutzers am SSO-Portal dank des Tunnels dann sowohl für interne Dienste als auch externe Cloudanwendungen. So genießen Administratoren und Nutzer weiterhin alle Vorteile ihrer SAML-Schnittstelle, können Daten allerdings über einen hochsicheren IPsec-Tunnel mit voller Geschwindigkeit übertragen.

### Volle Kontrolle dank Zero Trust

Technologien wie SAML/SSO sind oft auch Bestandteil einer übergeordneten Zero-Trust-Strategie, bei der Nutzer durch granulare Firewall-Regeln nur Zugriff auf für sie relevante Anwendungen haben (Least-privilege-Prinzip). Mithilfe einer zentralen Management-Komponente wie dem NCP Secure Enterprise Management (SEM) definieren Administratoren alle Zugriffsrechte ihrer Anwender mit wenig Aufwand. Zusätzlich profitieren Sie von einem großen Funktionsumfang der VPN-Software: Der NCP VPN-Bypass oder Split Tunneling helfen dabei, den VPN-Server zu entlasten, indem datenhungrige Anwendungen ohne Sicherheitsrelevanz am Tunnel vorbeigeleitet werden. Für die Sicherheit des gesamten Netzes sind auch Endpoint Policy Checks unerlässlich, die Endgeräte vor jedem Login-Versuch auf vordefinierte Security-Parameter hin überprüft. Stellt das System zum Beispiel veraltete Software auf einem Laptop fest, wird die Verbindung erst nach Abschluss der notwendigen Updates aufgebaut. Da der Administrator sowohl Policies als auch Updates mit wenigen Klicks an einzelne Nutzergruppen oder die gesamte Organisation verteilt, bleiben so auch große Anwenderzahlen immer auf dem neuesten Sicherheitsstand!

***www.ncp-e.com***

**Besuchen Sie uns auf der it-sa**
25.-27. Oktober 2022
**Halle 7A**, Stand 412

# ZERO TRUST

## VERTRAUE NIEMANDEM UND VERIFIZIERE JEDEN

Hand aufs Herz: Sichern Sie Ihre Systeme in der Cloud via Perimeterschutz mit einer Firewall ab? Da sich die Cyber-Crime-Branche zunehmend professionalisiert und Hacker-Angriffe ein attraktives Business sind, genügt das nicht mehr. Es braucht: Zero Trust.

Dabei sollten Firmen verinnerlichen, was Zero Trust bedeutet – und sich daran halten: „Vertraue niemandem außerhalb und innerhalb deiner Organisation. Und verifiziere jeden." Damit ist Zero Trust ein guter Ansatz, um die Angriffsfläche zu reduzieren – jedoch keine Lösung, die out-of-the-box freischaltbar ist. Als Designprinzip ist Zero Trust individuell umzusetzen.

**Multi-Faktor-Authentifizierung**

Dabei sollten Unternehmen zuerst bestehende Prozesse analysieren und Schutzziele wie die Multi-Faktor-Authentifizierung definieren: Damit Mitarbeitende cloudbasierte Lösungen nutzen dürfen, ist ein zweites Authentifizierungsmerkmal – eine SMS, eine App, ein Anruf oder ein weiteres Gerät – an allen Endpoints vorzusehen. Zudem ist bei BYOD-Szenarien (Bring Your Own Device) eine Null-Toleranz-Politik zu vertreten: Erfüllen die privaten Endgeräte der Mitarbeitenden die Security-Anforderungen nicht, dürfen sie nicht mit dem Netzwerk verbunden sein. Ebenso ist zu prüfen, ob das Patch Management im Homeoffice wirkungsvoll ist.

**Cloud Security betrifft alle**

Dabei müssen Unternehmen wissen: Zero Trust im Cloud-Umfeld ist kein reines IT-Thema, sondern wichtig für den Geschäftsbetrieb. Darum ist Cloud Security zunächst in der Unternehmensstrategie zu verankern und erst dann praktisch umzusetzen.

***www.arvato-systems.de***

arvato
BERTELSMANN
Arvato Systems

**it-sa 2022**
25.-27. Oktober 2022

Besuchen Sie uns auf dem Microsoft-Stand in **Halle 7**

---

# IT-SICHERHEIT

## TECHNOLOGIEN UND BEST PRACTICES FÜR DIE UMSETZUNG IM UNTERNEHMEN

Für Unternehmen ist es existenziell, die Sicherheit ihrer Informationen, Systeme und Produkte zu gewährleisten. Dies trifft heute mehr denn je zu, denn mit zunehmender Vernetzung wächst auch die Angriffsfläche: Jedes vernetzte Gerät ist ein potenzielles Einfallstor für Gefährdungen, und das erhöht das Risiko zusätzlich. Doch wie können Sie Ihr Unternehmen vor diesen Gefährdungen schützen und Sicherheit gewährleisten?

Die Antwort auf diese Frage – und viele hilfreiche Impulse und Best Practices – bietet Ihnen dieser Praxisratgeber zum Thema IT-Sicherheit. Es werden alle für Entscheider relevanten Aspekte der IT-Sicherheit beschrieben und das für weiterführende Entscheidungen erforderliche Know-how zielgerichtet vermittelt. Das Buch dient als Leitfaden auf Ihrem Weg zur konsequenten und gleichzeitig effizienten Sicherstellung und Umsetzung von IT-Sicherheit im Unternehmen.


**IT-Sicherheit – Technologien und Best Practices für die Umsetzung im Unternehmen; Michael Lang, Hans Löhr (Hrsg.), Carl Hanser Verlag GmbH & Co.KG; 06-2022**

**WIE WEIT SIND SIE MIT DER UMSETZUNG DER DATENSCHUTZ-GRUNDVERORDNUNG?**

(Quelle: www.bitkom.org)

| 20 % | 45 % | 29 % | 5 % | 3 % |
|---|---|---|---|---|
| Vollständig umgesetzt | größtenteils umgesetzt | teilweise umgesetzt | gerade damit begonnen | keine Angaben |


# DIGITALISIERUNGSBREMSE DATENSCHUTZ?

## HERAUSFORDERUNGEN UND CHANCEN AUF DEM WEG ZUM DIGITALEN UNTERNEHMEN

Laut einer Studie des Digitalverbands Bitkom sind zwei Drittel von über 500 befragten Unternehmen der Meinung, dass in Deutschland die Digitalisierung aufgrund des strengen Datenschutzes und dessen uneinheitlichen Auslegung erschwert wird. Klar ist, dass die Umsetzung der Datenschutzgrundverordnung (DSGVO) vor allem für kleinere und mittlere Unternehmen nicht leicht zu stemmen ist. Korrekt aufgesetzte digitale Prozesse sind jedoch nicht nur aus verbraucherschutztechnischen Gründen wichtig, sie bergen auch viele Wettbewerbsvorteile, die es auszuschöpfen gilt.

In der Bitkom-Umfrage gaben vier von zehn befragten Unternehmen an, dass sie seit der DSGVO-Einführung mehr Aufwand haben und dass dieser auch künftig bestehn beleiben wird. Insbesondere kleinere Unternehmen (20 – 99 Mitarbeitende) stehen hier vor großen Herausforderungen: Knapp 40 Prozent von ihnen konnten die Verordnung erst teilweise umsetzen.

### Worauf zu achten ist

Um zu vermeiden, dass digitale Innovationsprojekte aus Unsicherheit bezüglich des Datenschutzes ausgebremst werden, ist es zentral wichtig, dass IT-Berater und Software-Entwickler bei jeder Konzeption von IT-Systemen und -Prozessen permanent und von Beginn an sämtliche Fragestellungen hinsichtlich Datenschutz und Informationssicherheit berücksichtigen. Nur so fallen diesbezügliche Anforderungen nicht erst dann auf, wenn die entsprechende Lösung bereits fertig entwickelt ist.

Bei der Wahl eines passenden Datenschutz-Managementsystems (DSMS) wiederum gilt es darauf zu achten, dass sich die Anforderungen aus der EU-DSGVO konkret mithilfe verschiedener Workflows, Rollen, Templates und Überwachungsprozessen unkompliziert umsetzen lassen. Idealerweise lässt sich das Datenschutz-System einfach in die bestehende ITSM-Lösung integrieren und setzt auf die dort bereits etablierte Struktur auf.

### Wie Unternehmen vom Datenschutz profitieren

Grundsätzlich gesehen ist Datenschutz für Unternehmen schon deshalb weniger eine Hürde, als unerlässslicher Stützspfeiler für den Geschäftserfolg, da in der global operierenden, modernen Arbeitswelt mit Homeoffice, digitalen Anwendungen und mobilen Geräten betriebsinterne Daten immer öfter hohen Gefahrenpotenzialen durch Angriffe von außen ausgesetzt sind.

Darüber hinaus lassen sich im internationalen Vergleich aus den DSGVO-Vorgaben innerhalb der EU und aus der langjährigen Datenschutzkompenz in Deutschland wichtige Wettbewerbsvorteile ziehen. Für Unternehmen, die ihre Daten ausschießlich im EU-Raum hosten lassen sowie SaaS-, PaaS- und IaaS Provider, die Rechenzentren in diesem Gebiet nutzen bzw. betreiben und möglicherweise sogar eine ISO 27001-Zertifizierung vorweisen können, ist dies ein echter Wettbewerbsvorteil.

### Aufhebung des Gegensatzes

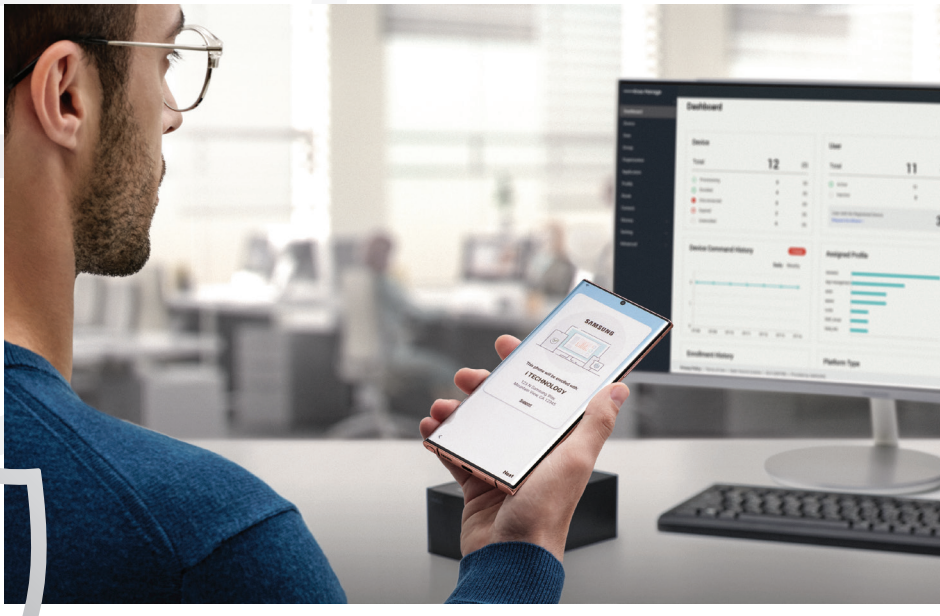
Datenschutz ist also nicht nur aus verbraucherschutztechnischen Gründen ein wichtiger Grundpfeiler der Digitalisierung. Er dient Unternehmen auch im Hinblick auf den Schutz ihrer eigenen Daten und schafft Wettbewerbsvorteile. Richtig verstanden und mit smarten Lösungen umgesetzt, werden datenschutzfreundliche Technologien so zum eigentichen Treiber der erfolgreichen Digitalisierung.

***www.on.de***

# SO GEHT SICHERHEIT HEUTE

## MOBILGERÄTE SICHERN, BEREITSTELLEN UND VERWALTEN MIT SAMSUNG KNOX

Mobile Mitarbeiter müssen immer einsatzbereit sein und sind auch unterwegs häufig online. Aber sind ihre Mobilgeräte dabei ausreichend gegen Cyberangriffe, Datenlecks, Viren und andere Bedrohungen gewappnet? Mit Samsung Knox können sich Mitarbeiter und IT-Verantwortliche jederzeit sicher sein – und den Fokus ganz auf ihre eigentlichen Aufgaben legen.



