itmanagement
MÄRZ 2022

INKLUSIVE 24 SEITEN
IT SECURITY

BÜRO, HYBRIDE FORMEN, HOMEOFFICE

BUSINESS-KOMMUNIKATION DER ZUKUNFT

Stephan Vanberg und Michael Steinberg, FP Digital Business Solutions GmbH

snom
25 Jahre IP-Telefonie
ab Seite 16

GREEN OFFICE
Wettbewerbsvorteil?

TWO SPEED IT
Hopp oder Top?

www.it-daily.net

SAVE THE DATE!

Storage im Fokus

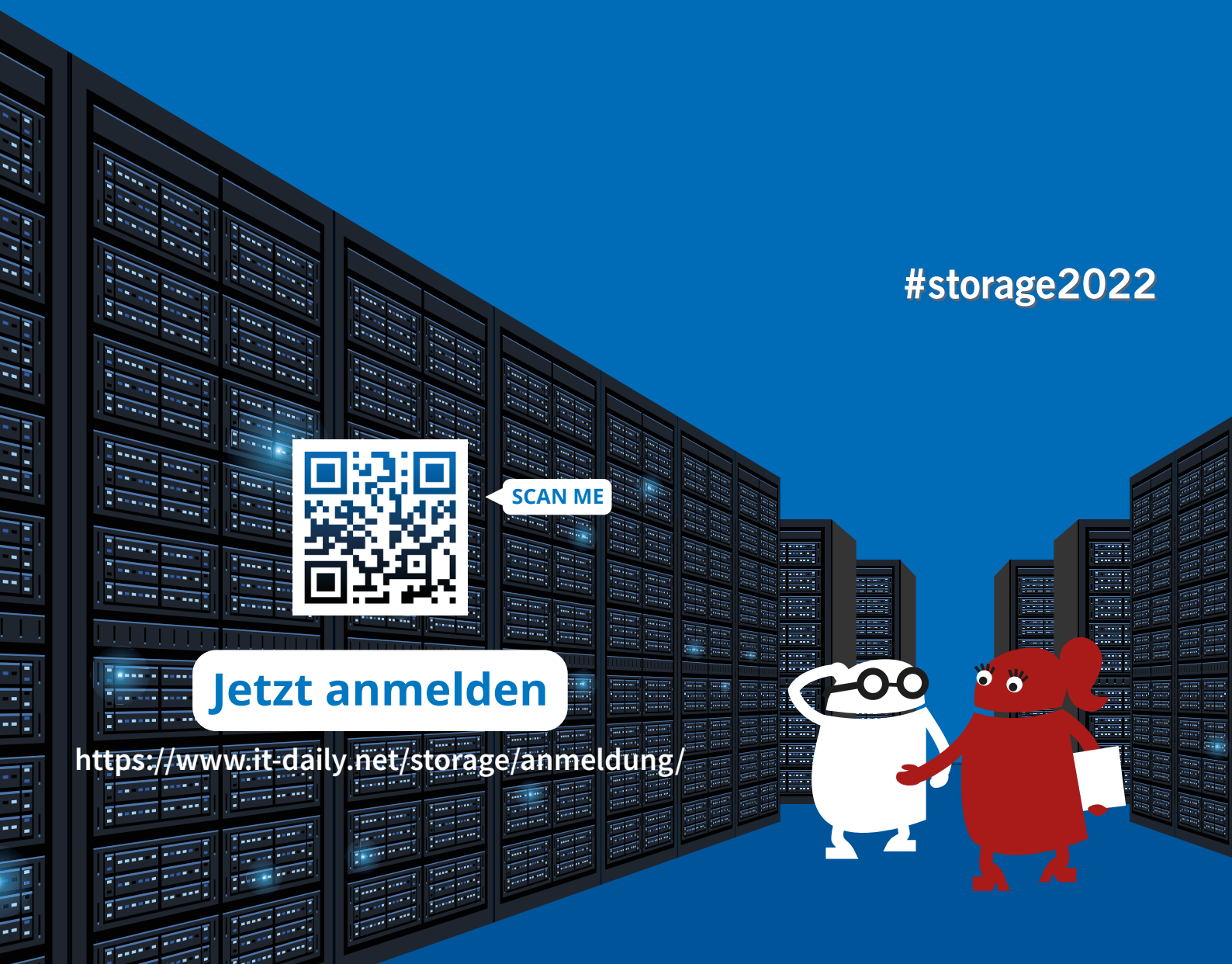
6. April 2022 | Digitalevent

#storage2022

SCAN ME

Jetzt anmelden

https://www.it-daily.net/storage/anmeldung/



EIN LEBEN NACH DEM HOMEOFFICE

Vor ein paar Jahren war das Thema Homeoffice noch eine verpönte und nicht unbedingt gern gesehene Beschäftigungsart. Mitarbeitern im Homeoffice wurde oft nachgesagt, nicht effizient zu sein und keine wirkliche Leistung zu erbringen.

Coronabedingt hat sich die Situation stark geändert. Um die Pandemiesituation zu entschärfen wurden Unternehmen verpflichtet Mitarbeiter, bei denen es möglich war, ins Homeoffice zu schicken. Nach anfänglichen Schwierigkeiten – fehlende Hard- und/oder Software, mangelnde Systemvoraussetzungen, unsichere Netzwerkzugänge, etc. – läuft das Thema Homeoffice jetzt mehr oder weniger rund. Sicherheitsinfrastrukturen wurden verbessert, Remotezugänge gesichert, Softwarelösungen wurden weiterentwickelt und das Arbeiten von zu Hause aus vereinfacht.

Und jetzt, wo wir uns alle irgendwie arrangiert haben, kommt die Rolle rückwärts: die Homeofficepflicht entfällt – demnächst. Da kommt schnell die Frage auf, wie das Arbeiten von morgen nun eigentlich aussehen soll?

Antworten darauf finden Sie in unserer aktuellen Coverstory – Büro, Homeoffice oder Hybrides Arbeiten? Offiziell ist alles möglich, wie die Realität aussehen wird, bleibt abzuwarten. Dennoch, die Entscheidungen werden jetzt gefällt und nicht erst in ein paar Jahren – für die Zukunft sollten wir uns aber merken, dass Flexibilität vielleicht die wichtigste Errungenschaft dieser Zeit sein wird.

In diesem Sinne, herzlichst

Carina Mitzschke | Redakteurin it management

22

INHALT

COVERSTORY

10 **Die Business-Kommunikation der Zukunft**
Büro, Homeoffice, hybride Formen – alles möglich

13 **Ganzheitlich, zukunftssicher, preiswert und schnell**
Business-Kommunikation sinnvoll digitalisieren

19

IT MANAGEMENT

16 **25 Jahre IP-Telefonie**
Aufbruch in eine neue Ära

19 **Mobile Arbeitsplätze**
Problem: Kritische Sicherheitsniveaus

22 **Ortsunabhängiges Arbeiten**
Es führt kein Weg mehr daran vorbei

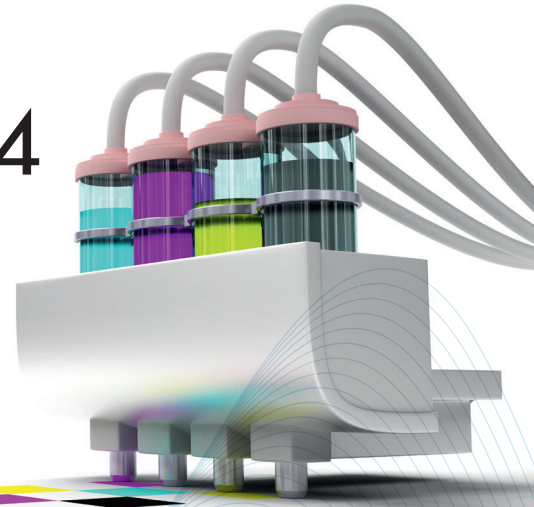
24 **Unverzichtbares Asset**
Das Green Office als Wettbewerbsvorteil

IT INFRASTRUKTUR

26 **Herausforderung Digitalisierung**
Mit No-Code trotz Fachkräftemangel Projekte umsetzen

30 **Kontroversthema: Two Speed IT**
Hopp oder Top? Was ist richtig, was falsch? (Teil 2 von 2)

10
COVERSTORY



24

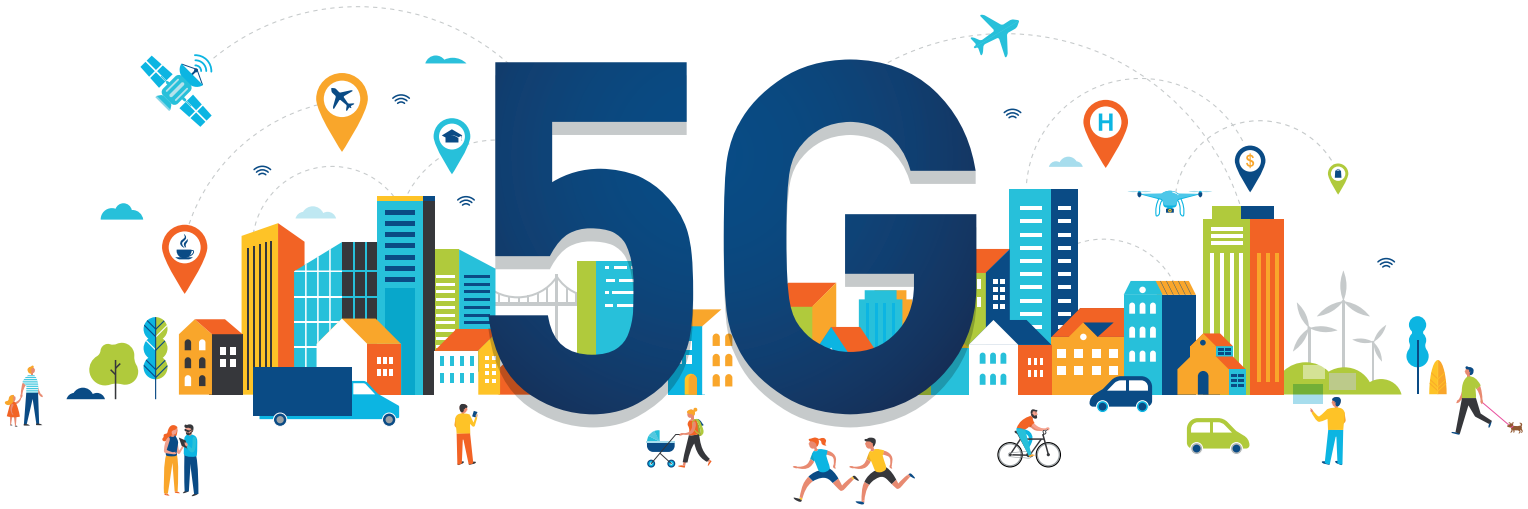
16

13

30

Inklusive
24 Seiten

IT SECURITY SPEZIAL



NEUES ZEITALTER?

5G FÜHRT UNTERNEHMEN IN DIE ZUKUNFT

Die Verbreitung des ultraschnellen Mobilfunkstandards und parallel dazu die Einführung von firmeneigenen 5G-Netzen, sogenannten Campus-Netzen, stehen noch ganz am Anfang. Nun mag 5G nicht für alle Wirtschaftszweige relevant sein – zahlreiche Branchen allerdings brauchen die Technologie, wenn sie weiterhin Wachstum generieren wollen.

Wenn Unternehmen Geschäftsmodelle oder Prozesse realisieren wollen, die bei niedriger Latenz hohe Datenmengen verarbeiten müssen, sind sie auf 5G angewiesen. Von Entwicklung bis Produktion, von Logistik bis Vertrieb – potenzielle Anwendungen gibt es fast überall. Gerade im industriellen Umfeld helfen Campus-Netze mit einem großen Ökosystem an Anbietern, bisherige technologische Hindernisse zu beseitigen.

Aus Sicht von NTT kann die 5G-Technologie Innovationen in folgenden Bereichen vorantreiben:

1. Smart City:
Intelligente Parksysteme, Real-Time-Diagnosen bei Stromausfällen oder eine optimierte Müllentsorgung – das sind nur einige Beispiele, die in einer vernetzten Stadt möglich sind. Basis dafür ist 5G, denn die Vernetzung einer ganzen Stadt erfordert das schnelle Versenden und Auswerten riesiger Datenmengen. Ein anderer Anwendungsbereich für 5G sind Smart Grids. Diese intelligent gesteuerten Stromnetze sorgen dafür, dass zu jeder Zeit die exakt benötigte Menge Strom erzeugt wird – im Idealfall bis auf das Watt genau.

2. Autonome Fahrzeuge:
Ebenfalls notwendig ist der 5G-Standard für zukünftige Mobilitätskonzepte wie dem autonomen Fahren. Nur wenn ein PKW kontinuierlich von außen mit Informationen versorgt wird, sind ein reibungsloser Transport und maximale Sicherheit für alle Verkehrsteilnehmer gewährleistet. 5G ermöglicht Echtzeit-Kommunikation mit anderen Fahrzeugen sowie mit der Infrastruktur wie Schildern und Ampeln.

3. Industrie 4.0:
Durch die Vernetzung der unterschiedlichsten Maschinen können Produktionsschritte besser aufeinander abgestimmt werden. Dies gilt sowohl firmenintern als auch zwischen verschiedenen, an der Produktion beteiligten Unternehmen. Das Ergebnis ist eine optimale Auslastung der Anlagen und eine schnellere Lieferung. Eine andere 5G-Option ist das Monitoring von kritischen Einrichtungen: Dazu gehören Sensoren für Temperatur, Feuchtigkeit, Druck, Spannung sowie für den Zustand von Reglern und Steuerventilen.

4. Telemedizin:
Im Gesundheitswesen kann mit 5G die Versorgung von chronisch Kranken deutlich verbessert werden, indem Patientendaten in Echtzeit mithilfe von mobilen Geräten zur Analyse übermittelt werden. Der Mediziner ist damit in der Lage, bei kritischen Werten rechtzeitig einzuschreiten. Gleichzeitig lassen sich Kosten sparen, da weniger Arztbesuche notwendig sind und Krankenhausbesuche verkürzt werden. Das Gleiche gilt für die Notfallversorgung.

5. Einzelhandel:
Ein digitaler Spiegel in Kombination mit einem 5G-Netz ermöglicht in Geschäften den Einsatz von Augmented-Reality- und Virtual-Reality-Lösungen. Kunden haben die Möglichkeit, das neue Outfit in Kombination mit verschiedenen Accessoires – ob Schuhe, Taschen oder Schmuck – zu visualisieren. Die 5G-Technologie ermöglicht darüber hinaus eine hochmoderne Bestandskartierung sowie ein abgestimmtes Flottenmanagement.

services.global.ntt

HYBRIDE ARBEITSMODELLE

FUTURE-FORUM-STUDIE

Hybrid Work ist zum weltweit vorherrschenden Arbeitsmodell geworden. Alleine in Deutschland sind 62 Prozent der Wissensarbeiter in hybriden Strukturen tätig. Dies zeigen die jüngsten Ergebnisse der globalen Pulse-Studie des Future Forum, ein von Slack und seinen Partnern ins Leben gerufener Think-Tank, der Unternehmen dabei unterstützt, die Arbeit in der digitalen Arbeitswelt neu zu gestalten.

Die Studie belegt, dass weltweit derzeit lediglich 30 Prozent aller Wissensarbeiter jeden Tag im Büro arbeiten. Dabei haben unterschiedliche Gruppen der Arbeitnehmenden abweichende Präferenzen für oder gegen Büropräsenz, was bei Führungskräften zu steigender Sorge angesichts eines „Proximity Bias" führt.

www.slack.com

41 %
der Führungskräfte geben als größte Sorge an, dass es zu Ungleichheiten zwischen den Mitarbeitern im Homeoffice und im Büro kommen könnte – das entspricht einem Anstieg von 33 % zum letzten Quartal

72 %
der Arbeitnehmer, die mit ihrer derzeitigen Flexibilität unzufrieden sind, können sich vorstellen den Job zu wechseln

58 %
der Wissensarbeiter arbeiten jetzt mit einer Hybrid-Lösung – das ist ein Anstieg von 46 % seit Mai 2021

96 %
der Mitarbeiter wünschen sich eine flexible Zeiteinteilung

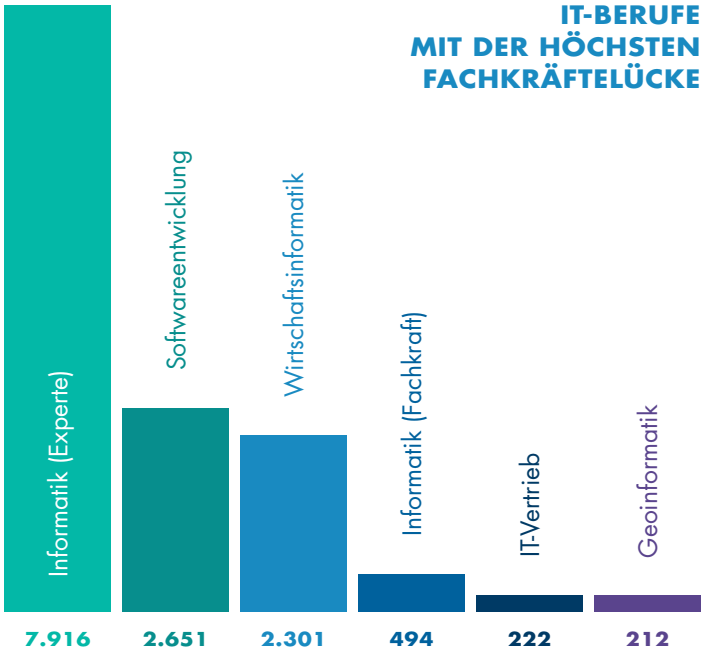
IT-BERUFE

FACHKRÄFTEMANGEL WEITER EIN PROBLEM

Die Beschäftigung in den IT-Berufen ist in den letzten Jahren stark gestiegen. Sie verzeichnet mit 41 Prozent das zweitstärkste Beschäftigungswachstum aller Berufshauptgruppen seit 2013. Im Jahresdurchschnitt 2020 arbeiteten damit circa 854.000 Beschäftigte in IT-Berufen. Im Zuge des digitalen Wandels und der verstärkten Nutzung von digitalen Formaten während der Corona-Pandemie ist zu erwarten, dass die Nachfrage nach IT-Kompetenzen in den Unternehmen eher noch zunehmen wird.

www.kofax.de

IT-BERUFE MIT DER HÖCHSTEN FACHKRÄFTELÜCKE



DIGITALISIERUNG

DAS BREMST UNTERNEHMEN

Unternehmen wollen digitaler werden, doch sehen sie sich auch mit vielfältigen Herausforderungen konfrontiert. Was bremst die digitale Transformation?

Als größte Herausforderungen sehen deutsche Firmen die hohen Anforderungen an den Datenschutz und die IT-Sicherheit. Darüber hinaus erachten vier von zehn Unternehmen langwierige Entscheidungsprozesse sowie fehlende Vorgaben aus der Geschäftsleitung als Bremsklötze ihres digitalen Wandels.

Fast ein Drittel der Unternehmen geben zudem an, dass ihnen schlichtweg die Digitalkompetenzen fehlen. Insbesondere im KI-Bereich mangelt es an entsprechenden Experten. Dabei hält jedes zweite Unternehmen den Einsatz von KI für den entscheidenden Faktor seiner zukünftigen Wettbewerbsfähigkeit.

Ein weiteres Problem: Immer mehr Unternehmen können sich keine Investitionen leisten. Tatsächlich berichtet jede achte Firma (12 %), aktuell kein Budget für die Digitalisierung zu haben. Das sind 5 Prozentpunkte mehr als im Jahr 2020. Ein kleiner Anteil der Firmen hat zwar ausreichend Geldmittel zur Verfügung, scheut jedoch das Risiko (7 %).

www.tcs.com/de

DIE GRÖSSTEN HERAUSFORDERUNGEN

62% Datenschutz

30% Fehlen von Digitalkompetenzen

40% langwierige Entscheidungsprozesse

56% IT-Sicherheit

30% fehlende Vorgaben aus der Geschäftsführung

Weitere Ergebnisse der Trendstudie von Bitkom Research und TCS finden Sie hier:

CYBER-SICHERHEIT

WARUM UNTERNEHMEN EINE PASSWORTRICHTLINIE BRAUCHEN

Passwörter sind zwar ein extrem wirksames Instrument, um Unternehmen vor Cyber-Angriffen zu schützen. Gleichzeitig sind kompromittierte Passwörter nach wie vor eine der Hauptursachen für Datendiebstahl. In 80 Prozent dieser Fälle werden die Kennwörter gehackt so der Data Breach Investigations Report 2020 von Verizon. Da Angestellte in der Regel eine Vielzahl an Passwörtern nutzen, ist die Angriffsfläche eines Unternehmens ziemlich groß. Außerdem zeigt die Studie „Psychologie der Passwörter", dass 65 Prozent der Nutzer für diverse Konten dasselbe oder ein ähnliches Passwort verwenden. Dadurch steigt das Risiko für einen Hackerangriff noch zusätzlich.

Abhilfe schafft einen effektive Passwortrichtlinie. Sie legt die Regeln fest, die Mitarbeiter bei der Erstellung, Verwendung, Speicherung und Freigabe von Kennwörtern beachten müssen.

EINE WIRKSAME PASSWORTRICHTLINIE ...

- ... ist klar und verständlich und vermeidet technischen und juristischen Fachjargon, damit alle Nutzer sie verstehen können
- ... ist im Mitarbeiterhandbuch oder Intranet des Unternehmens leicht zugänglich
- ... basiert auf bewährten Maßnahmen und erfordert keine häufig wechselnden Passwörter oder Sicherheitsfragen
- ... fördert mithilfe spezieller Technologie den richtigen Umgang mit Passwörtern
- ... bietet der IT-Abteilung eine zentrale Möglichkeit, die Passwortsicherheit im Unternehmen zu verwalten und zu überwachen
- ... wird von der IT-Abteilung aktualisiert, wenn sich die Bedrohungslage ändert
- ... wird den Mitarbeitern in regelmäßigen Schulungen nahegebracht

Die Passwortrichtlinie kann allerdings noch so gut formuliert sein – die eigentliche Herausforderung besteht in ihrer effektiven Umsetzung und Überwachung. Nur dann bietet sie einen wirksamen Schutz vor Cyber-Angriffen.

www.lastpass.com

UMGANG MIT PASSWÖRTERN IM UNTERNEHMEN

35%
der Arbeitgeber verpflichten die Mitarbeiter dazu, ihre Passwörter regelmäßig zu ändern

46%
der Mitarbeiter haben nicht von sich aus ihre Passwortsicherheit erhöht

47%
der Mitarbeiter haben ihr Sicherheitsverhalten nicht geändert, als sie ins Homeoffice wechselten

39%
der Unternehmen verpflichten ihre Mitarbeiter dazu, sich über sichere Netzwerke bei Unternehmens-Apps anzumelden

DIE BUSINESS-KOMMUNIKATION DER ZUKUNFT

BÜRO, HOMEOFFICE, HYBRIDE FORMEN – ALLES MÖGLICH

Wie wird unser Arbeiten morgen ausschauen? Viele Formen und viele Möglichkeiten ergeben sich. Ulrich Parthier, Herausgeber it management im Gespräch mit Stephan Vanberg und Michael Steinberg, die Geschäftsführer der FP DBS GmbH.