### Samsung Knox – hochwertiger Schutz für Android-Geräte

Samsung hat sich den weitreichenden Schutz von Unternehmensdaten auf seinen Android-Mobilgeräten zur Aufgabe gemacht. Die Lösung heißt: Secured by Knox. Sie beinhaltet Samsung Sicherheits- und Verwaltungslösungen, die die Mobilgeräte[1] ab dem ersten Einschalten vor Angriffen schützen können. Dabei wirkt ein kombinierter, auf mehreren Ebenen aktiver Schutz aus hardware- und softwaregestützten Maßnahmen, um potenzielle Bedrohungen abzuwehren. Über die hardwaremäßig integrierte Knox Plattform werden alle Daten standardmäßig mit einem zertifizierten[2] und von Regierungsbehörden anerkannten[2] Algorithmus verschlüsselt, damit bei Diebstahl oder Verlust nicht auf sensible Daten zugegriffen werden kann. Zudem können Daten in sicheren Containern auf dem Gerät isoliert werden. Neben dem gerätebezogenen Schutz bietet Samsung die vielseitige Knox Suite, die eine Integration mobiler Sicherheitslösungen in die bestehende IT-Infrastruktur und eine komfortable Verwaltung der miteinander verbundenen Lösungen ermöglicht.

### Eine Komplettlösung für Unternehmensmobilität: Knox Suite

In der Knox Suite werden die verschiedenen Knox-Einzellösungen gebündelt zur effektiven Sicherung, Bereitstellung, Verwaltung und Analyse mobiler Unternehmensgeräte über den gesamten Lebenszyklus hinweg. Dies beinhaltet den bereits erwähnten Schutz für jedes Gerät – sowohl integriert als auch verwaltet. Zudem ermöglicht die Knox Suite eine einfache Bereitstellung und Konfiguration der Geräte – und das sofort nach dem Hochfahren. Und nicht zuletzt ist eine weitreichende Geräteverwaltung inbegriffen, mit der Sie in allen Phasen sicher sein können, dass die Geräte zuverlässig von der IT kontrolliert werden.

### Secured by Knox

Apropos Geräte: Die Geräte der Galaxy Enterprise Edition – darunter auch viele robuste Ruggedized Smartphones und Tablets – sind speziell ausgerichtet auf die Anforderungen von Unternehmen in Sachen Leistungsfähigkeit, Funktionalität und Ausstattung. Die Geräte bieten zudem vier bis fünf Jahre garantierte Sicherheits-Updates ab Markteinführung sowie zwei Jahre Marktverfügbarkeit. Auch die Knox Suite für die umfangreiche Geräteadministration ist für ein Jahr bereits enthalten.[3]

Erfahren Sie mehr über mobile Sicherheit mit Samsung:

***https://www.samsungknox.com/de***

**Quellen:**

1 Samsung Knox ist auf allen seit 2015 eingeführten Mobilgeräten bereits ab Werk integriert.

2 https://www.samsungknox.com/de/knox-platform/knox-certifications

3 Knox Suite ist bei Erwerb der Enterprise Edition Modelle im ersten Jahr kostenlos mitenthalten. Danach ist eine kostenpflichtige Verlängerung bei einem Knox-Deployment Partner wahlweise um ein, zwei oder drei Jahr(e) möglich. Es findet keine automatische Verlängerung statt. Die Liste der Knox Deployment Partner kann auf samsungknox.com/de/resellers abgerufen werden. Zur Lizenzaktivierung ist ein Samsung Account und eine Registrierung auf samsungknox.com mit einer geschäftlichen E-Mail-Adresse (Business Domain) notwendig.

**Besuchen Sie uns auf der it-sa**
**Halle 7A,** Stand 616

# VON VIRTUELLEN ZU SICHEREN DATENRÄUMEN

## EINFALLSTORE FÜR CYBERKRIMINELLE

Durch das Abfangen unverschlüsselter E-Mails und angehängter Dateien sammeln Angreifende wichtige Informationen, die sie beispielsweise für die Erstellung von betrügerischen Phishings-Mails verwenden. Diese E-Mails erscheinen auf den ersten Blick seriös, doch hinter dem angezeigten, vertrauenswürdig wirkenden Absendenden verbirgt sich in der Regel eine andere Adresse. Sobald Mitarbeitende auf den scheinbar sicheren Link klicken oder einen manipulierten Anhang öffnen, wird Ransomware in die Systeme eingespielt.

Um ihre Systeme vor Cyberattacken zu schützen, setzen immer mehr Unternehmen, Organisationen und Behörden für den Datenaustausch auf virtuelle Datenräume. Diese hochgradig sicheren Online-Dokumentenspeicher und Kollaborationsbereiche ermöglichen mehreren Nutzenden einen standortunabhängigen Zugriff auf Dateien, die sie dort in der Regel ohne Größenbeschränkung ablegen und intern oder auch über Unternehmensgrenzen hinweg teilen können.

Doch nicht jeder virtuelle Datenraum bietet den gleichen Funktionsumfang. Datei- und Ordnermanagement, Datenschutz, die Verwaltung digitaler Rechte, Dokumentenablagen oder Benutzerfreundlichkeit können durchaus variieren.

Unternehmen, die ihre Daten in virtuellen Datenräumen teilen möchten, sollten bei der Wahl eines Anbietenden vor allem darauf achten, dass dieser über ein umfangreiches Sicherheitskonzept verfügt. Eine zusätzliche Orientierungshilfe bieten Zertifizierungen wie ISO 27001, eine weltweit anerkannte Norm für ein Informationssicherheitsmanagementsystem (ISMS), die festlegt, welche Bedingungen ein sicheres ISMS erfüllen muss.

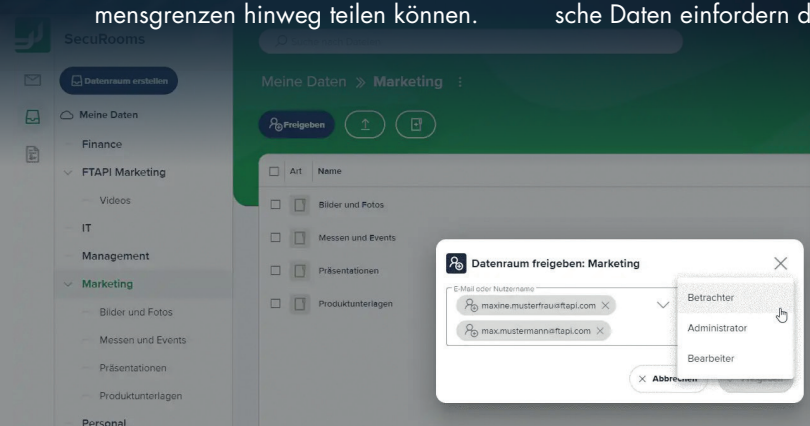
Siegel wie „Made/Hosted in Germany" informieren darüber, dass der Server von einem deutschen Anbietenden gehostet wird, sodass Behörden oder unbefugte Dritte, anders als bei Providern aus den USA, keine Einblicke in geschäftskritische Daten einfordern dürfen.

Ein sicherer Datenraum sollte sich vor allem durch folgende fünf Kriterien auszeichnen:

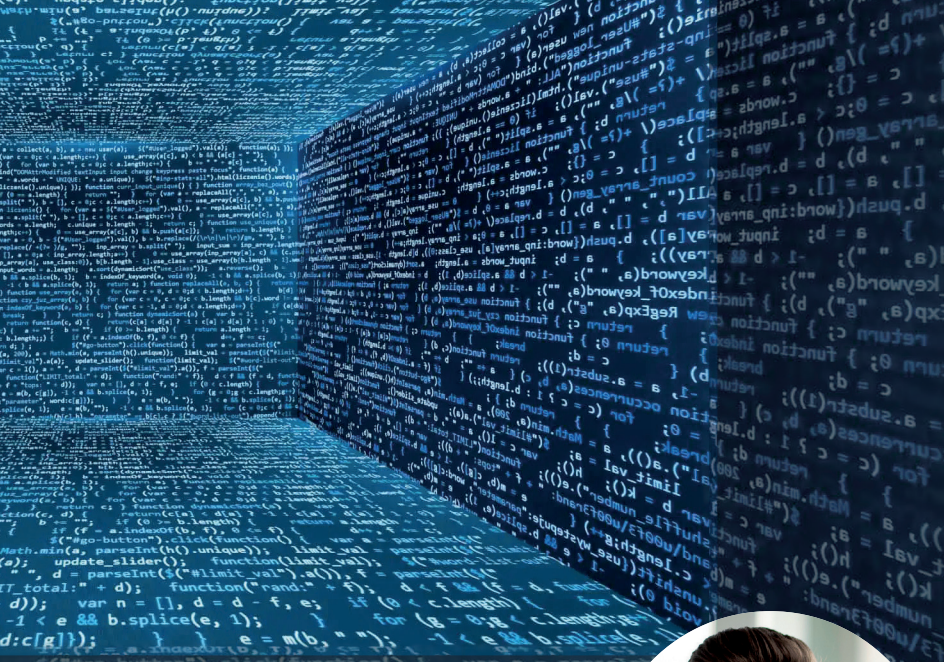
### 1. Ende-zu-Ende verschlüsselte Datenübertragung gewährleistet Sicherheit

Personenbezogene Daten sind durch die EU-DSGVO gesetzlich geschützt. Bei sensiblen Dateien, beispielsweise Finanzplänen, Patenten, Verträgen oder technischen Zeichnungen greift dagegen kaum ein gesetzlicher Mindestschutz. Trotzdem können geschäftskritische Informationen für Unternehmen überlebenswichtig sein und unterliegen einer strikten Geheimhaltung. Eine Offenlegung kann ernste Konsequenzen zur Folge haben, angefangen vom Betriebsstillstand, über Rufschädigung bis hin zu drastischen finanziellen Einbußen.

Im Gegensatz zu einer herkömmlichen Content-Collaboration-Plattform werden die Dateien in einem virtuellen Datenraum vollständig Ende-zu-Ende-verschlüsselt übertragen und abgelegt. Da sie an einem komplett separaten, durch Kontrollen gesicherten Ort gespeichert sind, ist es für Cyberkriminelle so gut wie unmöglich, unberechtigt auf Daten zuzugreifen und diese zu kompromittieren. Ein vorgeschalteter Virenscanner kann zusätzliche Sicherheit bieten.




Projektbeteiligte sollten zu einem virtuellen Datenraum ausschließlich die Zugriffsrechte erhalten, die sie für ihre jeweilige Rolle benötigen.



### 2. Flexible, feingranulare Rechtevergabe

Nur ein klar definierter Empfängerkreis darf zu einem virtuellen Datenraum Zugang erhalten. Jeder Projektbeteiligte sollte dabei – ganz im Sinne des Zero-Trust-Ansatzes – ausschließlich die Zugriffsrechte erhalten, die er oder sie für die jeweilige Rolle benötigt. Externe Partner können etwa nur Leserechte bekommen und Daten herunterladen. Mitarbeitende dagegen dürfen hinzufügen, löschen oder im größeren Rahmen Daten verwalten. Die Rechte können für den gesamten Datenraum vergeben werden oder nur für Teilbereiche, etwa für einzelne Dokumente.

Über Aktivitätsprotokolle behalten Admins dabei stets die genaue und transparente Übersicht über alle Prozesse im Datenraum. Sie können beispielsweise nachverfolgen, wer Dokumente angezeigt, heruntergeladen oder bearbeitet hat. Auf diese Weise ist es möglich, die Datenspuren präzise nachzuvollziehen und die Datensouveränität innerhalb des Unternehmens zu stärken.

> IN DEN AKTUELLEN ZEITEN DES DIGITALEN UMBRUCHS SIND UNTERNEHMEN FÜR SICHERE FREIGABEN, STRIKTE ZUGRIFFSKONTROLLEN UND EIN EFFIZIENTES, GLEICHZEITIG ABER GESCHÜTZTES TEILEN VON INFORMATIONEN ZUNEHMEND AUF DIGITALE PLATTFORMEN ANGEWIESEN.
>
> Kornelius Brunner, Chief Product Officer, FTAPI Software GmbH, www.ftapi.com

### 3. Zwei-Faktor-Authentifizierung

Ein zweistufiges Authentifizierungssystem ist eine effektive zusätzliche Sicherheitsmaßnahme, um unberechtigte Zugriffe zu verhindern. Für die Authentifizierung müssen sich Nutzende am System neben ihren Zugangsdaten mittels eines zusätzlichen Faktors ausweisen – beispielsweise durch spezielle Sicherheitstoken oder das Smartphone. Auf diese Weise erhalten Unbefugte keinen Zutritt zum Datenraum. Auch dann nicht, wenn Passwörter in falsche Hände gelangen sollten.