? **Ulrich Parthier:** *Die beiden Unternehmen FP Mentana-Claimsoft GmbH und FP IAB Communications GmbH haben sich Ende 2021 zusammengeschlossen zur FP DBS GmbH. Was waren die Gründe für diese Fusion?*

Stephan Vanberg: Bekanntermaßen gibt es einen stark steigenden Bedarf an digitalen Kommunikationslösungen, die komplexe Geschäftsprozesse abbilden, dabei auch das Homeoffice einbinden und gleichzeitig höchste Sicherheitsanforderungen erfüllen. Große Konzerne, mittelständische Unternehmen und Behörden stellen sich jetzt nach und nach dauerhaft um, denn eine Rückkehr in das alte Büroleben, wie wir es vor Corona kannten, wird es nicht mehr geben. Mit jeder neuen Corona-Welle steigt dieser Bedarf weiter an. Und um diese Aufgaben ganzheitlich zu erfüllen, bieten wir gemeinsam als „FP DBS GmbH" jetzt ein komplettes Bouquet an digitalen Business-Kommunikationslösungen an.

Michael Steinberg: Das Traditionsunternehmen FP ist unser Mutterkonzern und DBS steht für „Digital Business Solutions". Dazu gehört auch unser Schwesterunternehmen „FP Neo Monitor GmbH", die Digitalisierungslösungen gezielt für die Immobilienbranche anbietet. Wir arbeiteten als FP-Tochtergesellschaften schon lange zusammen und ergänzen uns optimal: Von der leicht zu bedienenden, rechtskonformen elektronischen Unterschrift „FP Sign", über Behördenpostfächer und „Transactmail" für kleine Briefmengen, bis hin zum komplexen In-und Outputmanagement mithilfe von KI und Robotic Automation für große Organisationen. „Backoffice-Automation" ist das Stichwort!

Stephan Vanberg: Eine wesentliche Erleichterung im Arbeitsalltag – gerade auch im Homeoffice - ist tatsächlich die Möglichkeit, Dokumente blitzschnell digital unterschreiben zu können, egal wo man gerade ist – und zwar rechtskonform. Mit unserem „FP Sign" signiert man einfach online digital ein PDF und versendet es verschlüsselt an die Empfänger. Dabei behält man immer die Kontrolle darüber, wer schon unterschrieben hat und wer noch nicht. Das geht mit verschiedenen Sicherheitsstufen: Von der fortgeschrittenen elektronischen Unterschrift für beispielsweise genehmigte Urlaubsanträge, bis hin zur qualifizierten elektronischen Signatur, die unter anderem für Geschäftsprozesse in der Zeitarbeitsbranche oder im Finanzsektor eingesetzt wird. Man muss also nichts mehr ausdrucken, händisch unterschreiben, in den Scanner legen und wieder hochladen, geschweige denn, zur Post bringen.

Michael Steinberg: Für Unternehmen und Behörden, die noch Briefe versenden oder empfangen, bieten wir Hybridlösungen: Wir scannen deren Papierpost und leiten sie digital intern weiter bis zur zuständigen Person – das sogenannte Inputmanagement – dabei kommen Machine Learning und Robotic Automation zum Einsatz. Und andersherum: wenn eine Organisation Papierpost versenden muss, bereiten wir deren Daten auf und drucken, kuvertieren und versenden sie vollautomatisch. Wir übernehmen also auch das sogenannte Outputmanagement. Das ist für sie sogar preisgünstiger, als wenn sie es selbst machen würden.

? **Ulrich Parthier:** *Schon vor der Pandemie war die Trennung von privater und geschäftlicher Kommunikation auf den verschiedensten Devices ein Problem. Wo sehen Sie Unterschiede, Hindernisse und welche Entwicklung prognostizieren Sie?*

Michael Steinberg: Das stimmt. Man sollte das unbedingt trennen, auch im Homeoffice. Hardwaretechnisch werden wir immer mobiler und es wird sicher auch in der Arbeitswelt bald fast alles über eine App mobil abgewickelt werden können. Doch für lange Texte und detaillierte Bilder wird man weiterhin große Bildschirme und ruhige Umgebungen brauchen. Wir bieten für jede Organisation maßgeschneiderte Software-Lösungen, die nicht nur anwender-

freundlich sind, sondern dabei eben auch alle gesetzlichen Anforderungen erfüllen.

Ulrich Parthier: *Besonderheiten gibt es wie so oft in der Öffentlichen Verwaltung (ÖV). So haben Behörden zum Beispiel besondere Sicherheitsanforderungen. Wie unterstützen Sie die ÖV im Bestreben effizienter, sicher und rechtskonform zu sein?*

Stephan Vanberg: Tatsächlich achten Behörden ganz besonders auf unsere Top-Sicherheitszertifikate. Wir liefern die Software zur Integration aller EGVP-, beBPo und De-Mail-Funktionalitäten, also für die ab 2022 verpflichtenden Behörden- beziehungsweise Bürgerpostfächer – nur wenige Anbieter können mit unseren Sicherheitsstandards mithalten. Und wir automatisieren die Korrespondenz ganzer Gemeindeverwaltungen, zum Beispiel in Hildesheim.

Ulrich Parthier: *Welche Anwendungsbeispiele können Sie zum Beispiel für die rechtskonforme elektronische Unterschrift nennen?*

Stephan Vanberg: Wir haben insbesondere bei Steuerberatungskanzleien einen durchschlagenden Erfolg mit „FP Sign“: inzwischen ist unsere Lösung auch im DATEV DMS integriert und Kanzleien nehmen das Angebot dankbar an. Dadurch wird nicht nur der Arbeitsalltag vieler Steuerberater sehr erleichtert, sondern auch der ihrer Mandanten.

Michael Steinberg: Oder in der Immobilienwirtschaft: Mietverträge, Wohnungsübergabeprotokolle oder Dienstleisterverträge können mit „FP Sign“ unterschrieben werden. Viele Abläufe in der Mieterkommunikation funktionieren schon per App, aber manches muss es eben doch noch per Brief mitgeteilt werden. Wir arbeiten seit Jahren mit der PROMOS consult Projektmanagement, Organisation und Service GmbH in Berlin zusammen, um mieterfreundliche Kommunikationslösungen anzubieten, die sich rechnen und gleichzeitig alle gesetzlichen Erfordernisse einhalten. Auch zu erwähnen ist die bereits benannte „NeoMonitor“ - hier wird die Technische Gebäudeausstattung (TGA) ganzer Immobilienportfolios digitalisiert und deren Effizienz zentral dem Immobilienverwalter am Schreibtisch per Software aufgezeigt.

WIR BIETEN KOMMUNIKATIONSTECHNOLOGIEN FÜR ORGANISATIONEN JEDER GRÖSSE UND JEDER BRANCHE, UM DEREN SCHRIFTLICHE BUSINESS-KOMMUNIKATIONS-PROZESSE GESETZESKONFORM DIGITAL ZU VEREINFACHEN.

Stephan Vanberg, Geschäftsführer, FP Digital Business Solutions GmbH

Ulrich Parthier: *Eingangs sprachen Sie die Transactmail, kurz TAM, an. Was genau kann sie leisten und wo kommt sie zum Einsatz?*

Michael Steinberg: Das ist unser Online-Self-Service für kleinere Bedarfe. Viele Freelancer, Selbständige oder Einzelunternehmer haben nicht einmal mehr einen Drucker, geschweige denn Briefmarken zur Hand, wenn sie plötzlich doch einmal einen Papierbrief versenden müssen. Mit dieser SaaS-Lösung wird deren digitaler Briefentwurf ausgedruckt, kuvertiert, frankiert und für weniger Gebühren versendet, als wenn sie selbst Briefpapier und Briefmarken kaufen würden - und das alles natürlich wesentlich schneller, als wenn man selbst zum Briefkasten laufen müsste. Das rechnet sich schon ab dem ersten Brief.

Ulrich Parthier: *Wie ordnen Sie ihr Produktportfolio im Zusammenhang mit der Digitalen Transformation und New Work ein?*

Stephan Vanberg: Wir bieten Kommunikationstechnologien für Organisationen jeder Größe und jeder Branche, um deren schriftliche Businesskommunikations-Prozesse gesetzeskonform digital zu vereinfachen. Unsere Angebote können über ein Portal als SaaS-Lösung genutzt oder tief integriert werden in Fachsoftware, DMS-, ERP- oder CRM-Systeme.

Video und Telefonie überlassen wir anderen, beziehungsweise binden wir auch solche Lösungen mit in unsere Prozessautomatisierungen ein, wenn sie zu den Bedürfnissen unserer Kunden und wiederum deren Kunden passen - und sie die jeweiligen gesetzlichen Anforderungen erfüllen können. Dabei begleiten wir unsere Kunden auf dem Wege der Digitalen Transformation und oft sind unsere Ansprechpartner sehr überrascht, wie schnell und einfach wesentliche Schritte hier umgesetzt werden können.

Michael Steinberg: New Work bedeutet auf dem Weg durch die Digitale Transformation gerade im Homeoffice, dass man auch darauf achten muss, dass Mitarbeitende nach Dienstschluss ihre Freizeit genießen können. Das gehört zum Arbeitsschutz und zu einer gesunden Firmenkultur dazu. Es ist im Interesse der Arbeitgeber, wenn die eingesetzten neuen Technologien nicht nur schnelleres Arbeiten rund um die Uhr ermöglichen, sondern sinnvolle Arbeitserleichterungen sind und auch zur Gesunderhaltung beitragen.

Ulrich Parthier: Herr Vanberg, Herr Steinberg, wir danken für das Gespräch!

THANK YOU

WIR BIETEN FÜR JEDE ORGANISATION MASSGESCHNEIDERTE SOFTWARE-LÖSUNGEN, DIE NICHT NUR ANWENDERFREUNDLICH SIND, SONDERN DABEI EBEN AUCH ALLE GESETZLICHEN ANFORDERUNGEN ERFÜLLEN.

Michael Steinberg, Geschäftsführer,
FP Digital Business Solutions GmbH

BUSINESS-KOMMUNIKATION SINNVOLL DIGITALISIEREN

GANZHEITLICH, ZUKUNFTSSICHER,PREISWERT UND SCHNELL

Entscheider:innen in Firmen und Behörden stehen vor der Herausforderung, wie sie vorhandene Kommunikationslösungen, die über Jahre quasi organisch gewachsen sind, zukunftssicher und rechtskonform in neue tragfähige, digitale Strukturen überführen sollen - ohne, dass es ewig dauert oder ein Vermögen kostet. Für diese Aufgabe sucht man sich am besten Partner, die bereits Erfahrungen auf dem Gebiet der Business-Kommunikation haben, ganzheitlich denken und den Markt sowie die tatsächlichen Bedürfnisse der Anwender kennen.

Die Corona-Pandemie war und ist ein „Technologieakzeptanztreiber". Inzwischen ist die Arbeitswelt ohne Videokonferenzen nicht mehr vorstellbar und mit dem Homeoffice haben sich die meisten Arbeitgeber und Arbeitnehmer mental und technisch inzwischen arrangiert, sodass auch Konzerne dies jetzt als Dauerlösung etablieren.

Kulturwandel in der Arbeitswelt – der Mix macht's

Sämtliche Arbeitsmittel, die in den privaten Räumen der Mitarbeitenden benutzt werden, müssen dauerhaft zuverlässig Datenschutz- und Datensicherheitsvorschriften erfüllen und gleichzeitig sollen sie benutzerfreundlich, bezahlbar und stabil sein.

Im Privatleben sind zeitversetzte Sprachnachrichten und Kurztexte beliebt, doch im Businesskontext gilt die Schriftform als ideales Kommunikationsformat – Texte kann man diskret (ohne dass die Verwandtschaft im Nebenzimmer mithört) und revisionssicher bearbeiten. Die Business- und Behördenkommunikation wird sich also weiter verstärkt auf Mails und Dokumente - und damit auf Document Management Systeme (DMS) - stützen, trotzdem behalten viele andere Kommunikationsformen weiterhin ihre Existenzberechtigung und neue kommen hinzu.

Die gesamte Business-, beziehungsweise Verwaltungskommunikations-Infrastruktur muss flexibel bleiben, um mit den sich ständig verändernden Arbeitswelten mitzuhalten. Backoffice-Automation-Lösungen dürfen also niemals starr sein.

Professionelle Businesskommunikation vereinfacht Abläufe

Viele Gesetze und Richtlinien regeln die geschäftliche und behördliche Kommunikation, allen voran die DSGVO zum Schutz personenbezogener Daten. Manche empfinden das als Regulierungswahn, aber man darf nicht vergessen, dass dieser Regelkomplex dazu gedacht ist, um Verbraucher, Bürger, Arbeitnehmer - und auch Arbeitgeber - vor Schaden zu bewahren. Das Gesetz gegen den Unlauteren Wettbewerb beispielweise dämmt Spam ein. Ein Segen. Das Onlinezugangsgesetz soll die Interaktion zwischen Bürgerinnen, Bürgern und Unternehmen mit der Verwaltung endlich schneller und nutzerfreundlicher machen, genau wie das EGVP, also das elektronische Gerichts- und Verwaltungspostfach für die verschlüsselte Übertragung von Dokumenten und Akten zwischen authentifizierten Teilnehmern. Diese Gesetze und Regelungen bieten die Chance für sinnvolle, unkomplizierte Workflows, die das Leben leichter machen - wenn man sie richtig aufsetzt.

Schlank, elegant und leicht: Cloudlösungen

Cloud-, Portal- und SaaS-Lösungen verbrauchen keinen Platz und sind stets auf dem neuesten Stand. Ein Paradebeispiel dafür ist die „Elektronische Signatur". Sie boomt. Verträge, Anträge, Testate, Steuererklärungen oder Zeugnisse werden nicht mehr ausgedruckt, mit Füllhalter unterschrieben und per Post hin- und hergeschickt – den Aufwand kann man sich sparen. Ein Dokument wird nun innerhalb von Minuten digital unterschieben. Anschließend ist es möglich, es innerhalb eines DMS-, ERP- oder CRM-Systems den entsprechenden Vorgängen zuzuordnen und in einem Archiv jahrzehntelang aufzubewahren.

Grundlage ist die eIDAS-Verordnung der Europäischen Union, die elektronische Zertifizierungen und Vertrauensdienste für elektronische Transaktionen regelt.

Vertrauen, Kontrolle und reibungsloses Zusammenspiel

Das Vertrauen in funktionierende elektronische Transaktionen ist dort am schwersten zu erlangen, wo analoge Prozesse jahrzehntelang hervorragend funktioniert haben. War die Idee vom „papierlosen Büro" bis in die 2010er Jahre meistens nur Gerede, setzten sich jedoch in den letzten Jahren dann endlich flächendeckend Dokumenten Management Systeme (DMS), Customer Relationship Management Systeme (CRM), Content Management Systeme (CMS) und digitale Archive durch, weil sie nun soweit sind, dass sie die Arbeit vereinfachen, anstatt sie zu verkomplizieren.

Zusätzlich ermöglicht eine zunehmende Vernetzung von Objekten über das Internet der Dinge (IoT) die durchgängige Digitalisierung von Arbeitsprozessen wie etwa in der Immobilienbranche die Erfassung und Abrechnung von Energieverbrauchswerten von Gebäuden.

Im Grunde ist bei vielen Organisationen die Digitale Transformation längst vollzogen, jetzt müssen sie noch dafür sorgen, dass alle Systeme sinnvoll ineinandergreifen, um wirkliche Arbeitserleichterung zu bieten - und offen für Neues bleiben.

Ganz ohne Papier geht es (noch) nicht

In vielen Branchen und Behörden geht es noch nicht vollständig ohne Papierbriefe und auch im Homeoffice muss man ja irgendwie seine physische Geschäftspost erhalten. Solche Aufgaben lösen Dienstleister, die entweder Briefe tagesaktuell vom Büro zu den Arbeitnehmern ins Homeoffice bringen oder hybride Dienste, die physische Dokumente zentral sammeln, scannen und an die Adressaten digital weiterleiten. Auch andersherum: Digitale Korrespondenz wird preiswert entweder in der Firma oder an einer zentralen Sammelstelle ausgedruckt, kuvertiert, frankiert und dann zugestellt. Durch Mengenrabatte bei der Deutschen Post AG können diese Dienstleister ihren Service günstiger anbieten, als wenn man Briefpapier, Umschläge und Briefmarken selbst kaufen würde. Das In- und Output-Management kann passgenau auf jedes Unternehmen zugeschnitten werden.

Kleine Firmen und Freelancer brauchen bald keinen Drucker mehr: Wenn sie gelegentlich doch einmal einen Brief zu versenden haben, können auch sie solche Hybriddienste preiswert nutzen, um ihren digitalen Entwurf drucken, kuvertieren, frankieren und versenden zu lassen. Dieser Service ist schon für 80 Cent pro Brief zu haben (Stand März 2022).

Die Kunst, gute Partner zu finden

Entscheider und IT-ler sollten sich auf eine ganzheitliche Betrachtungsweise einlassen, bei der die Bedürfnisse aller Stakeholder berücksichtigt und die entsprechenden Lösungen sinnvoll aufeinander abgestimmt miteinander verwoben werden.

Gute Dienstleister bieten Beratungspakete an und analysieren zunächst die bisherigen Abläufe und Strukturen. Danach geben sie Empfehlungen, wie man mit welchen Mitteln schrittweise auf sinnvolle neue Systeme umsteigt, ohne den laufenden Betrieb zu stören. Die neuen Lösungen sollen nicht nur Zeit und Geld sparen, sondern auch einfach in die bisherige Software-Architektur integriert werden oder Schnittstellen nutzen - und gleichzeitig sicher sein. Zertifikate bieten hier Orientierung: Hält ein Dienstleister beispielsweise das ISO 270001 vor, weiß man, dass man es mit echten Sicherheitsexperten zu tun hat.

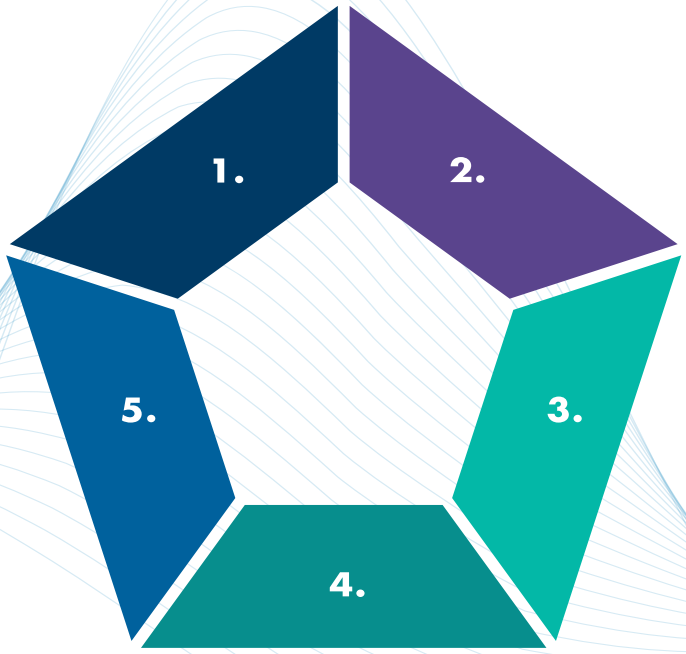
Magisches Fünfeck

Fünf Kriterien muss ein Kommunikationssystem gewährleisten: 1. Sicherheit, 2. Anwendungsfreundlichkeit, 3. Bezahlbarkeit, 4. Flexibilität und 5. Antizipation künftiger Entwicklungen, denn was nützt es, wenn das neue System nicht den technologischen Weiterentwicklungen der kommenden Jahre mithalten kann?

FP Digital Business Solutions GmbH

MAGISCHES FÜNFECK

Fünf Kriterien muss ein Kommunikationssystem gewährleisten:



1. **Sicherheit,**
2. **Anwendungsfreundlichkeit**
3. **Bezahlbarkeit**
4. **Flexibilität**
5. **Antizipation künftiger Entwicklungen**

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

IP-TELEFONIE

AUFBRUCH IN EINE NEUE ÄRA

UNSER BESTREBEN LAG DARIN, NICHT IRGENDEIN UPGRADE ZU ENTWICKELN. NACH ÜBER 20 JAHREN WURDE ES VIELMEHR ZEIT, DAS TISCHTELEFON UND SEINE FUNKTIONALITÄT VÖLLIG NEU ZU DENKEN.

Gernot Sagl, CEO,
Snom Technology GmbH,
www.snom.com

Snom war einer der Pioniere im Bereich Voice over IP. 25 Jahre sind seit der Gründung des Unternehmens vergangen. Zeit, um über die Entwicklung und Zukunft mit Gernot Sagl, CEO bei der Snom Technology GmbH, zu sprechen.