### 4. Ortsunabhängiger Zugriff

Mitarbeitende und Projektteilnehmende können auf virtuelle Datenräume ortsunabhängig zugreifen. Egal, ob vom Laptop zuhause oder vom Smartphone unterwegs, die sichere Aufbewahrung und Weitergabe vertraulicher Geschäftsinformationen ist dabei in keinem Moment gefährdet. Die Dateien werden in nahezu unbegrenzter Größe verschlüsselt abgelegt und für ausgewählte Kollegen, Partner oder Kunden freigegeben. Für international operierende Unternehmen sind virtuelle Datenräume darüber hinaus eine adäquate Möglichkeit, um sensible oder zeitkritische Informationen einer großen Zahl von Projektbeteiligten über Abteilungs- und Standortgrenzen hinweg zum Lesen und Bearbeiten zur Verfügung zu stellen.

### 5. Sicherer Betrieb in der Cloud

Vieles spricht dafür, virtuelle Datenräume in einer Cloud zu betreiben, liegt doch der Sicherheitsstandard von Cloud-Providern in der Regel höher als bei firmeneigenen Servern. Da die Verantwortung für die Wartung und Erstellung von Backups beim Datenraum-Anbietenden liegt, werden Updates und neue Features automatisch eingespielt, meist über Nacht, um unnötige Ausfallzeiten zu vermeiden. Damit sind die Systeme immer auf dem neuesten Stand und mögliche Schwachstellen werden effizient geschlossen. Außerdem gehören professionelle, hochsichere Rechenzentren sowie die Einhaltung von gesetzlichen Vorgaben wie der DSGVO hier zum Standard.

In den aktuellen Zeiten des digitalen Umbruchs sind Unternehmen für sichere Freigaben, strikte Zugriffskontrollen und ein effizientes, gleichzeitig aber geschütztes Teilen von Informationen zunehmend auf digitale Plattformen angewiesen. Virtuelle Datenräume schließen dank ihrer Sicherheit und transparenten Benutzerfreundlichkeit hier eine kritische Lücke. Sind die browserbasierten Datenräume, die Geräte-unabhängig und ohne Download und Installation von Clients funktionieren, einmal vom Unternehmen und den Mitarbeitenden adaptiert, wird sich die Verwendung anderer, kostenfreier Lösungen verringern und das Entstehen einer Schatten-IT vermieden.

***Kornelius Brunner***

# REVEELIUM UEBA: INNOVATIV & VIELFÄLTIG

## INTELLIGENTES SIEM UEBA, BEDROHUNGSJAGD, XDR UND SOAR & MORE

Mit ITrust kommt ein neuer Player aus Frankreich auf den deutschen Markt. Gerade SOCs stehen vor neuen Herausforderungen. Ein unverzichtbares Werkzeug für eine tiefgreifende Verteidigung und die einzige Möglichkeit, die Erkennung moderner Bedrohungen zu gewährleisten. Warum ein SIEM, warum KI, was sind die zu vermeidenden Fallstricke?

Die Plattform besteht in Summe aus vier Teilen:

**1. SOC**
Ausgwählte Technologien für das Security Operations Center
**2. Reveelium**
Optimierung der Cybersicherheit mit Hilfe Künstlicher Intelligenz
**3. IKare**
Vereinfachung des Schwachstellenmanagements mit IKare
**4. SOC Reveelium**
einem EDR – ACSIA-Modul

Cybersicherheit wird künftig nur mit Hilfe von Künstlicher Intelligenz zu beherrschen sein.

Werfen wir hier einen Blick auf Reveelium. Dies ist eine SIEM UEBA Verhaltensanalysetechnologie, die die Erkennung von bekannten und unbekannten Cyber-Bedrohungen ermöglicht: APT (Advanced Persistent Threat), unbekannte Malware, Viren, Lecks, Datendiebstahl, abnormales Verhalten innerhalb von Informationssystemen und die Verfolgung der Spuren des Cyberangriffs.

Durch die Kombination von KI, Threat Hunting, Threat Intelligence und SOAR („Security, Orchestration, Automation and Response to Computer Security Incidents") ermöglicht Reveelium die Nutzung von Ereignissen, die das Informationssystem bedrohen könnten, und die Vorwegnahme von Bedrohungen.

Die Software erkennt dank seiner UEBA-Technologie (User and Entity Behaviour Analysis) abnormales Maschinen- und Nutzerverhalten: Sobald es installiert ist, identifizieren die Algorithmen des unüberwachten Lernens das Verhalten aller im System vorhandenen Assets und ermitteln relevante und kontextualisierte Anomalien.

Der verwendete Ansatz kombiniert in der Praxis Methoden des maschinellen Lernens und des Deep Learning aus der akademischen Forschung im Bereich der Cybersicherheit: Graphentheorie, temporale neuronale Netze vom Typ LSTM, überwachte und nicht überwachte Klassifizierungsalgorithmen und so weiter.

Mode Forensik ist ein neuer Begriff. Diese innovative Technologie ermöglicht die Offline-Analyse von Protokollen, um forensische Operationen durchzuführen oder eine nachträgliche Kontrolle der Aktivitäten des Informationssystems vorzunehmen. In dieser so genannten „Cold Log Control"-Konfiguration können die Protokolle in eine Art Reveelium-Quarantäne Raum eingespeist werden, um sicherzustellen, dass die traditionellen Kontrollen keine Computerbedrohung oder abweichendes Verhalten übersehen haben, die ein Merkmal eines Cyberangriffs oder internen Betrugs sein könnten.

### 360°-Visualisierung von Bedrohungen

Das Dashbooard bietet einen globalen Überblick über alle betroffenen Ressourcen Ihres Netzwerks. Die Lösung betrachtet das gesamte Netzwerk hervor, das von der Ausbreitung bedroht sein könnte, identifiziert die zugehörigen IP-Adressen


Verringerung von Fehlalarmen. Reveelium reduziert die Anzahl der Fehlalarme des Informationssystems. Es synthetisiert die Bedrohungen, die sich aus der Menge der als Bedrohung identifizierten Warnmeldungen ergeben. Diese innovative Methode ermöglicht es den Teams, sich ausschließlich auf die identifizierte Bedrohung zu konzentrieren, ohne Zeit mit der Analyse von Hunderten von oft unpassenden Warnmeldungen zu verschwenden.

und ermöglicht es so, eine Ausbreitung zu vermeiden.

### Anomalien

Die Identifizierung von abnormalem Verhalten geschieht durch einen Entscheidungsbaum. Das System identifiziert in der SI den Ursprung und den Weg des Verhaltens, das als abnormal angesehen wird, und stellt dessen Merkmale dar. Es ist in der Lage, die Warnmeldungen zu identifizieren, die eine Bedrohung darstellen, und das Entscheidungsschema darzustellen, das zur Erhöhung des Schweregrads dieser Bedrohung geführt hat. Sobald die Bedrohung nachgewiesen und als solche erkannt wurde, findet die Technologie ähnliche Verhaltensweisen im Informationssystem und kann potenzielle Angriffsszenarien zum Schutz vor dieser Bedrohung aufzeigen.

### Anwendungsfälle

Zusätzlich zur Parametrisierung der Algorithmen mit Metadaten und Anwendungsfällen, die der Cybersicherheit dienen, wird den Anwendern die Möglichkeit angeboten, auf Anfrage Anwendungsfälle zu entwickeln, um Reveelium im Kontext einer spezifischen Kontextualisierung zu nutzen.

### KPIs

Die Messung von Bedrohungen mit Hilfe der Künstlicher Intelligenz. Die Software erstellt automatisch Berichte zur Quantifizierung seiner Tätigkeit und enthält Indikatoren für Bedrohungen: Betroffene IP(s), Anzahl der Warnungen pro Bedrohung, Kritikalitätsindikator, Histogramm, Entwicklung des Risikos der Bedrohung im Laufe der Zeit, Entscheidungsbaum usw.

**Fazit:** In der Gesamtbetrachtung handelt es sich um ein Sicherheitstool der neuen Generation, dessen Reichtum und Stärke in der Verwendung von drei sich ergänzenden Engines liegt. Alle Engines arbeiten auf einer leistungsstarken Datenbank, die in der Lage ist, große Mengen an Daten und Protokollen von IT- oder OT-Sensoren zu verarbeiten.

Geschäftsregeln werden in einem Business Correlator implementiert und befolgt. Die grafische Benutzeroberfläche (GUI) ermöglicht die Anzeige von Korrelationen und die Verfolgung von Abweichungen, so dass der Benutzer interagieren und Feedback geben kann.

***Ulrich Parthier | https://www.itrust.fr/en***

## DIE HIGHLIGHTS IM ÜBERBLICK

- UEBA/Verhaltensanalyse: Die Macht der KI bei der Erkennung
- Angriffserkennung der neuesten Generation (APT): Algorithmen ermöglichen die Erkennung von unbekannten Bedrohungen
- Reduzierung von Fehlalarmen: Geht nur auf qualifizierte Bedrohungen ein
- Erhebliche Verkürzung der Erkennungszeit: Die Erkennungszeit wird von 16 Monaten auf 1 Stunde reduziert.
- Verwendung der MITRE-Matrix: Die Verwendung eines anerkannten Repository dient als gemeinsame Sprache
- Die französische Lösung unterliegt nicht den Patriot & Cloud Acts: Sichere Architektur, NIS / PDIS / OIV / OSE kompatibel
- Agentenlose und nicht-intrusive Lösung: Keine Beeinträchtigung, ein zentraler Kollektor, keine Sonden zu installieren
- Einsatz im ITrust SOC oder als eigenständige Lösung mit Log-Ingest: Möglichkeit, die Art der Verwaltung vollständig zu definieren: intern, hybrid, ausgelagert

## FÜR SOCS IST EIN STRESSTEST VERFÜGBAR

**Der Cyber Threat Report**
Edition 2021/2022
kann hier kostenlos
heruntergeladen werden:
***https://bit.ly/3UjOK22***

# CYBER THREAT REPORT

## GEFAHR DURCH BRAND IMPERSONATION WÄCHST

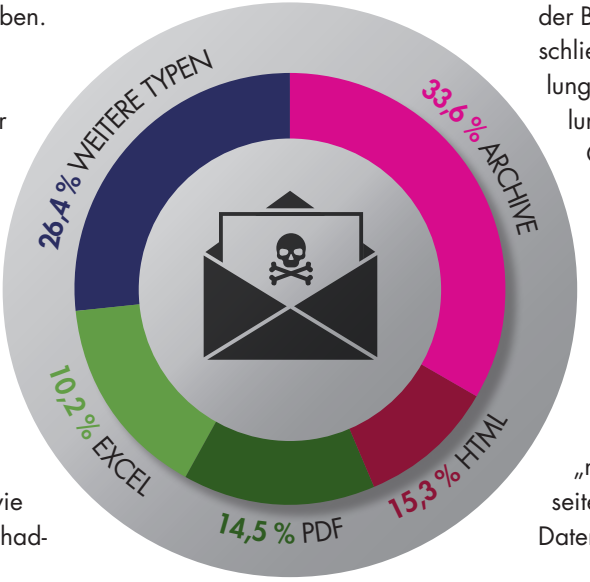
Cyberkriminalität bleibt eine der größten Bedrohungen weltweit: Im neuen Cyber Threat Report Edition 2021/2022 Hornetsecurity die neusten Insights und Daten zur aktuellen Bedrohungslage mit Fokus auf den Haupteinfallsvektor E-Mail-Kommunikation. Der Report gibt unter anderem Einblicke in die Entwicklungen des Spam- und Advanced Threat-Aufkommens, zeigt auf welche Branchen derzeit am meisten bedroht sind und identifiziert die am häufigsten verwendeten Methoden bei Cyberangriffen. Zudem werden die „Threat-Highlights" des vergangenen Jahres hervorgehoben.