Ulrich Parthier: *Herr Sagl, ein Vierteljahrhundert ist seit der Start-up Zeit vergangen. Was hat sich technologisch gesehen am meisten verändert und wie hat sich das Unternehmen weiterentwickelt? Stichwort Produktportfolio.*

Gernot Sagl: Zwischenzeitlich machten Audio-Codecs enorme Qualitätssprünge, und die anfänglich benötigte Kompatibilität zum Signalisierungsprotokoll H.323 ist tatsächlich Schnee von gestern. Doch abgesehen von Bits & Bytes hat sich in den letzten 25 Jahren ganz sicher die Art zu arbeiten weiterentwickelt! Hätte sich irgendwer zur damaligen Zeit vorstellen können, nicht vom gemeinsamen Firmenbüro aus zu arbeiten? Natürlich wirkte die Gesundheitskrise durch die diversen Lockdowns als Katalysator. Allerdings waren Flexibilität und das Prinzip der ortsunabhängigen Erreichbarkeit schon länger ein Thema, besonders für die Telekommunikation. Bei Snom lief die Entwicklung folgerichtig vom Bürotischtelefon, das quasi ein reines Kommunikationsgerät basierend auf IP war, hin zu immer autarkeren Endgeräten. Ob DECT over IP oder mobile Konferenzlösungen bis hin zu Tracking-Systemen wie unsere Beacon-Lösungen: Gefragt ist mittlerweile ein möglichst flexibles und breites Spektrum an Produkten und dahin geht ganz klar auch die Entwicklung bei Snom.

Ulrich Parthier: *Ende 2016 war ein einschneidendes Datum, das mittelständische Unternehmen Snom wurde vom VTech-Konzern mit Sitz in Hongkong übernommen, einem Unternehmen mit damals immerhin 37.000 Mitarbeitern. Welche Effekte haben Sie sich erwartet und sind sie eingetroffen?*

Gernot Sagl: Meine Erwartungen in Bezug auf die Übernahme waren immer positiv. Die Mitarbeiter hatten anfänglich verständlicherweise Sorgen. Aber VTech setzte konkret die Intention um, in den Erfolg von Snom Technology als eigenständige Gesellschaft zu investieren: Durch die Unterstützung des Konzerns konnten wir uns am Markt ganz neu positionieren. Die Synergieeffekte eröffneten Einsparpotenziale in der Produktion, sodass Snom seine Preise senken konnte – beziehungsweise in heutigen Zeiten der extremen Frachtkosten die Preise halten kann. Auch konnte VTech uns schnell davon überzeugen, dass sie uns wirklich als die Experten im Bereich IP an Bord geholt hatten. So findet zwar die zentrale Forschung und Entwicklung in Eigenregie weiter in Berlin statt, doch das Team umfasst mittlerweile auch bedeutende Engineering-Ressourcen an diversen Standorten beim Mutterkonzern, die ausschließlich für Snom tätig sind.

Ulrich Parthier: *Wie sieht die aktuelle Marktsituation für Snom aus. Wie viele Kunden und Partner zählen sie und in wie vielen Ländern sind sie aktiv?*

Gernot Sagl: Als Snom Berlin erstreckt sich unser Kernmarkt auf ganz EMEA. In unseren Fokusländern betreiben wir eigene Niederlassungen. Wir zählen aktuell weit über 10.000 aktive Fachhändler, haben viele namhaften Carrier im Boot und verfügen über ein wirklich gutes Netz an Distributoren. Asien überlassen wir naturgemäß unserem Mutterkonzern. Den amerikanischen Kontinent betreut Snom Americas. Einmal alle 25 Jahre darf man auch eine Bilanz über Verkaufsvolumina ziehen: Es wurden bislang über zehn Millionen Geräte verkauft, der Großteil davon in den letzten zehn Jahren.

Ulrich Parthier: *Stichwort time-to-market. Wo findet die Entwicklung statt und wie gewährleisten sie die Umsetzung bei so vielen verschiedenen Standards in den zahlreichen Ländern, in denen sie vertreten sind?*

Gernot Sagl: Glücklicherweise arbeiten wir auch im Sinne eines produktiven Ideenaustausches sehr gut mit dem Mutterkonzern zusammen. Doch Snoms-Produkte müssen schon unseren Standards bezüglich Qualität, Stabilität, Robustheit der Materialien und gebotener Sicherheit entsprechen. Die Anforderungen in diesen Bereichen sind in EMEA gleich hoch, weshalb unsere Produkte einen international hervorragenden Ruf genießen. Bei Sonderfällen setzen wir auf unsere lokalen Ansprechpartner im Vertrieb, aber auch im Support, und stehen gern für Personalisierungen zur Verfügung.

Ulrich Parthier: *In der ganzen IT-Industrie sind Themen wie Green IT und Nachhaltigkeit zu einem wichtigen Argument geworden. Wie sehen Sie diesen Aspekt?*

Gernot Sagl: Das Thema liegt uns ebenfalls sehr am Herzen. Bereits vor Jahren haben wir die Lieferung von Netzteilen zu allen Telefonen abgesetzt. Damals hatte sich Power over Ethernet als Stromzufuhr bereits durchgesetzt. Eine Partnerumfrage ergab, dass Netzteile nur bei 3 Prozent der Nutzer nötig waren. Die überflüssigen Plastikanteile unserer Verpackungen haben wir vor Kurzem durch Kunststofffreies ersetzt und bereits über 10 Tonnen Plastik gespart. Der nächste Schritt könnte der Einsatz von recycelten Materialien zur Erstellung geeigneter Komponenten unserer Endgeräte sein.

Ulrich Parthier: *Recycelte Materialien, gibt es da immer noch Vorbehalte auf Anwenderseite?*

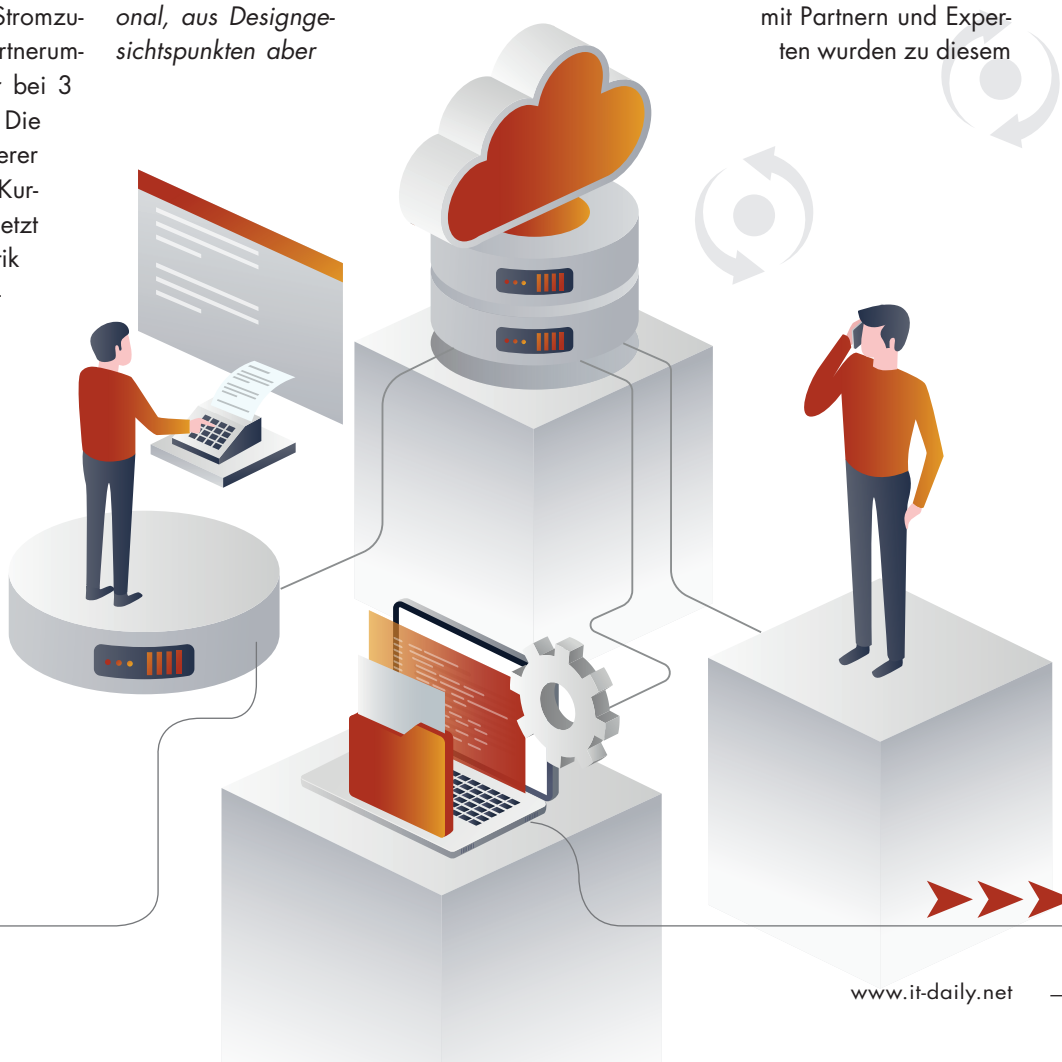
Gernot Sagl: Wir haben dazu im November das unabhängige Meinungsforschungsinstitut Norstat mit der Durchführung einer europaweiten Umfrage beauftragt. Die Ergebnisse sind verblüffend! 75 Prozent der Befragten würden gern nachhaltigere IP-Telefone nutzen. 66 Prozent davon wären sogar bereit, für die erhöhte Umweltfreundlichkeit einen Aufpreis zu zahlen. Die Teilnehmer aus fünf Ländern maßen zu erstaunlichen 83 Prozent dem Einsatz von Komponenten aus recycelten Materialien Bedeutung bei und erklärten, alle Zusatzkomponenten (etwa Standfuß, Hörer oder Kabel) sollten nur daraus bestehen. Dieser Wert schwankte allerdings in den einzelnen Regionen. Während sich in Deutschland „nur" 75 Prozent der Nutzer für mehr Nachhaltigkeit auch bei der Büro-Hardware aussprachen, waren es in Spanien 88 Prozent.

Ulrich Parthier: *Kommen wir zur Zukunft. IP-Telefone sind bisher eher funktional, aus Designgesichtspunkten aber eher nicht die Hingucker. Da sehen wir noch erheblichen Verbesserungsbedarf. Ist hier Land in Sicht?*

Gernot Sagl: Tatsächlich scheiden sich beim Design die Geister: Stylisches ist häufig nicht funktional genug – oder umgekehrt. Uns kann man womöglich vorwerfen, der Funktionalität Priorität über das Design gewährt zu haben! Aber das hat sich ebenfalls geändert: Im September kündigten wir eine komplett neue Linie von IP-Geschäftstelefonen an: die D8xx-Serie. Hier wurde alles neu gedacht – und das Ergebnis kann sich, meiner Meinung nach, auch in puncto Design wirklich sehen lassen!

Ulrich Parthier: *Inwiefern?*

Gernot Sagl: Unser Bestreben lag darin, nicht irgendein Upgrade zu entwickeln. Nach über 20 Jahren wurde es vielmehr Zeit, das Tischtelefon und seine Funktionalität völlig neu zu denken. Gemeinsam mit Partnern und Experten wurden zu diesem



Zweck in Design-Thinking-Workshops die unterschiedlichsten Ansprüche in den entsprechenden Szenarien erörtert. Daraus wurde eine Modellreihe entwickelt, in der alles kann, aber nichts muss – außer unserem hohen Qualitätsanspruch gerecht zu werden.

Allein die Anpassung der Audioqualität an unsere Ansprüche wurde etwas Besonderes: Alle Geräte verfügen über mindestens HD-Audioqualität, manche sogar über Super-Wideband-Audio – etwas, was sonst nur in Tonstudios eingesetzt wird. So ging es bei Funktionalität und Design weiter – die D8xx sind sicher in jeder Hinsicht ein Hingucker!

Ulrich Parthier: *Hat Corona bei Ihnen als Innovations-Booster gewirkt?*

Gernot Sagl: Das mag so wirken, aber jeder ahnt, dass eine solche Entwicklung Zeit braucht – und zwar mehr als in der zum Teil lähmenden Pandemie-Phase. In der Tat hat die Nachfrage allerdings auch hier die Entwicklung beflügelt – da dürfen Sie also auf weitere Neuigkeiten gespannt sein, die für den Einsatzbereich „work from home" oder sogar „work from anywhere" entwickelt werden. Zu diesem Schritt wurden wir nicht durch die Pandemie veranlasst, allerdings hat sie den Fokus darauf verstärkt.

Ulrich Parthier: *Wo werden hier die Schwerpunkte liegen?*

Gernot Sagl: Der maßgebliche Fokus wird auf der Flexibilität liegen. Wir begegnen einer Trendwende in der Kommunikation und möchten ihr vorgreifen: Unsere IP-Endgeräte und Lösungen sollen sich in Zukunft immer nahtloser in die Arbeitsumgebung integrieren, sowohl im Sinne der Büroautomation als auch der Anwendungen. Kurzgefasst: Unser Bestreben gilt nach wir vor der maximalen Abdeckung eines gesamten Portfolios an Anforderungen – von der klassischen Bürokommunikation bis hin zu smarten Lösungen.

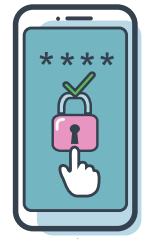
Ulrich Parthier: *In der Pandemie hat das New Work, auch Homeoffice genannt, einen unerwarteten Push bekommen. Unmittelbar damit verbunden ist das Thema der Videokonferenzen und Unified Communication. Sind hier konkrete Ankündigungen von Snom zu erwarten und wie lässt sich das Thema in der IP-Welt bei Telefonen abbilden?*

Gernot Sagl: Wie bereits angerissen, war die Pandemie meines Erachtens nur ein Beschleuniger einer längst stattfindenden Entwicklung. In Zeiten horrender Mieten in den Ballungsgebieten und einer neuen Generation Mensch, die sich nicht nur über Arbeit definiert, hat die Bewegung hin zu mehr Flexibilität schon lange eingesetzt. Noch nutzt gemäß unserer Umfrage die Mehrheit der Angestellten ein Tischtelefon, aber die notgedrungene Zunahme an mobilen Lösungen ist unweigerlich: Der Markt entwickelt sich natürlich weiter von einem trotz erfolgter Verlagerung noch recht ortsgebundenen Arbeiten im Home-Office hin zu noch flexibleren Lösungen für das „Work from Anywhere". In diesem Rahmen eine gute Unified-Communication- oder Videokonferenz-Schnittstelle zu bieten, die Anwenderkomfort, aber auch Datensicherheit für den Arbeitgeber bietet, ist die Kunst. Und ja, wir arbeiten aktuell selbstverständlich an unterschiedlichen Lösungen für diesen wachsenden Flexibilitätsbedarf.

Ulrich Parthier: *Design bei Hard- und Software – Ergonomie – Funktionalität – Nachhaltigkeit – Vision, wie würden Sie diese unterschiedlichen Aspekte gewichten und wie sieht die Zukunft der Telefonie und der IP-Welt aus?*

Gernot Sagl: Oh, ich denke, ob nun Design oder Ergonomie an vorderster Front steht, wird jeder Anwender für sich entscheiden. Der Markt wird entsprechend reagieren und Unternehmen ihre Vision anpassen. In puncto Nachhaltigkeit und Sicherheit sehe ich allerdings keine Kompromissmöglichkeit: Beides mit einem flexiblen Einsatz kombiniert, schon ist der Eckstein für die Zukunft der Telekommunikation gelegt. Kommuniziert wird immer weiter, mal per Video und Kopfhörer, mal per Tischtelefon und Hörer. Zudem können Geräte untereinander kommunizieren und für eine Optimierung von Umgebung und Prozessen sorgen – die Möglichkeiten und Szenarien sind vielfältig!

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



MOBILE ARBEITSPLÄTZE

PROBLEM: KRITISCHE SICHERHEITSNIVEAUS

Überlastete Netzwerke, Sicherheitsmängel bei der mobilen Arbeit und verteilte Datensilos sind nur einige Herausforderungen, mit denen Unternehmen noch vielerorts zu kämpfen haben. In Krisenszenarien gilt es nicht nur die kritischen Prozesse und die Produktivität zu erhalten, sondern auch, das bestehende Sicherheitsniveau im Datenverkehr nicht zu verringern. Mit der wachsenden Zahl an Zugriffspunkten durch Heim-Arbeitsplätze wachsen jedoch die Sicherheitsrisiken in den Unternehmensnetzwerken. Auch die Vermischung von privaten und betrieblichen Infrastruktur-Komponenten untergraben in vielen Betrieben bestehende Sicherheitsrichtlinien.

Die Arbeit im Homeoffice prägt den Alltag bei vielen Unternehmen in Deutschland. Da der Begriff „Homeoffice" recht inflationär Verwendung findet, muss man hier allerdings klar unterschieden, denn nur die wenigsten Arbeitnehmer verfügen tatsächlich über ein klassisches Homeoffice: nämlich einen Arbeitsplatz in den eigenen vier Wänden oder an einem externen Standort, der nicht nur mit der benötigten Soft- und Hardware vom Arbeitgeber ausgestattet ist, sondern auch über DSGVO-konforme Zugangsbeschränkungen verfügt. Das, worauf viele Arbeitnehmer in den Krisenjahren 2020 und 2021 zurückgegriffen haben, ist eher als mobiles Arbeiten zu verstehen. Gefährlich wird es vor allem dann, wenn Lösungen schnell und nicht mit der erforderlichen Sorgfalt eingeführt werden, nur um den Betrieb aufrechtzuhalten, auch wenn dies zu Lasten der Sicherheit und des Datenschutzes geht. Diese Sicherheitslücken zu schließen, wird auch 2022 noch viele Unternehmen beschäftigen.

Sichere Anbindung von Heim-Arbeitsplätzen

Welche Auswirkungen der Übergang zur modernen Heimarbeit für die Betriebsabläufe in deutschen Unternehmen mit sich gebracht hat, hängt entscheidend vom Geschäftsmodell, den individuellen Anforderungsprofilen der Mitarbeiter und nicht zuletzt von der betrieblichen IT-Infrastruktur ab. Welche Ansprüche werden zum Beispiel an die Kommunikation und den Datenaustausch gestellt? Während für den einen etwa ein einfaches Dokumenten-Sharing ausreicht, benötigt ein anderer Mitarbeiter einen Remote-Arbeitsplatz, um an einem komplexen 3D-Modell zu arbeiten. Viele Betriebe mussten zudem mehr Arbeitnehmer in die Heimarbeit schicken, als betriebliche Ressourcen zur Verfügung standen. „Vor diesem Hintergrund verzeichnen wir bis heute eine deutliche Zunahme an Anfragen, um teilweise mehrere Hundert Arbeitsplätze remote arbeitsfähig zu machen und die bestehenden Sicherheitslücken zu schließen. Das Prinzip: Der Nutzer greift mit seinem privaten Arbeitsgerät über eine per Hardware-authentifizierte Terminal-Session auf eine virtuelle Desktop-Umgebung (VDI: Virtual Desktop Infrastructure) des Unternehmens zu. Die private Betriebssystemumgebung und die betriebliche Anwendungsoberfläche sind dabei jederzeit physisch vollständig voneinander getrennte Systemwelten. Auf dem privaten Endgerät können so keine betrieblichen Daten abgespeichert werden, da es keinen Datenzugriff zwi-

DER BEGRIFF „HOMEOFFICE" WIRD OFT FALSCH INTERPRETIERT, WAS DEN BLICK AUF DIE EIGENTLICHEN HERAUSFORDERUNGEN MOBILER ARBEITSPLÄTZE VERDECKT.

Holger Priebe, Teamleiter Microsoft & Virtualisierung, Netzlink Informationstechnik GmbH, www.netzlink.com

MIT DER ZUNEHMENDEN NUTZUNG DES MOBILEN ARBEITENS WIRD DER ITK-BETRIEB FÜR ALLE UNTERNEHMEN NOCH WICHTIGER.

Sven-Ove Wähling, Geschäftsführer, Netzlink Informationstechnik GmbH, www.netzlink.com

schen privater und betrieblicher Umgebung gibt. Das ist eine einfache und effektive Lösung, um eine Vielzahl von Heim-Arbeitsplätzen anzubinden und auch unter Wirtschaftlichkeitsaspekten ein ausreichend hohes Schutzniveau aller Clients zu gewährleisten", so Holger Priebe, Teamleiter Microsoft und Virtualisierung bei Netzlink.

Engpässe physischer Kapazitäten

Mit der konzeptionellen Frage der Anbindung an das Unternehmensnetzwerk schließen sich auch Fragen nach den physischen Kapazitäten des bestehenden Netzwerkes an: Habe ich eine ausreichende Firewall und genügend Bandbreite zur Verfügung, um alle meine mobilen Mitarbeiter gleichzeitig remote per VPN anzubinden? Müssen die Mitarbeiter überhaupt auf Microsoft-Maschinen remote arbeiten oder reicht es aus, sie über einen klassischen Client arbeiten zu lassen, zum Beispiel durch lokalen Zugriff auf die Office-365-Cloud, sodass die Bandbreite des eigenen Netzwerkes nicht belastet wird? Dabei ist zu beachten, dass es nicht damit getan ist, den Zugang einmalig herzustellen. Es müssen aufgrund dynamischer Anpassungen der IT-Infrastruktur auch Belastungstests stattfinden, um einen reibungslosen und zuverlässigen Live-Betrieb ohne Unterbrechung der Arbeitsabläufe zu gewährleisten.

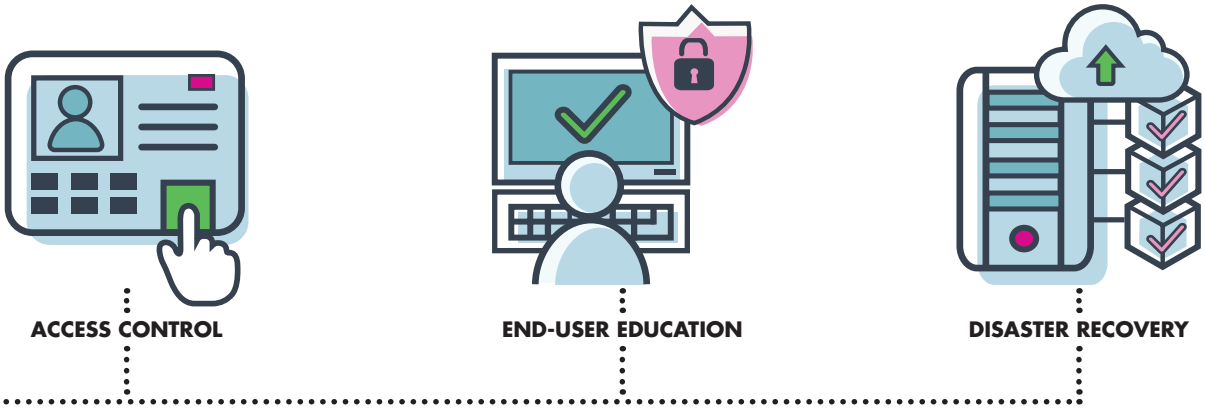
OPTIMALERWEISE WIRD FÜR DIE HEIMARBEIT EIN WLAN-GASTZUGANG VERWENDET, DAMIT ETWAIGE FIRMENDATEN NICHT ÜBER DASSELBE NETZ ÜBERTRAGEN WERDEN, DAS AUCH ANDERE ANWENDER IM HAUS NUTZEN.