### Potenzielle Bedrohung

Als Hauptkommunikationsmittel für Unternehmen ist die E-Mail eines der Haupteinfallstore für Cyberkriminalität. Die Threat Researcher des Hornetsecurity Security Labs stellten fest, dass 40 Prozent aller eingehenden E-Mails des gesamten E-Mail-Verkehrs im Untersuchungszeitraum eine potenzielle Bedrohung darstellten. Darunter fallen vor allem Spam, Phishing E-Mails sowie Advanced Threats, wie CEO-Fraud und jegliche Art von Schadsoftware.

Phishing, schädliche Links und Ransomware zählen zu den populärsten Angriffstaktiken der Hacker. Beliebt ist vor allem die „Brand Impersonation". Hierfür kopieren Cyberkriminelle das Corporate Design der imitierten Firma und benennen die Absenderadresse so, dass sie von der originalen E-Mail-Adresse kaum zu unterscheiden ist. Ziel ist es an die Zugangsdaten der Nutzer zu gelangen oder über versteckte Links Malware zu verbreiten. Mit 16,5 Prozent ist die Deutsche Post unter den Top 5 der am häufigsten imitierten Marken.

**MEISTGENUTZTE DATEI-TYPEN IN SCHÄDLICHEN E-MAILS**




### Ransomleaks: Trend nimmt größere Ausmaße an

Vor knapp zwei Jahren noch in den Kinderschuhen, sind Ransomleaks mittlerweile weit verbreitet. Diese stellen eine Erweiterung der bisher bekannten Angriffe mit Ransomware dar: Bei Ransomleak-Angriffen werden sensible Daten der Betroffenen zunächst kopiert und anschließend verschlüsselt. Wird die Zahlung des Lösegelds für die Entschlüsselung allerdings abgelehnt, drohen die Cyberkriminellen, die kopierten Daten auf sogenannten Leak-Webseiten zu veröffentlichen.

Auf der Leak-Website der Ransomware REvil wurden rund 140 Daten veröffentlicht, beinahe täglich kommen neue hinzu. Damit liegt die Hackergruppe jedoch „nur" auf dem 5. Platz der Leak-Webseiten mit den meisten veröffentlichten Daten von Ransomleak-Opfern.

***www.hornetsecurity.com/de/***

# PROTEKT 2022

## DIE KRITIS-KONFERENZ IN LEIPZIG

**protekt**
**2.–3.11.2022**
leipzig

konferenz für
den schutz kritischer
infrastrukturen

Vor dem Hintergrund des Krieges in der Ukraine und den Nachwirkungen der Corona-Pandemie stehen kritische Infrastrukturen vor großen Herausforderungen. Drohende Engpässe in der Energieversorgung zählen ebenso dazu wie gestörte Lieferketten und eine zunehmende Zahl an Cyberangriffen. Diesen und vielen weiteren wichtigen Themen rund um den Schutz kritischer Infrastrukturen widmet sich die protekt (2. bis 3. November 2022 in Leipzig).

Die protekt ist die einzige Konferenz in Deutschland, die den Schutz kritischer Infrastrukturen vollumfänglich beleuchtet. Sie thematisiert gleichermaßen IT-Sicherheit und den physischen Schutz. Mit ihrem Konzept aus Vorträgen, Workshops und Diskussionsrunden sowie begleitender Ausstellung und vielfältigen Networking-Möglichkeiten hat sie sich in den vergangenen Jahren als wichtiger Treffpunkt von KRITIS-Betreibern und der Sicherheitsindustrie etabliert. Mit Spannung erwartet wird die Keynote von Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Er wird interessante Einblicke in die Rolle des BSI bei der Cyber-Sicherheit kritischer Infrastrukturen liefern.

Die etablierte Konferenz versammelt Experten aus ganz Deutschland, vermittelt aktuelles Know-how und treibt den sektorenübergreifenden Austausch voran. Die Schirmherrschaft haben Nancy Faeser, die Bundesministerin des Innern und für Heimat, und Thomas Popp, Sächsischer Staatssekretär für Digitale Verwaltung und Verwaltungsmodernisierung, übernommen. Zum Einzugsgebiet zählt inzwischen auch Österreich.

***www.protekt.de***

# CYBER SECURITY

## FRÜHZEITIGE IDENTIFIKATION

Für Finanzdienstleister ist der Schutz vor Cyber-Angriffen ein zentrales Thema, weil sie bei der Verarbeitung sehr sensibler Kunden- und Geschäftsdaten an regulatorische und gesetzliche Vorgaben gebunden sind. Infolge der steigenden Nutzung von Cloud Services gelten neue, stärkere regulatorische Anforderungen, die von Banken, Versicherungen und Vermögensverwaltungen umzusetzen sind. Bereits 79 Prozent der Finanzdienstleister sehen in diesen einen wesentlichen Einflussfaktor für die IT-Security ihres Unternehmens.

Finanzdienstleister stehen daher vor der Herausforderung, die Erwartungen der Branche nach einer intensiveren Cloud-Nutzung zu erfüllen und entsprechende Cloud-Strategien zu entwickeln. 29 Prozent der befragten Finanzdienstleister verfolgen bereits eine Cloud-First-Strategie. Weitere 37 Prozent verlagern einzelne Anwendungen in die Cloud (Hybrid-Cloud-Ansatz) und 29 Prozent planen die Entwicklung einer Cloud-Strategie innerhalb der nächsten zwei Jahre. Lediglich fünf Prozent der befragten Finanzdienstleister wollen auch zukünftig keine Cloud-Strategie entwickeln. Dies sind ausgewählte Ergebnisse der Lünendonk-Studie 2022 „Von Cyber Security zur Cyber Resilience – wie Finanzdienstleister auf die neue Bedrohungslage reagieren", die in Zusammenarbeit mit KPMG erstellt wurde.

### Fokus auf Identifikation, Prävention und Überwachung

Durch die zunehmende Digitalisierung von Schnittstellen und Prozessen, zunehmende Cloud-Nutzung und höhere Anforderungen an Daten- und IT-Sicherheit rückt Cyber Security in den nächsten Jahren immer mehr in den Fokus.

Die Mehrheit der befragten Finanzdienstleister (94 %) wollen sich deshalb innerhalb der kommenden zwei Jahre stärker auf das Identity & Access Management (IAM) fokussieren, also die Verwaltung der Benutzerkonten und Zugriffsberechtigungen. Weitere 82 Prozent setzen ihren Schwerpunkt im Bereich Vulnerability Management, also die präventive Erkennung und Behebung von Schwachstellen in der eigenen IT-Infrastruktur beziehungsweise im gesamten Ökosystem.

Aufgrund von steigenden regulatorischen und gesetzlichen Anforderungen bei der Cloud-Nutzung, der Speicherung von Kundendaten (DSGVO) und einer zunehmenden Anzahl von Angriffen in der Branche rückt für die Finanzdienstleister auch der Bereich Security Monitoring mehr in den Fokus. In den kommenden Jahren wollen sich 94 Prozent der Finanzdienstleister verstärkt mit Security Monitoring beschäftigen.

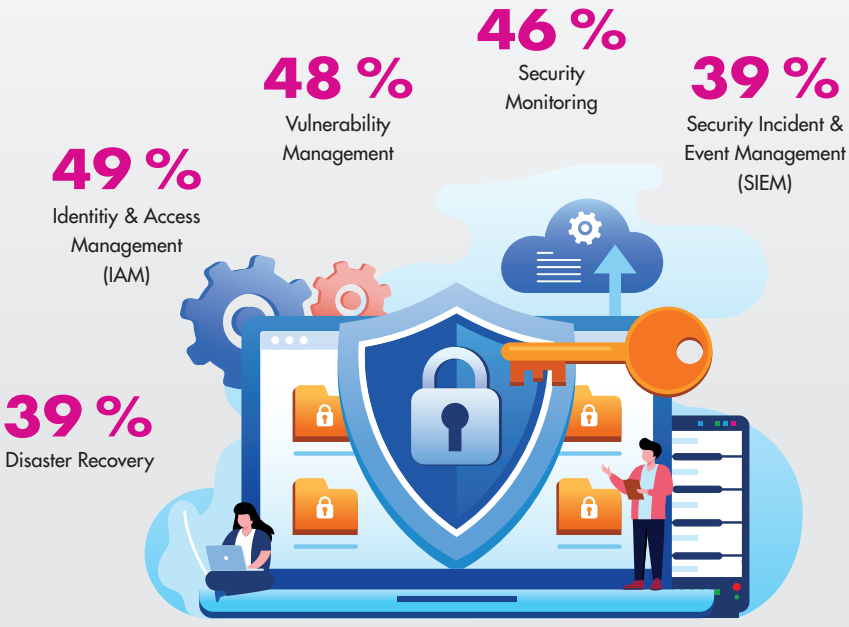
Um nach einem Cyber-Angriff die Kontrolle über die Prozesse zurückzuerlangen, sind Business-Continuity-Strategien zwingend erforderlich. Da auch die Finanzaufsicht entsprechende Disaster-Recovery-Konzepte fordert, wollen sich 90 Prozent der Befragten in den Jahren 2022 bis 2023 auf die Optimierung ihrer Recovery-Maßnahmen fokussieren.

### Externe Dienstleister

Aufgrund der Vielzahl von Aufgaben und eines gleichzeitigen Mangels an Inhouse-Expertise setzen viele Finanzdienstleister auf externe Unterstützung. Besonders im Bereich Recovery arbeiten 49 Prozent der Unternehmen mit externen Dienstleistern zusammen, um ihre Business-Continuity-Prozesse zu verbessern. Ebenso in den Bereichen Incident Response (50 %) und Cloud Security (54 %) benötigen viele Unternehmen Unterstützung von externen Fachkräften.

***www.luenendonk.de***

### WELCHE MASSNAHMEN STEHEN STARK IM FOKUS?



itsa EXPO CONGRESS

HOME OF IT SECURITY

# HIT HACKERS HARD

## LET'S TALK ABOUT IT SECURITY!

25. – 27. Oktober 2022
Nürnberg, Germany

Jetzt Gratis-Ticket sichern:
itsa365.de/hit-hackers-hard

NÜRNBERG MESSE

# ATTRIBUTBASIERTES DATA MASKING FÜR SAP

## DEN SCHUTZ VON ERP-DATEN EFFEKTIV VERBESSERN UND COMPLIANCE-RISIKEN DEUTLICH REDUZIEREN

SAP-Anwendungen enthalten große Mengen sensibler Daten. Von geschützten personenbezogenen bis hin zu privilegierten Finanzinformationen bergen diese stets auch Risiken, denen Unternehmen begegnen müssen, da es in SAP ERP von Haus aus keine Maskierungsfunktionen zur passgenauen Anonymisierung in den Ansichten gibt. Die ungehinderte Offenlegung von Daten stellt somit ein potenzielles Leck dar und bietet eine riesige Angriffsfläche, die ausgenutzt werden kann. Obwohl Add-ons und Lösungen von SAP und Drittanbietern existieren, um das Problem anzugehen, bestehen immer noch erhebliche Herausforderungen. Hier setzt das Konzept des attributbasierten Data Maskings an.

Nicht erst seit der zunehmenden Internationalisierung, seit Corona und vermehrtem Homeoffice sind prozessrelevante, aber sensible Daten in Gefahr, auch von externen oder internen Betrachtern eingesehen zu werden, deren Einsicht situativ oder generell weder nötig noch gewünscht ist. Konkret bedeutete dies: Wenn der Mitarbeiter der Personalabteilung aus dem Ausland arbeitet und Stammdatenpflege betreibt, sollten weder ein Passant, der ihm über die Schulter blickt, noch der Sitznachbar ungehinderten Einblick auf sensible Daten bekommen. Ein Packer muss anhand der Materialstammnummer natürlich wissen, welches Paket er nehmen soll, aber er muss nicht im Detail wissen, welchen Inhalt es hat. Wenn ein Vertrieb mit Stammdaten arbeitet, um Angebote zu erstellen, muss er in der Stammkarte das richtige Produkt finden, die richtige Verpackungseinheit, das Gebinde sehen können, jedoch nicht alle Einkaufspreise kennen.