Niklas Lay,
Teamleiter Netzwerk & IT Security,
Netzlink Informationstechnik GmbH,
www.netzlink.com

Aber auch der Mitarbeiter braucht eine ausreichende Bandbreite im Heimnetzwerk, um mit der gewohnten IT-Qualität remote zu arbeiten. Ist der Mitarbeiter nur mit einem Client online, sodass es ausreicht, einen VPN-Tunnel aufzubauen, oder muss er vielleicht sogar über einen abgesetzten Access-Point angebunden werden? Das private WLAN ist vielleicht auch durch andere Benutzer bereits ausgelastet oder entspricht nicht den Sicherheitsanforderungen des Unternehmens. Hier kann mit einer LTE-Karte und einem LTE-Modem des Arbeitgebers die Performance und Sicherheit der Verbindung kostengünstig verbessert werden.

Absicherung des Zugangs

Die Absicherung des Zugangs ist dabei stets ein neuralgischer Punkt. „Der WLAN-Zugang sollte mit einem starken Passwort versehen sein, das in regelmäßigen Abständen gewechselt wird. Optimalerweise wird für die Heimarbeit ein WLAN-Gastzugang verwendet, damit etwaige Firmendaten nicht über dasselbe Netz übertragen werden, das auch andere Anwender im Haus nutzen. Je nach



Rolle und Berechtigung stellt sich zudem die Frage, ob die Anmeldung im Netzwerk lediglich über Username und Passwort ausreichenden Schutz bietet oder die Zugriffssicherheit mit einer Zwei-Faktor-Authentifizierung erhöht werden sollte," führt Niklas Lay, Teamleiter Netzwerk und IT Security bei Netzlink, aus. „Benötigt man bei einzelnen Arbeitsgeräten zusätzlichen Schutz, so kann man auch die Verschlüsselung der Festplatte aktivieren."

BYOD – Bewusstsein für Risiken schärfen

Eine latente Gefahr für Unternehmen besteht darin, den Einsatz privater Endgeräte ohne bestehende Leitlinien zu dulden, etwa um eine vermeintlich hohe Mitarbeiterproduktivität zu erhalten. Private Endgeräte sind auch nach zwei Jahren im Krisenmodus für die Datensicherheit im Unternehmen ein ernstzunehmendes Risiko, da sie sich weitgehend der unternehmerischen Kontrolle entziehen. „Vielen Arbeitnehmern fehlt hier zudem das Sicherheitsbewusstsein, dass Smartphones mobile und recht leistungsfähige kleine Rechner mit mitunter nennenswerten Datenspeichern darstellen, die ebenso wie ihre Desktop-Pendants über Firewalls und aktuellen Virenschutz abgesichert werden müssen. Viele Nutzer sind bei einer schlagartigen Veränderung der Arbeitssituation nicht in der Lage, Gefahren und Risiken für sich und das Unternehmen abzuschätzen. Insofern liegt es im Interesse der Unternehmen, das Sicherheitsbewusstsein der Mitarbeiter für die betriebliche Nutzung privater Smartphones mit entsprechenden Leitfäden zu schärfen, um das Unternehmen vor Angriffen auf die IT von außen zu schützen", mahnt Lay.

Rüstzeug für die nächste Krise: Notfallplan in der Tasche

Mit der zunehmenden Nutzung des mobilen Arbeitens wird der IKT-Betrieb für alle Unternehmen noch wichtiger. Die Anwendungen und Daten dürfen einfach nicht mehr ausfallen. Die beste Vorbereitung für ein erfolgreiches Business Continuity Management ist ein Notfall-Handbuch. Dieses dient der Aufrechterhaltung und Fortführung der kritischen Prozesse, wenn bestimmte Ereignisse die Betriebsabläufe stören oder verhindern. Die komplexen (IT-)Strukturen unserer globalen Kollaborationsnetzwerke machen uns in hohem Maße abhängig von einem kontinuierlichen Geschäftsbetrieb zwischen allen Prozessbeteiligten – intern und extern. Mit der fortschreitenden Digitalisierung wird dies noch wichtiger. Ein nachhaltiges Risikomanagement muss Bestandteil jeder Organisation sein, um die negativen Auswirkungen von Störungen auf den Geschäftsbetrieb einzugrenzen. Leider muss oft erst ein Schadensereignis eintreten, bevor tatsächlich gehandelt wird. Um auf Störungen angemessen zu reagieren, bedarf es einer vorher geplanten und streng methodischen Vorgehensweise, die sämtliche kritischen Prozesse berücksichtigt, Verantwortlichkeiten festlegt und Kommunikationsprozesse definiert, um in kürzester Zeit zu einem produktiven ITK-Betrieb zurückzukehren.

Sven-Ove Wähling

Das eBook „Mobiles Arbeiten:
Eine Orientierungshilfe von Netzlink"
steht zum kostenlosen
Download bereit.
www.netzlink.com

ORTSUNABHÄNGIGES ARBEITEN

ES FÜHRT KEIN WEG MEHR DARAN VORBEI

Wie lässt sich ortsunabhängiges Arbeiten für Mitarbeitende im gesamten Unternehmen realisieren? Gemeinsam diskutieren Dirk Ramhorst, CDO und CIO in der Chemieindustrie, und Eric Schott, CEO von Campana & Schott, welche Schritte dafür nötig sind.

it management: *Ortsunabhängiges Arbeiten ist ein Thema mit vielen Facetten. Was müssen Unternehmen aus Ihrer Sicht nun konkret angehen?*

Dirk Ramhorst: Ich glaube, die technische Readiness kann man nun schon fast abhaken. Daher steht das Thema Organisation derzeit im Mittelpunkt, um auch nach der Pandemie reibungslose Abläufe zu gewährleisten. Dazu zählt vor allem die Vorbereitung auf Hybrid Work. So müssen die Mitarbeitenden ihre Ausstattung in Büro und Homeoffice flexibel nutzen können. Dies ist richtig zu organisieren, zu dimensionieren und bei Bedarf mit Betriebsvereinbarungen zu formalisieren.

Eric Schott: Da kann ich mich nur anschließen. Unternehmen haben in der Vergangenheit bewiesen, dass Homeoffice technologisch umgesetzt werden kann. Aber die bisherige Polarisierung zwischen Büro und Homeoffice muss überwunden und ein wirkliches Seamless Office realisiert werden. Es geht eben weniger um die Frage, von wo aus Mitarbeitende arbeiten, sondern vielmehr darum, wie jeder Einzelne die jeweiligen Aufgaben optimal erfüllen kann. Zum Beispiel startest Du im Büro mit einem Meeting am PC, legst es auf das Handy, um von unterwegs weiter daran teilzunehmen, und arbeitest dann zu Hause an der zuvor begonnenen Präsentation nahtlos weiter. Das erhöht Effizienz, Produktivität und Zufriedenheit der Mitarbeitenden, da bisherige Medienbrüche vermieden werden. Dafür ist jedoch eine Strategie erforderlich, wie die Zukunft der Arbeit aussehen soll.

it management: *So wie das klingt, verändert sich die Art der Zusammenarbeit signifikant. Wie macht sich das bemerkbar?*

Eric Schott: Wir sehen derzeit, dass sich das Verhältnis zwischen Arbeitgeber und Arbeitnehmer umdreht. Bislang stand im Vordergrund, wie der Mitarbeitende den Betrieb des Unternehmens aufrechterhalten kann. Heute geht es um die Frage: Wie kann das Unternehmen eine mitarbeiterzentrische Umgebung bereitstellen, also die Employee Experience verbessern? Das beginnt bei der Ausstattung

WER ZU VIELE BAUSTELLEN GLEICHZEITIG AUFMACHT, VERZETTELT SICH HÄUFIG IN DEN VERSCHIEDENEN PROJEKTEN UND KOMMT NICHT VORAN.

Eric Schott, CEO, Campana & Schott, www.campana-schott.com

und bezieht sich dann vor allem auf die Denkweise, dass die Umgebung des Mitarbeitenden weniger von den Vorgaben des Unternehmens geprägt sein soll, sondern mehr von seinen Bedarfen. Aber es geht noch weiter: Erste Unternehmen bewerben sich quasi schon von sich aus bei den Bewerbern.

Dirk Ramhorst: Das kann ich bestätigen. Bei Bewerbungsgesprächen ist Homeoffice immer ein Thema. Dabei ist die grundsätzliche Möglichkeit schon selbstverständlich. Es geht inzwischen darum, wie ein Unternehmen es unterstützt: mit Equipment, Licht, Mikrofon, Kamera, Collaboration-Anwendungen. Hier formulieren Bewerber auch entsprechende Erwartungen.

it management: *Nach wie vor gibt es viele Unternehmensbereiche, in denen Mitarbeitende nicht „einfach ins Homeoffice" geschickt werden können. Endet also Hybrid Work am Schreibtisch?*

Eric Schott: Nein, Hybrid Work erfordert nicht nur eine Anpassung der Arbeitsplätze von Information Workern, die hauptsächlich am Schreibtisch arbeiten, sondern auch von Frontline Workern. Dazu gehören mehr als 80 Prozent der Belegschaft, wie beispielsweise Techniker an Fertigungsstraßen, Pflegepersonal in Kliniken, Fahrer, Sicherheits- und Reinigungskräfte, Kassen- oder Verkaufspersonal. Hier müssen sich Unternehmen Gedanken machen, wie sie diese in den zunehmend digitalen Arbeitsplatz einbinden.

Dirk Ramhorst: Auf jeden Fall. Ich durfte die letzten beiden Jahre in Bayern die Initiative Arbeitswelt 4.0 begleiten. Da ging es nicht nur um das Thema Homeof-

fice, sondern auch generell darum, wie Digitalisierung Arbeitswelten verändern kann. Ein großes Anliegen war, dass Homeoffice die Gesellschaft nicht spaltet – in diejenigen, die es nutzen können, und diejenigen, die vor Ort sein müssen. Dazu muss man überlegen, wie Digitalisierung den Frontline Workern helfen kann. Zum Beispiel hat das Thema digitaler Zwilling einen großen Beitrag geleistet. Wir konnten dadurch eine ganze Chemie-Anlage bis zu einem gewissen Grad aus der Ferne kontrollieren und steuern. Eine Inbetriebnahme in Korea ließ sich über Videokonferenz durchführen. Dabei wurden alle Sensordaten im digitalen Zwilling in Deutschland angezeigt. So konnten die deutschen Ingenieure den Kolleginnen und Kollegen in Korea genau sagen, welche Einstellungen sie auf welche Weise anpassen mussten.

it management: *Was ist bei den sogenannten Frontline Workern vor allem zu beachten?*

Eric Schott: Wir haben bei unseren Kunden immer wieder erlebt, dass zum Beispiel Mitarbeitende in der Produktion per WhatsApp-Gruppen Schichtwechsel organisieren. Teilweise tauschen sie darüber sogar Dokumente aus. Hier muss die IT die Chance erkennen, die Sicherheit über eine vom Unternehmen zentral bereitgestellte Lösung zu erhöhen. Wenn man also über digitale Arbeitsplätze nachdenkt, sollte man Frontline Worker berücksichtigen. Das ist für mich auch eine Form von nachhaltiger Arbeit, denn es fördert ein neues Miteinander. Die technologische Einbindung von Frontline Workern lässt wirklich alle im Unternehmen wieder näher zusammenrücken. Für mich ist das auch eine gesellschaftliche Aufgabe.