### Data Loss Prevention

Data Masking erstreckt sich also nicht allein auf die Reduzierung missbräuchlicher Ansicht (Fraud) personenbezogener Daten und ist wesentlich weiter gefasst als die reine Anonymisierung und Pseudonymisierung von Personen- und Adressdaten. Vielmehr lassen sich alle denkbaren Datentypen maskieren. Ziel des Maskierens der Originaldaten ist stets die sogenannte Data Loss Prevention, das Problem von Datendiebstahl, Datenmissbrauch oder anderen Formen von Datenkriminalität dadurch zu lösen, dass man die Ansichten der Datenbasis selbst verändert: „Vereinfacht gesagt", so Ralf Kempf, CTO des SAP-Securityspezialisten Sast Solutions sowie Vice President ABAP Architecture der neuen multinationalen Pathlock-Gruppe, „geht es um den Schutz von Daten, die notwendig und da sind, die aber nicht jeder sehen soll, um das Einschränken der Ansichten auf situativ relevante Informationen."

ES GEHT UM DEN SCHUTZ VON DATEN, DIE NOTWENDIG UND DA SIND, DIE ABER NICHT JEDER SEHEN SOLL, UM DAS EINSCHRÄNKEN DER ANSICHTEN AUF SITUATIV RELEVANTE INFORMATIONEN.

Ralf Kempf, CTO Sast Solutions und Vice President ABAP Architecture der Pathlock-Gruppe, www.sast-solutions.de

### Datenmaskierung in einem Regelsatz

Die meisten Data-Masking-Lösungen von SAP und Drittanbietern stehen diesbezüglich immer noch vor einigen Herausforderungen, weil sie rein auf der Ebene von Berechtigungen operieren. Statische Maskierungsrichtlinien berücksichtigen dabei nicht den Kontext des Zugriffsrisikos und zwingen zu einem Kompromiss zwischen Datensicherheit und Zugänglichkeit. Privilegierte Benutzer können auf sensible Datenfelder zugreifen, selbst wenn dies in einem speziellen Kontext nicht erforderlich oder gewünscht ist. Add-ons zur Datenmaskierung erfordern zudem Anpassungen, die in jedem Feld der Anwendung repliziert werden müssen, was zu einer nicht skalierbaren Ad-hoc-Lösung führt. Im Gegensatz zu solchen Standard-Maskierungslösungen zentralisiert der Pathlock-Ansatz von Sast Solutions die Durchsetzung der Datenmaskierung in SAP in einem einzigen Regelsatz, um Daten in der gesamten Anwendung zu definieren und zu maskieren, und setzt zusätzlich dynamische Richtlinien ein, die

den Risikokontext einbeziehen, um die sensiblen Daten zielgenauer zu schützen, ohne dass für die Implementierung zusätzliche Anpassungen an SAP nötig sind.

Diese attributbasierte Maskierungsfunktion bedeutet eine fein abgestufte Kontrolle darüber, welche Informationen für einen bestimmten Benutzer in einer bestimmten Situation maskiert werden. Dies ist etwa dann besonders wichtig, wenn ein multinationales Unternehmen missbräuchliche Ansichten verhindern will. Daten werden beispielsweise maskiert bei Zugriffen aus Ländern, die nicht zu den Unternehmensstandorten gehören, die von remoten Arbeitsplätzen von außerhalb des Netzwerks, unbekannten IP-Adressen oder VPNs ausgehen oder außerhalb der jeweiligen Geschäfts- oder plausiblen Uhrzeiten stattfinden. Eigentlich lesbare und für die Rolle erlaubte Inhalte sind so je nach Ausprägung von frei konfigurierbaren Attributen wie dem User, der IP-Adresse, Uhrzeit, von Ländern beziehungsweise Standorten, der Zugriffsart – Remote-Arbeit von außerhalb oder Zugriff innerhalb des Netzwerks – oder der Netzwerk-Art (etwa VPN) nicht sichtbar. „Erfolgt ein Zugriff mit ungewöhnlichen Parametern, werden je nach Attribut für den konkreten Fall unnötige Daten auch nicht lesbar sein“, fasst Kempf zusammen.

**Risiken minimieren**

Dies ist allein über User-Berechtigungen so nicht umsetzbar und berücksichtigt die je nach Branche unterschiedliche Kritikalität etwa von Stammdaten wie Personal-, Lokations-, Logistikdaten sowie Lieferanteninformationen oder Stücklisten, Einkaufspreisen und Rezepturen. Attributbasiertes Data Masking bedeutet hier einen erheblich verbesserten Schutz sensibler Unternehmensdaten durch feingranulare Einschränkung der Ansichten. Die richtlinienbasierte dynamische Maskierungsfunktion der zentralisierten und skalierbaren Maskierungslösung bietet Unternehmen damit zusätzlich zum Berechtigungsschutz eine individuell anpassbare Kontrolle darüber, welche sensiblen Datenfelder sie für einen bestimmten Benutzer in einer konkreten Situation maskieren wollen. Durch die Implementierung einer vollständigen oder teilweisen Maskierung eines Datensatzes minimiert sie damit das Risiko einer Datenpanne und erfüllt auch Verschlüsselungs- und Anonymisierungsanforderungen etwa von Aufsichtsbehörden.

Durch das Herausfiltern sensibler Daten auf der Darstellungsebene ohne zusätzliche Anpassungen an SAP entsteht kein zusätzlicher Wartungsaufwand für Aktualisierungen, aber es gelingt in hohem Maße, den Schutz von ERP-Daten zu verbessern und Compliance-Risiken zu reduzieren. Dies gilt für sensible Daten in Produktions- und Nicht-Produktionsumgebungen gleichermaßen. Kombiniert man das attributive Data Masking dann zusätzlich mit einem Data-Loss-Detection-Konzept und einer guten Echtzeitüberwachung der Abweichungen von Compliance-Vorschriften, führt dies zu einer signifikanten Steigerung des Datenschutzes in einer Qualität, die so kaum eine andere Lösung weltweit bieten kann.


# ONLINE-BETRUG

## PHISHING-MAILS ERKENNEN

Die Zahlen sprechen für sich: Der durch Cyberkriminalität verursachte Schaden beträgt in Deutschland jährlich 40 bis 70 Millionen Euro.

Phishing ist eine Variante des digitalen Identitätsdiebstahls und betrifft in erster Linie Banken (25 %), globale Internetportale (20%) und soziale Netzwerke (12 %). Allein der durch Phishing zwischen 2010 und 2015 in Deutschland verursachte finanzielle Schaden im Online Banking beträgt 123 Millionen Euro.

***www.betrugstest.com***

An diesen Merkmalen erkennt man eine präparierte **Phishing-E-Mail:**

direkt@sparkasse.de
Von: Ihre Sparkasse — Absender trägt einen bekannten Namen
An: undisclosed recipients; — Verteiler-Liste als Empfänger
Cc:
Betreff: Online Banking Zugang - Dringend! — Handlungsaufforderung
ZIP — Komprimierte Datei im Anhang

Sehr geehrter Kunde, — Unpersönliche Anrede

Bitte beachten Sie, dass Ihr Online-Banking Zugang bald abläuft. Ihr Nutzerkonto wurde temporer gesperrt. Uber den folgenden Link, sie können die Sperre deaktivieren:
Rechtschreibung, Grammatik, seltsame Sonderzeichen

http://goonswiss.t15.org
Hier Klicken >> — Der Link verweist auf eine unbekannte URL

Nach Abschluss der Bestätigung wird Ihr Nutzerkonto automatisch freigeschaltet. Kommen Sie dieser E-Mail innerhalb 14 Tagen nicht nach, ist die Freischaltung nur über den Postweg möglich. Dabei wird eine Bearbeitungsgebühr in Höhe von 19,95€ fällig, welche wir anschließend von Ihrem Konto abbuchen werden.

Druckaufbau und weitere Handlungsaufforderungen

Respektvoll,
Ihre Sparkasse — Untypische Redewendungen

Falls Sie auf den Link geklickt haben, werden Sie auf eine **präparierte Webseite** geleitet:

Diese Webseite wurde als Betrugsversuch gemeldet
und gemäß der Sicherheits-einstellungen blockiert.

Der PHISHING-FILTER des Browsers sollte automatisch vor der betrügerischen Seite warnen.

http://sparkasse-daten-kontrolle.org
Bank
Ihr Anmeldename
Ihr Passwort

Kontrollieren Sie, ob die URL https beinhaltet und Verschlüsselung aktiv ist.

**PHISHING-URLS**
http://sparkasse-daten-kontrolle.org
http://123.456.789.123/amazon.de
http://paypal-kundensicherheit.de
http://banking.postbank-vd.com

**ECHTE URLS**
https://www.ihre-sparkasse.de
https://www.amazon.de
https://www.paypal.de
https://banking.postbank.de

Vergleichen Sie die URL der Seite mit der richtigen Adresse aus Ihren Favoriten.

### LOGIN-DATEN EINGEGEBEN?

Das können Sie jetzt noch tun:

Rufen Sie sofort eine Sperr-Hotline Ihrer Bank an. Diese ist rund um die Uhr erreichbar.

Kontaktieren Sie einen auf Internet-Betrug spezialisierten Rechts-anwalt.

Leiten Sie die Phishing-E-Mail an Ihre Bank oder sonstiges betroffenes Unternehmen weiter.

# MANAGED DETECTION AND RESPONSE

## IT-SICHERHEIT BEDARF DER EXPERTISE VON SICHERHEITSANALYSTEN

Komplexe mehrstufige Cyberattacken bedrohen nicht mehr allein große Unternehmen. Zunehmend sind auch kleine und mittelständische Unternehmen den Risiken wie Datendiebstahl, Spionage oder Ransomware ausgesetzt. Unternehmen mit kleineren Budgets, IT-Sicherheitsteams oder Managed Security Partnern fällt es daher immer schwerer, sich oder ihre Kunden zu schützen. Sie benötigen mehr denn je Verstärkung durch eine Managed Detection and Response (MDR).

Ein MDR-Dienst kombiniert moderne Sicherheitstechnologien mit der Kompetenz zertifizierter IT-Sicherheitsexperten in einem externen Security Operations Center (SOC). Der Dienst basiert auf grundlegenden Abwehrtechnologien und Sicherheitsplattformen. Zusätzliche Sensoren können über eine Extended-Detection-and-Response(XDR)-Erweiterung sicherheitsrelevante Informationen aus weiteren Quellen für einen umfassenden Schutz korrelieren. Diese Art von Dienst bietet einen Mehrwert, der für die meisten Unternehmen in der Regel außer Reichweite ist:

➜ **Erkennen, Beobachten und Abwehr von Gefahren rund um die Uhr:** Die Experten beobachten kontinuierlich Attacken über Endpunkte, Netzwerke und Cloud-Umgebungen hinweg. Bei einem Sicherheitsereignis übernehmen sie die führende Rolle, um Alarme zu priorisieren, Gefahren zu analysieren sowie Abwehrmaßnahmen zu empfehlen und durchzuführen.

➜ **Proaktives Threat Hunting:** IT-Sicherheitsexperten suchen aktiv nach Auffälligkeiten wie etwa Advanced Persistent Threats (APTs) in der Infrastruktur des Kunden. Letztere halten sich nach dem Eindringen oft längere Zeit in den Opfersystemen auf, um den eigentlichen Ernstfall vorzubereiten. Fileless Malware wird in dieser Zeit von einer herkömmlichen EDR unter Umständen nicht oder erst zu spät erkannt. MDR-Experten analysieren daher Anomalien interner und externer Quellen. Sie interpretieren die Informationen, welche die Künstliche Intelligenz (KI) einer Cyberabwehr ihnen liefert. Zusätzlich wissen sie um die aktuellen branchenbezogenen Risiken, die sich aus den dort eingesetzten Technologien oder Prozessen ergeben. Die Experten profitieren darüber hinaus von ihrem persönlichen Hintergrund aus militärischer IT-Abwehr sowie digitaler Strafverfolgung. Dort gewonnene Erfahrungen helfen beim Schutz gegen die immer noch menschlichen Hacker, die manuell Netze ausspähen wollen.

➜ **Verbesserte Abwehrabläufe:** Kunden und Managed Security Provider kooperieren eng mit den Sicherheitsanalysten im MDR SOC. Über ein eigenes MDR-Portal können sie direkt miteinander kommunizieren, die gezielten Alarme ebenfalls einsehen und ihre Systeme verwalten. Zugleich können sie über ein zentrales Dashboard empfohlene Abwehrmaßnahmen durchführen oder Risiken beheben.

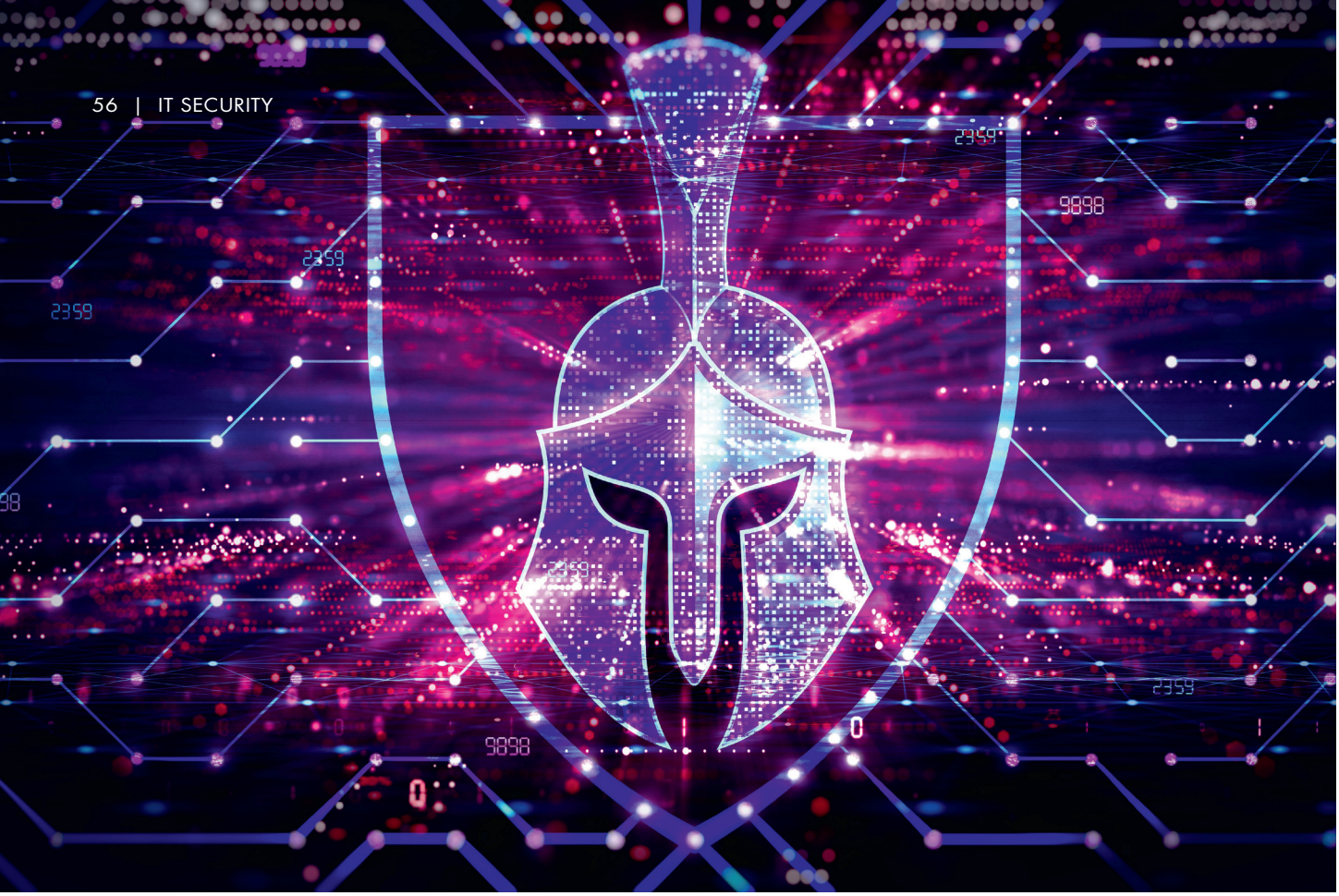
Die Implementierung einer MDR ist weniger aufwändig als man vermutet. Viele Prozesse des Onboardings erfolgen automatisiert. Zugleich starten die Experten zu Anfang der Zusammenarbeit mit einer Aufnahme der Sicherheitslage und einer ausführlichen Gefahrendiagnose. Dies ist der Auftakt für eine nachhaltige Zusammenarbeit zwischen Unternehmens-IT und MDR-Experten am Projekt IT-Sicherheit.

***Jörg von der Heydt | www.bitdefender.de***


Bildquelle: Bitdefender.

### KOSTEN INTERNER SOC IM VERGLEICH MIT EXTERNEM SOC

Im Vergleich zum internen SOC mit einem von der Anzahl der Nutzer unabhängigen Aufwand über drei Jahre von über 1,2 Millionen Euro kostet ein MDR-Dienst mit externem SOC bei 500 Usern mitsamt der eingekauften Expertise nur ein Zehntel: Jährlich ca. 40.000 Euro, 120.000 Euro auf drei Jahre gerechnet.



# IT-NETZWERK-SICHERHEIT

## MIT EINEM SASE-ANSATZ NETZWERK, SECURITY UND DIE CLOUD VERBINDEN

Digitalisierte, dezentralisierte IT-Infrastrukturen stehen natürlich nicht erst seit Corona auf der Agenda: Die Realitäten des Marktes sowie der verteilten Unternehmensorganisation und Produktionsabläufe diktieren konkrete technische Vorgaben für einen sicheren Zugriff auf Applikationen, Dienste und Daten von überall her. Denn immer mehr Ressourcen befinden sich außerhalb physikalischer Rechenzentren oder Unternehmensservern.

Mit dem Homeoffice hat sich die Angriffsfläche für Unternehmen rapide vergrößert. Aus Sicht der Unternehmens-IT ist das Heimnetzwerk eines Mitarbeiters nicht sicherer als ein öffentlicher WLAN-Zugang und damit ebenso risikobehaftet. Herkömmliche Sicherheitslösungen können ein Gerät nicht schützen, wenn es sich außerhalb des Unternehmensnetzwerks befindet. Die deutlich gestiegene Cloud-Akzeptanz infolge der digitalen Transformation und einem daraus resultierenden erhöhten Bedarf an Online- und digitalen Diensten, hat zu weiteren Komplikationen geführt.

All dies hat gezeigt, dass herkömmliche IT-Sicherheitslösungen für den Zugriff von extern recht wirkungslos sind, da die Mitarbeitenden nicht mehr mit den Sicherheitsarchitekturen vor Ort verbunden sind, auf die sie sich früher verlassen konnten.

### Vertrauen ist gut – eine Cloud-verwaltete Kontrolle ist besser

Das Konzept eines standortunabhängigen Arbeitens erfordert zwangsläufig eine ebenso neue Security-Strategie der Unternehmen, die auch einen effektiven Schutz vor Datenschutzverletzungen, etwa durch Ransomware-Attacken berücksichtigt. Die bloße Verlagerung der zentralisierten Security-Infrastruktur in die Cloud reicht nicht aus - die Cloud an sich muss Teil dieses neuen Ansatzes sein. Denn es braucht überall Sicherheitskontrollen, die sich über die Cloud verwalten und überwachen lassen. Wenn etwa Sales-Mitarbeitende von unterwegs SaaS-Anwendungen wie Office 365 nutzen und mit sensiblen Daten in der Cloud arbeiten, ist es extrem wichtig, dass Unternehmen eine Lösung anbieten können, die einen sicheren Zugriff auf ebensolche Dienste und Anwendungen gewährleistet.

Die in Unternehmen zunehmend akzeptierte Public Cloud spielt als zentraler Hub eine immer größere Rolle. Der Eintrittspunkt in diese IT-Architektur, der sogenannte Edge, wird dadurch zum entscheidenden Ort, um Aufgaben wie Verfügbarkeit und Sicherheit der Kommunikation zu leisten.

**Randschauplätze mit steigender Bedeutung**

Kriterium für das Erteilen des Zugriffs ist dabei nicht mehr die Zugehörigkeit zu einem Segment der IT-Infrastruktur, sondern die Identität der Benutzer. Am Ort der Zugriffsanfrage stehen in einer einzigen Konsole die notwendigen Werkzeuge bereit. Bekannt ist dieser Cloud-basierte Architektur-Ansatz als Secure Access Service Edge (SASE). SASE stellt Sicherheitsfunktionen überall dort bereit, wo sie benötigt werden: Büroarbeitsplätze oder Homeoffice, Coworking-Bereiche oder Niederlassungen, sogar an öffentlichen Orten wie Cafés. Zentralisierte Sicherheitslösungen können Remote-Arbeitende nur schwer schützen, und sie lassen sich nicht einfach in die Cloud verlagern, um dies zu erreichen. Während ein zentralisierter Ansatz in der Cloud den gesamten Datenverkehr über die Cloud abwickeln muss, sichert SASE Geräte und Netzwerke überall und bietet geräte- und standortunabhängig das gleiche Sicherheitsniveau.

Häufig haben Unternehmen einen lockeren Security-Ansatz, der mehrere Lösungen verschiedener Anbieter nutzt. Dies führt jedoch zu einer wenig organisierten Infrastruktur mit verschiedenen Komponenten, die jeweils für unterschiedliche Funktionen zuständig sind. SASE als eine integrierte Lösung hingegen konsolidiert die Prozesse und verringert damit die Komplexität sowie die Kosten.

**Maximaler Schutz**

Die eigentliche Herausforderung besteht nicht in der Wahl des Standorts einer Sicherheitslösung, sondern wie diese funktioniert. Es reicht nicht aus, den Sicherheitsstack aus dem Rechenzentrum herauszulösen und in die Cloud zu verlagern. Viel wirkungsvoller ist es, Standorte, IoT-Geräte, Menschen und die Cloud sicher und effizient miteinander zu verbinden. Darum geht es im Kern bei SASE.

Um ein effizientes Sicherheitsniveau mit SASE zu gewährleisten, sollten die folgenden Dienste integriert sein:

- SD-WAN (Software Defined Wide Area Network), um mehrere Büros kosteneffizient und ausfallssicher miteinander zu verbinden.
- Firewall-as-a-Service-Funktionen zum SD-WAN-Netzwerk, welche die Sicherheit des Unternehmensnetzwerks zusätzlich erhöhen.
- Zero Trust Network Access (ZTNA) ist eine weitere Schlüsselkomponente, die in die SASE-Lösung eingebunden sein sollte. ZTNA fügt eine zusätzliche Sicherheitsebene hinzu, indem Benutzern der Zugriff auf Daten oder Anwendungen erst nach einer Authentifizierung gewährt wird und sie erst dann über eine verschlüsselte Verbindung zugreifen können, standortunabhängig.
- Ein Secure Web-Gateway (SWG) verhindert, dass nicht autorisierter Datenverkehr in das Unternehmensnetzwerk gelangt. Dies verhindert, dass böswillige Benutzer eindringen, und schützt vor Viren und Malware, die sich im Netzwerk verbreiten könnten.
- Extended Detection and Response (XDR) bietet eine Bedrohungserkennung, die über das bloße Warten auf Vorfälle hinausgeht. Ein XDR bietet eine 24/7-Bedrohungserkennung und -reaktion, so dass Probleme sofort behoben werden, sobald sie erkannt sind.
- Ein Cloud Access Security Broker (CASB), der Benutzern auf Basis ihrer Berechtigungen sicheren Zugriff auf Cloud-Dienste gewährt.

Ein SASE-Konzept, das mehrere Dienste in seiner Architektur kombiniert, indem es Benutzer, Standorte und Geräte miteinander verbindet, ermöglicht eine umfassende, ganzheitliche Cloud-basierte Sicherheitslösung. Im Gegensatz zu zentralisierten On-Premises-Lösungen kann diese alle Herausforderungen einer zunehmenden Remote- und Hybridarbeit annehmen und ein hohes Maß an Sicherheit gewährleisten.

DIE PUBLIC CLOUD SPIELT ALS ZENTRALER HUB EINE IMMER GRÖSSERE ROLLE. DER EINTRITTSPUNKT IN DIESE IT-ARCHITEKTUR WIRD DADURCH ZUM ENTSCHEIDENDEN ORT, UM AUFGABEN WIE VERFÜGBARKEIT UND SICHERHEIT DER KOMMUNIKATION ZU LEISTEN.

Stefan Schachinger,
Produktmanager Network Security,
Barrcuda Networks, www.barracuda.com

**Fazit**

SASE ist die Zukunft der Netzsicherheit und des Netzzugangs. Die Digitale Transformation, mobile Mitarbeiter, die Nutzung von Cloud-Services und neue Edge-Computing-Plattformen haben den Unternehmensbetrieb nachhaltig verändert. Unternehmen können nur dann wirklich erfolgreich sein, wenn jederzeit und überall auf Apps und Services zugegriffen werden kann. SASE bietet diese Netzwerk- und Sicherheitsfunktionen, die bei Bedarf jederzeit und weltweit Zugriff auf Daten und Workloads ermöglichen.

***Stefan Schachinger | www.barracuda.com***

# CLOUD SECURITY

## MEHR DIALOG, WENIGER TECHNIKFOKUS

Andreas Nolte,
Head of Cyber Security,
Arvato Systems,
www.arvato-systems.de

Cyber-Angriffe können schwere Folgen haben – bis hin zum kompletten Stillstand des Unternehmens. Zeit also, Cloud Security auf Entscheider-Ebene zu priorisieren. Denn woran Security-Initiativen häufig scheitern, ist der fehlende Dialog zwischen IT und Geschäftsführung.

Natürlich wissen IT-Abteilungen um die Gefahren und Chancen, wenn Daten und Systeme in der Cloud liegen. Aber warum sind Unternehmen auf dem Security-Auge blind? Es scheint, als würden IT und Management keinen Dialog führen. Während mancher CEO nicht weiß, wie wichtig Cloud Security für den Geschäftsbetrieb ist, gelingt es einigen IT-Experten nicht, die positiven Auswirkungen adäquater Schutzmaßnahmen auf das operative Business zu vermitteln. Im Zweifel steht die Produktion still – was Firmen hart trifft.

### Echter Dialog

Die Technologie sollte zunächst außen vor bleiben. Es geht darum, den Möglichkeiten der Cloud und der Komplexität von Cloud Security mit bewussten Entscheidungen zu begegnen. Wichtig ist, dass der Produktionsbezug im Zentrum steht. Ist etwa ein für den Geschäftsbetrieb relevanter Service in die Cloud zu migrieren, stellen sich Fragen wie: Soll das bisherige On-Premises-Konzept eins zu eins in der Cloud abgebildet sein – einschließlich Wartung und Updates? Oder wäre es nicht sinnvoller, das digitale Produkt als Software-as-a-Service bereitzustellen? Und wie gelingt es, die SaaS-Lösung wirkungsvoll abzusichern?

### Cloud Security ist ein strategisches Thema

Allesamt strategische Fragen. Darum ist Cloud Security in der Unternehmensstrategie nachhaltig zu verankern und erst im zweiten Schritt praktisch umzusetzen. Diese Herausforderung geht weit über die IT-Abteilung hinaus. Sie betrifft alle Fachbereiche.

***Andreas Nolte***

---

# PENETRATION TESTING MIT METASPLOIT

## PRAXISWISSEN FÜR MEHR IT-SICHERHEIT

Metasploit ist ein mächtiges Werkzeug, mit dem auch unerfahrene Administratoren gängige Angriffsmethoden verstehen und nachstellen können, um Sicherheitslücken im System aufzuspüren. Der Autor erläutert in diesem Buch gezielt alle Funktionen von Metasploit, die relevant für Verteidiger (sogenannte Blue Teams) sind, und zeigt, wie sie im Alltag der IT-Security wirkungsvoll eingesetzt werden können.

Als Grundlage erhalten Sie das Basiswissen zu Exploits und Penetration Testing und setzen eine Kali-Linux-Umgebung auf. Mit dem kostenlos verfügbaren Portscanner Nmap scannen Sie Systeme auf angreifbare Dienste ab. Schritt für Schritt lernen Sie die Durchführung eines typischen Hacks mit Metasploit kennen und erfahren, wie Sie mit einfachen Techniken in kürzester Zeit höchste Berechtigungsstufen in den Zielumgebungen erlangen.

Schließlich zeigt der Autor, wie Sie Metasploit von der Meldung einer Sicherheitsbedrohung über das Patchen bis hin zur Validierung in der Verteidigung von IT-Systemen und Netzwerken einsetzen. Dabei gibt er konkrete Tipps zur Erhöhung Ihres IT-Sicherheitslevels. Zusätzlich lernen Sie, Schwachstellen mit dem Schwachstellenscanner Nessus zu finden, auszuwerten und auszugeben.


**Penetration Testing mit Metasploit – Praxiswissen für mehr IT-Sicherheit; Sebastian Brabetz, mitp Verlags GmbH & Co. KG; 07-2022**

# PHISHING-RESISTENTE MFA

## AUF NUMMER SICHER IN STÜRMISCHEN ZEITEN

Einer aktuellen Umfrage des Digitalverbands Bitkom zufolge, sind gut zwei Drittel der deutschen Unternehmen angesichts der aktuellen Bedrohungslage alarmiert. Doch nur gut ein Drittel der Befragten hat seine IT-Schutzmaßnahmen kurzfristig hochgefahren. In den Fokus gerückt ist insbesondere die Bedeutung sicherer digitaler Identitäten. Der BSI betont einmal mehr, wie wichtig in diesem Kontext der Einsatz der Multi-Faktor-Authentifizierung (MFA) ist.

Laut dem Verizon Data Breach Report 2021 sind 89 Prozent der Datenschutzverletzungen bei Webanwendungen auf falsch verwaltete Anmeldeinformationen, einschließlich schwacher Passwörter, zurückzuführen. Die Verwendung einer phishing-resistenten MFA als Teil einer Zero-Trust-Architektur erschwert es Angreifern, über die Identität der Nutzer in die Systeme der Unternehmen einzudringen. Doch wie genau definiert sich eine phishing-resistente MFA?

Im Prinzip gelten zwei Authentifizierungstechnologien als phishing-resistent: die Personal Identity Verification (PIV)/ Smart Card und moderne FIDO WebAuthn. Im Gegensatz hierzu haben sich Ansätze wie SMS, mobile Push-Benachrichtigung und Einmal-Passwörter (OTP) in der Vergangenheit als anfällig für Phishing erwiesen. Wenn es sich also bei der verwendeten Authentifizierung nicht um PIV/ Smart Card oder FIDO/ WebAuthn handelt, dann ist sie nicht phishing-resistent. Ein Sicherheitsschlüssel wie der Yubikey 5er Series unterstützt beide Authentifizierungsstandards und ist darüber hinaus optional auch als FIPS oder CSPN-validierte Variante verfügbar – eine Anforderung in vielen Szenarien des öffentlichen Sektors und der Regierung sowie der Privatwirtschaft.

### Schutz vor Angriffen auf die Cybersicherheit

Im ersten Schritt empfiehlt es sich, ein internes Planungsteam zusammenzustellen und es mit einer umfassenden Prüfung zu beauftragen, im Rahmen derer der Zugang zu sensiblen Daten im Vordergrund steht. Des Weiteren wird eine vollständige Buchführung über Daten, Software und Kontrollen sowie über alle Auftragnehmer oder Dritte, die Zugang zum Netzwerk haben, benötigt. Sobald die priorisierten Systeme und Risiken identifiziert sind, sollten auch weitere Assets mit niedrigerer Priorität rasch angegangen werden. Denn meist werden letztere von den Angreifern ins Visier genommen, da deren Schutz in der Tat von vielen Unternehmen vernachlässigt wird.

Im nächsten Schritt ist es wichtig, einen nachhaltigen Sicherheitsplan zu erstellen, der schnelle Lösungen ausklammert. Eine moderne, phishing-resistente MFA kann in einigen Fällen rasch implementiert werden, in anderen steckt mehr Aufwand dahinter. Richten Unternehmen ihre Authentifizierungsstrategie an phishing-resistenten Standards wie PIV und FIDO aus, können sie das Thema IT-Sicherheit optimal angehen und entsprechende Maßnahmen schnell in die Wege leiten.

### IT-Sicherheit erfordert Überzeugungsarbeit

Die Realität ist jedoch, dass die Verbesserung der IT-Sicherheit nicht nur Ressourcen verschlingt, sondern auch die Zustimmung der Geschäftsleitung und die Genehmigung benötigter Mittel verlangt. Darüber hinaus sollten sich Unternehmen bewusst sein, dass es sich hierbei nicht um einen einmaligen Prozess handelt. Vielmehr sollte die Stärkung der Resilienz und damit der Schutz des Unternehmens als fester Bestandteil in die Budgetplanung einfließen. An dieser Stelle lohnt es sich, wichtige Führungskräfte, wie etwa den Chief Risk Officer, hinzuzuziehen, um der Geschäftsführung sowie den Mitarbeitern die Dringlichkeit des Schutzes vor Cyberangriffen zu vermitteln.

### Fazit

Unsichere und unvorhersehbare Zeiten wie diese erfordern es, die Angriffsfläche zu minimieren und die Cyberabwehr zu stärken. Richten Unternehmen ihre Strategie so aus, dass sie dem Schutz vor Cyberangriffen, einschließlich phishing-resistenter MFA, oberste Priorität einräumt, sind sie besser auf die aktuellen und zukünftigen Bedrohungen der Cybersicherheit vorbereitet.

***Alexander Koch | www.yubico.com***

yubico

# STIEFKIND IT-SECURITY

## WIE AUS SICHERHEITSLÜCKEN KEIN SCHEUNENTOR WIRD


Viele Unternehmen haben erheblichen Aufwand in ihre Digitalisierung gesteckt. Doch dann wurde ihr Netzwerk infiltriert und später ihre Services mit Ransomware angegriffen. So teuer wie an der IT-Sicherheit haben Unternehmen noch nie gespart.

Allzu oft wissen Unternehmen nicht einmal, dass sie angegriffen werden, da sie keine geeigneten Erkennungsmechanismen besitzen. Eine solche Sparsamkeit und Zurückhaltung in Sachen IT-Security wirkt angesichts der aktuellen Bedrohungslandschaft unangebracht. Häufig wird IT-Security eher als Hindernis empfunden, das der Effizienzsteigerung oder der Einführung neuer Technologien im Wege steht. Der Mangel an Skills, Ressourcen, Zeit und Investitionsbereitschaft ist ebenfalls ein Hemmschuh. Zudem wird IT-Sicherheit oft in Form von Einzellösungen gedacht, die spezielle Probleme beheben.

Ziel muss es sein, die Synergien zwischen den Security-Lösungen zu erkennen und zu heben. Bei echten Synergien addiert sich 1+1 eben nicht auf 2, sondern auf 3. Dazu müssen die Tools auf Framework-Prozesse gemappt werden, um alle Funktionen wie Identifikation, Schutz, Erkennung, Reaktion und Wiederherstellung abzudecken. Auch ist geeignetes Personal mit entsprechendem Know-how nötig, denn der beste Markengrill hilft nichts, wenn man ihn nicht fachgerecht bedienen kann.

IT-Security ist auch kein Projekt, das zu einem bestimmen Zeitpunkt abgeschlossen ist. Sie muss ständig weiterentwickelt und angepasst werden. Kein Wunder, dass durch die aktuellen Trends sogar viele CIOs und CISOs von der Komplexität der Aufgabe überfordert sind und einfach so weitermachen wie bisher.

### Effiziente Lösungen

Dabei ist es gar nicht so schwer, zum Beispiel Grundsteine für Zero Trust zu legen. Diese Security-Transformation basiert auf dem Grundsatz, keinem Gerät, Nutzer oder Dienst innerhalb oder außerhalb des eigenen Netzwerks zu vertrauen. Das erfordert ganzheitliche Maßnahmen zur Authentifizierung aller Anwender und Dienste sowie zur ständigen Überprüfung der Kommunikation.

Allerdings ist eine wichtige Voraussetzung, dass die Top-Management-Ebene Informationssicherheit in ihren Business-Modellen verankert und zusätzlich die Rolle eines CISO besetzt. Dies ermöglicht das strukturierte Management der Informationssicherheit, ohne Kompromisse für andere KPIs eingehen zu müssen. Eine wirtschaftliche Bewertung der Risiken fördert sogar die Investitionsbereitschaft für Security.

### Die wichtigsten Aufgaben des CISO sind:

- Etablierung eines Managementsystems zur Informationssicherheit (ISMS)
- Durchführung von Risikoassessments und Business-Impact-Analysen
- Aufbau und Betrieb einer Organisationseinheit zur Umsetzung der Sicherheitsziele
- Bewusstsein der Mitarbeitenden für Informationssicherheit durch Kampagnen schaffen
- Portfolio-Management der sicherheitsrelevanten Geschäftsprozesse
- Kontinuierliche Analyse und Optimierung der Informationssicherheit im Unternehmen
- Austausch zur Informationssicherheit und Cyber Security in Verbänden und Netzwerken

Diese Aufgaben gehen über die Verantwortung der IT-Abteilung hinaus. Zum Beispiel bietet Campana & Schott Hilfestellung für Zero Trust und ISMS, Informationssicherheit für Dokumente sowie der technischen Implementierung. Dabei kann eine ganzheitliche Strategie und Roadmap komplexe Herausforderungen in kleine Probleme teilen und schrittweise lösen.

Eine veränderte Sicherheitskultur muss mit entsprechendem Change Management begleitet werden. Der Partner kann Mitarbeitende des Kunden zu Security-Helfern ausbilden. Denn Know-how ist ein unverzichtbarer Baustein im Konzept der IT-Sicherheit. Dieses Potenzial muss gehoben werden. Dann öffnen sich die digitalen Tore auch nur noch für erwünschte Besucher.

***Manuel Maierhofer, Michael Matthies***

***www.campana-schott.com***

# DATEN EFFIZIENT NUTZEN

## GESCHÄFTSFORTFÜHRUNGSPLANUNG LEICHT GEMACHT

Die Erstellung einer Geschäftsfortführungsplanung (GFP) ist einer der relevantesten Schritte bei der Einführung eines Business Continuity Managements und stellt Organisationen jeder Größe vor enorme Herausforderungen. Wer vorhandene Datenbestände geschickt nutzt, kann sich die Arbeit leichter machen.

Im Vorfeld haben sich die Organisationen bereits mit der Identifikation der kritischen Geschäftsprozesse beschäftigt, Prozesslandkarten erstellt und die Abhängigkeit der Prozesse von bestimmten Anwendungen und IT-Systemen des Unternehmens dokumentiert. Auch zur Aufbauorganisation liegen in den meisten Fällen bereits detaillierte Informationen vor, zum Beispiel Verantwortlichkeiten, Kontakte und Alarmierungsketten. Wie lässt sich dieser Datenschatz für die Erstellung einer Geschäftsfortführungsplanung nutzen?

Ein Blick in einen fertigen GFP oder eine GFP-Vorlage des BSI-Standards zeigt, dass die oben beschriebenen Datengrundlagen weitgehend dem Inhaltsverzeichnis entsprechen. In dieser vorgegebenen Struktur müssen also „nur noch" die Kapitel mit weiteren Inhalten befüllt werden.

### GFP in einem Dokument

Zunächst erscheint es am einfachsten, den GFP direkt in der gewohnten Arbeitsumgebung einer Textverarbeitung zu erstellen. Dabei fällt allerdings schnell auf, dass die Unterkapitel sehr dynamisch sind. Jede kritische Ressource muss einzeln betrachtet werden und jede Änderung in den vorhergehenden Schritten erfordert eine Überarbeitung aller darauf basierenden Kapitelbestandteile. Es ist nur eine Frage der Zeit, bis die Bearbeiter den Überblick verlieren und die Pläne falsche und widersprüchliche Informationen enthalten.

### BCM-Tool verwenden

Softwaretools mit entsprechenden Datenverknüpfungen bieten hier einen klaren Vorteil: Einzelne Änderungen fließen allumfassend in den GFP ein. Ändert sich ein Ansprechpartner oder wird die Meldekette angepasst, lassen sich die Pläne automatisiert und konsistent aktualisieren.

Die Pflege von Texten für Strategien, Workarounds und Maßnahmen für die kritischen Ressourcen ist allerdings oft nicht so einfach wie in einem Textverarbeitungsprogramm.

### Alle Vorteile in einem System

Im Modul HiScout BCM fließen alle Schritte, die im Vorfeld der Geschäftsfortführungsplanung durchgeführt werden, automatisch in den jeweiligen GFP ein. Sobald sich die zentral bereitgestellten Daten ändern, werden diese automatisch nachgeladen. Eine Life-Vorschau zeigt jederzeit den aktuellen Bearbeitungsstand des GFP. Zur Erfassung der Strategien, Workarounds und Maßnahmen steht ein komfortables Fragebogentool zur Verfügung. Die verantwortlichen Fachkollegen können die benötigten Informationen wie in einem normalen Textdokument neu anlegen oder ändern und dabei auf Textbausteine zugreifen. Nach erfolgter Freigabe wird der GFP automatisch aktualisiert. So wird nichts vergessen und eine schnelle Bearbeitung durch die Fachbereiche ist gewährleistet.

### Fazit

Die Inhalte einer Geschäftsfortführungsplanung lassen sich großenteils direkt aus der vorausgehenden Analyse der geschäftskritischen Prozesse ableiten. Bei der Erstellung eines GFP mit dem Modul HiScout BCM können BCM-Verantwortliche die Vorteile einer dokumentbasierten und einer toolgestützten Bearbeitung in einem System nutzen.

***Steffen Voigt, www.hiscout.com***

## IMPRESSUM

***Geschäftsführer und Herausgeber:***
Ulrich Parthier (-14)

***Chefredaktion:***
Silvia Parthier (-26)

***Redaktion:***
Carina Mitzschke

***Redaktionsassistenz und Sonderdrucke:***
Eva Neff (-15)

***Autoren:***
Kornelius Brunner, Conor Coughlan, Andreas Fuchs, Jörg von der Heydt, Anton Kreuzer, Manuel Maierhofer, Michael Matthies, Carina Mitzschke, Andreas Nolte, Silvia Parthier, Ulrich Parthier, Stefan Schachinger, Linda Schmittner, Stephan Schweizer, Thorsten Urbanski, Steffen Voigt

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

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

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

***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. 30,
gültig ab 1. Oktober 2022.

***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,
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




# STATE-OF-THE-ART SECURITY

## MANAGED SERVICES FÜR DIE ERKENNUNG VON CYBERANGRIFFEN

Längst sind nicht mehr nur große Unternehmen von ausgeklügelten Cyberangriffen betroffen. Auch der Mittelstand verzeichnet immer mehr Vorfälle. Um geschäftsfähig zu bleiben und Schaden zu vermeiden, ist es entscheidend, Bedrohungen und Eindringlinge schnell zu erkennen und zu stoppen. Moderne Security-Tools wie Security Information and Event Management (SIEM) und Security Orchestration und Automation and Response (SOAR) ermöglichen dies. Die große Herausforderung besteht aber darin, im Security Operations Center (SOC) die generierten Sicherheitsdaten aller angebundenen Security-Lösungen, wie beispielsweise Firewalls, Endpoint Detection oder Cloud-Services, auf einer Meta-Ebene intelligent zusammenzuführen und zu bewerten. Das ist aufwändig, erfordert Expertenwissen und gleicht der Suche nach einer Nadel im Heuhaufen.

Mit indevis Managed Detection and Response profitieren Unternehmen von State-of-the-art Security-Lösungen, ohne diese selbst kaufen und betreiben zu müssen. Zudem erhalten sie eine persönliche sowie auf ihre individuellen Bedürfnisse angepasste Betreuung. Alle Ereignisse werden rund um die Uhr überwacht, um Anomalien und Angriffe zu erkennen. Ein SOC-Team wertet die gesammelten Daten kontinuierlich aus und bestimmt die Quelle, die Art und den Umfang der Bedrohung. Durch das Outsourcing erhöhen Unternehmen ihre IT-Sicherheit und lösen zwei drängende Probleme der unternehmensinternen IT-Abteilung: den Fachkräftemangel und die Ressourcenknappheit.

***www.indevis.de***

Eine Veranstaltung von itsecurity & it-daily.net
Das Online-Portal von itmanagement & itsecurity

**SAVE THE DATE**

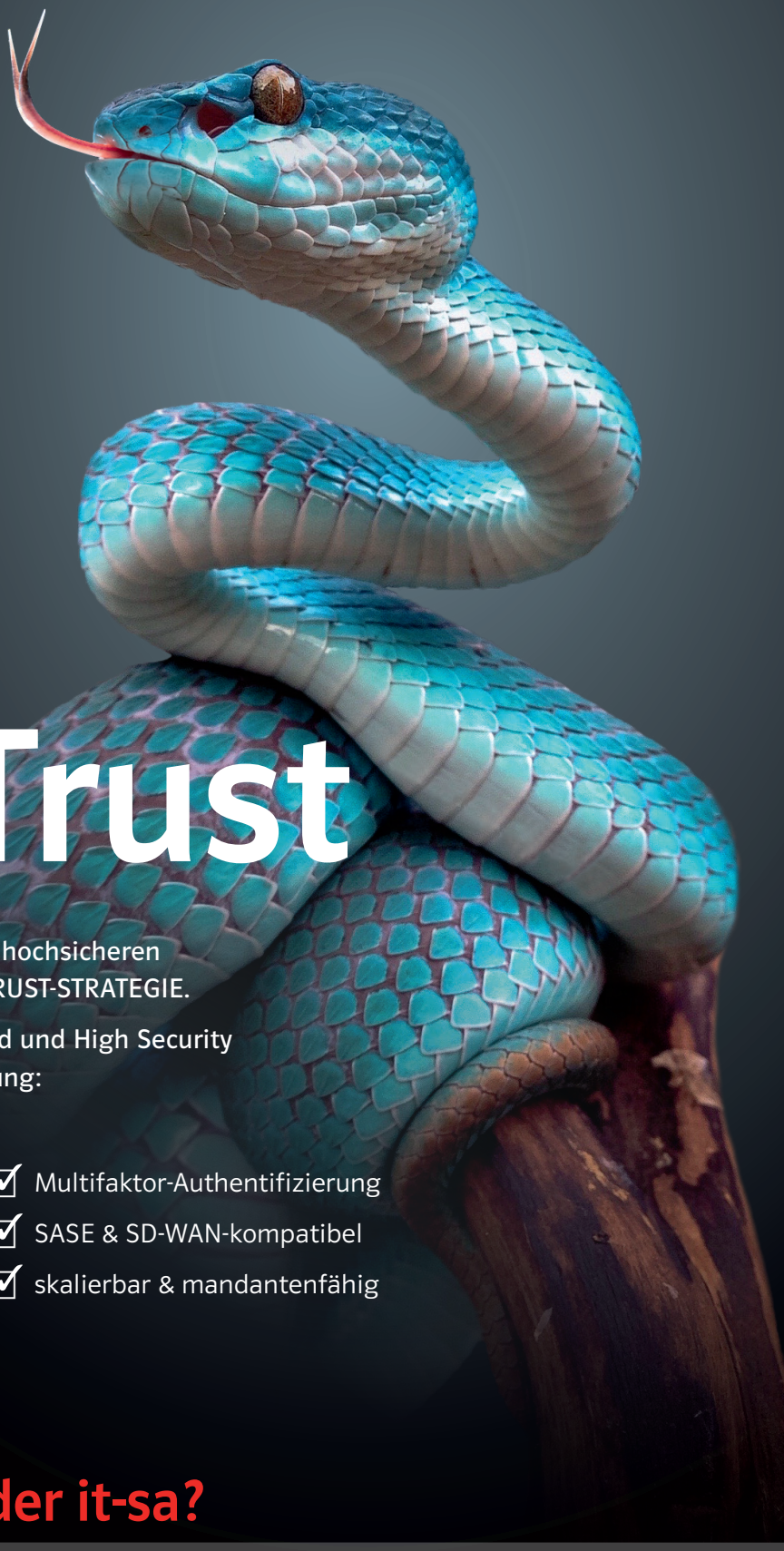
# IAM CONNECT 2022

## Dynamisches IAM

07.12.2022 | Digitalevent

#dynamicIAM
#IAMConnect2022

NCP
SECURE COMMUNICATIONS



# Zero Trust

Integrieren Sie die Technologie einer hochsicheren IPsec VPN-Verbindung in Ihre ZERO-TRUST-STRATEGIE.

Nutzen Sie die Vorteile von VPN, Cloud und High Security durch die NCP Secure Enterprise Lösung:

- ☑ SSO / SAML integriert
- ☑ ZTNA
- ☑ Endpoint Security
- ☑ Multifaktor-Authentifizierung
- ☑ SASE & SD-WAN-kompatibel
- ☑ skalierbar & mandantenfähig

## Sehen wir Sie auf der it-sa?

Kostenfreies Ticket sichern!

it sa

NCP SECURE COMMUNICATIONS my access

Secur|Ty made in Germany
Trust Seal www.teletrust.de/itsmig

www.ncp-e.com