Dirk Ramhorst: Dazu habe ich auch ein Beispiel, das Projekt „Digitales Programm für alle". Produktionsmitarbeitende besitzen keinen Bildschirmarbeitsplatz und damit auch kein Intranet. Mit diesem Projekt haben wir den Mitarbeitenden Zugang zu bestimmten Intranet-Services,

DIE „ONE SIZE FITS ALL"-LÖSUNG EXISTIERT NICHT. DAS GILT FÜR DIE DIGITALISIERUNG IM ALLGEMEINEN UND FÜR NEW WORK IM SPEZIELLEN.

Dirk Ramhorst, CDO und CIO in der Chemieindustrie

von HR bis zur Brotzeit-Bestellung, per App auf ihrem privaten Smartphone oder per Kiosk-PC zur Verfügung gestellt. Damit konnten wir eine Connectivity im Sinne der Digitalisierung des Arbeitsplatzes für diese Mitarbeitenden erreichen. Dabei wurden auch viele bislang papierbasierte Prozesse digitalisiert. Das kam wahnsinnig gut an.

it management: *Wie können Unternehmen nun konkret den digitalen Arbeitsplatz angehen?*

Eric Schott: Viele Unternehmen haben durch die Erfahrungen der vergangenen Jahre eine Wunschvorstellung, wie die Implementierung des digitalen Arbeitsplatzes aussehen kann und möchten alles am besten sofort angehen. Aber wer zu viele Baustellen gleichzeitig aufmacht, verzettelt sich häufig in den verschiedenen Projekten und kommt nicht voran. Daher macht es Sinn, sich jedes Unternehmen einzeln anzuschauen. Welche Wünsche haben die Mitarbeiter und welche die Führungspersonen? Welche Hindernisse stehen im Weg? Welche Implementierungen sind sofort nötig und für was hat man noch etwas Zeit? Die Einführung eines digitalen Arbeitsplatzes sollte strategisch geplant und um die geeigneten organisatorischen Prozesse ergänzt werden. Dazu gehören eine moderne Unternehmenskommunikation, eine aktuelle Sicherheitskultur und -architektur sowie eine erhöhte Agilität der Mitarbeitenden. Dass man auf diesem Weg auch mal die Richtung wechselt und Dinge ausprobiert, gehört dazu. Denn: die eine ideale Lösung direkt zu entwickeln ist eine Illusion. Die grundlegende Strategie und Roadmap sind entscheidend.

Dirk Ramhorst: Die „One Size fits all"-Lösung existiert nicht. Das gilt für die Digitalisierung im Allgemeinen und für New Work im Speziellen. Es gibt unterschiedliche Kulturen, Organisationen, Generationen und technische Awareness. Darauf muss man spezifisch eingehen und analysieren, wo stehe ich, wo komme ich her, welche Services sind schon etabliert. Auf dieser Basis können Unternehmen ihren individuellen Weg gehen.

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

UNVERZICHTBARES ASSET

DAS GREEN OFFICE ALS WETTBEWERBSVORTEIL

Unternehmen stehen vor großen und vielfältigen Herausforderungen, denn die Erwartungen von Kunden und Mitarbeitern nehmen sie in einer Vielzahl an Themen in die Pflicht. Neben dem Kerngeschäft müssen Entscheider die digitale Transformation, flexible Arbeitsmodelle und konkrete Maßnahmen für den Klima- und Umweltschutz vorantreiben. Nachhaltigkeit ist dabei zu einem entscheidenden Wettbewerbsfaktor geworden, der ganzheitlich gedacht werden muss.

Der Klimaschutz ist eine der größten gesellschaftlichen Aufgaben unserer Zeit und erfordert insbesondere bei Unternehmen ein Umdenken, bei denen papiergebundene Prozesse noch immer den Ton angeben. Das Schonen von Ressourcen bei der Erfassung, Bearbeitung und Archivierung von Informationen leistet einen wichtigen Beitrag für den Schutz der Umwelt – und auch für die eigene Klimabilanz. Ein zeitgemäßes Informationsmanagement zeichnet sich deshalb nicht nur durch eine schnelle Verfügbarkeit von Informationen aus, sondern auch durch nachhaltige Prozesse und die Nutzung klimaschonender Technologien.

Nachhaltigkeitsstrategien klammern das Büro oft aus

Prozesse rund ums Informationsmanagement sind ein wichtiger Teil einer ganzheitlichen Strategie für mehr Nachhaltigkeit. Obwohl sie von immer mehr Unternehmen als wichtiges strategisches Thema gesehen werden, scheinen Umwelt- und Klimaschutz in vielen Fällen noch immer nur punktuell oben auf der Agenda Platz zu finden. Die Prozesse im Büro werden dabei häufig ausgeklammert.

So hatte jedes dritte Unternehmen in Deutschland auch im Jahr 2021 noch keine Nachhaltigkeitsstrategie für die eigenen Büroprozesse etabliert, wie eine Umfrage von Statista im Auftrag von Kyocera Document Solutions Deutschland zeigt. Bei kleineren Unternehmen liegt die Quote sogar noch deutlich höher: Fast die Hälfte gab an, keine Strategie für das Green Office zu haben.

Großes Potenzial bleibt ungenutzt

Dabei steckt in Büroprozessen oft ungeahnt großes Potenzial für eine bessere Klimabilanz. Ihr ökologischer Fußabdruck entsteht nicht nur durch den „sichtbaren" Verbrauch von Material, sondern auch im Hintergrund – etwa durch den Rohstoffeinsatz bei der Herstellung und den Energiebedarf bei der Nutzung des IT-Equipments. Dabei spielt es keine Rolle, ob sich die Mitarbeiter im Corporate- oder im Homeoffice befinden.

Green-Office-Strategien, die digitale Prozesse und einen schonenden Umgang mit Ressourcen in den Mittelpunkt stellen, können einen immensen Beitrag zur Erreichung von CSR- und Klimazielen leisten, indem sie papiergebundene Vorgänge ablösen und bei IT-Anschaffungen auch deren CO_2-Fußabdruck einbeziehen.

Kleine Schritte – große Wirkung

Erster Ansatzpunkt vieler Unternehmen, die eine Strategie für das Green Office verfolgen, ist die Digitalisierung von papierintensiven Prozessen wie der Rechnungsbearbeitung, dem Vertragsmanagement oder der Archivierung von Dokumenten. Neue Prozesse für eine Vielzahl unterschiedlicher Dokumente einzuführen, muss dabei nicht von heute auf morgen alle Prozesse oder alle Abteilungen von Grund auf reformieren – und oft ist das auch gar nicht notwendig. Moderne Dokumentenmanagement-Lösungen sind deshalb modular aufgebaut und ermöglichen Unternehmen, Prozesse im individuellen Tempo digital abzubilden und entsprechend des eigenen Bedarfs Schwerpunkte zu setzen.

Viele analoge Vorgänge haben sich über viele Jahre hinweg etabliert. Deshalb ist es wichtig, Mitarbeiter früh mit einzubeziehen und für den Nutzen der Veränderungen für ihre Arbeit und den Erfolg des Unternehmens zu sensibilisieren. Das betrifft grundlegende Veränderungen wie die Einführung neuer Dokumentenmanagement-Software genauso wie vermeintlich kleine Umgewöhnungen wie die Festlegung neuer Regeln für den Ausdruck von Dokumenten wie dem beidseitigen Duplex-Druck als Standard, um Papier zu sparen. Auch mit solchen Maßnahmen kann bereits viel erreicht werden.

Nachhaltigkeit als Entscheidungskriterium

Nachhaltigkeit hat auch als Kriterium bei Kaufentscheidungen, etwa beim Autokauf – aber auch im Supermarkt –, an Bedeutung gewonnen. Deshalb wird auch Mitarbeitern zunehmend wichtig, zu mehr Nachhaltigkeit in ihrem Arbeitsplatz beitragen zu können. Laut der Umfrage von Statista würden beispielsweise 80 Prozent der befragten Büroangestellten, die aktiv in Entscheidungen zur Nachhaltigkeitsstrategie involviert sind, den Druckeranbieter wechseln, wenn dieser auf die CSR-Ziele einzahlt.

Dass soziale und ökologische Verantwortung zu einem entscheidenden Kaufkriterium geworden ist, hat auch Einfluss auf die Kriterien, nach denen Unternehmen und Behörden Lieferanten und Dienstleis-

ter auswählen. Öffentliche Ausschreibungen und auch immer mehr Geschäftsentscheidungen beziehen die Klimabilanz des Anbieters mit ein. Wer hier das Büro außer Acht lässt, verspielt vielleicht die Chance auf wichtige Projekte und gerät im Wettbewerb schnell ins Hintertreffen. So wird das Green Office langfristig zum unverzichtbaren Asset für Unternehmen, weil Nachhaltigkeit unverzichtbar für wirtschaftlichen Erfolg sein wird. Nachhaltigkeit und Wirtschaftlichkeit zu vereinen wird in den kommenden Jahren deshalb eine der größten Aufgaben für Unternehmen sein.

Klimafreundlich drucken und kopieren

Dass das Thema Drucken bei Green-Office-Strategien eine wichtige Rolle spielt erkennen inzwischen immer mehr Unternehmen in Deutschland. Laut Statista-Umfrage haben 38 Prozent deshalb feste Regeln für das Ausdrucken von Dokumenten eingeführt. In vielen Unternehmen und Behörden haben sich beispielsweise Print-and-Follow-Lösungen bewährt, bei denen sich Mitarbeiter am Gerät authentifizieren müssen, um den Druckvorgang auszulösen. Das vermeidet Fehldrucke, die versehentlich ausgelöst wurden oder auf dem falschen Drucksystem im Netzwerk gelandet sind.

Auch die Hardware selbst kann dabei zu einer besseren Klimabilanz beitragen, indem bei der Anschaffung auf Ressourcenschonung, Langlebigkeit und Energieeffizienz geachtet wird. Die CO_2-Emissionen, die über den gesamten Lebenszyklus eines Druckers oder Multifunktionssystems noch nicht vermieden werden können, können über Klimaschutzprogramme wie Kyocera Print Green in zertifizierten Klimaschutzprojekten kompensiert werden.

Informationsprozesse: flexibel, schnell und nachhaltig

Die effiziente Gestaltung digitaler und analoger Prozesse zählt zu den effektivsten Hebeln, die Unternehmen zur Verfügung stehen, um dem Wettbewerb einen Schritt voraus zu sein. Nur wer ohne Zeitverzug auf alle wichtigen Informationen zugreifen und Wissen einfach teilen kann, ist in der Lage, informierte Entscheidungen schnell zu treffen und Herausforderungen zu bewältigen, bevor sie zu Hindernissen anwachsen.

Dabei darf Nachhaltigkeit nicht außen vor bleiben, denn auch das nachhaltige Management von Informationen zählt zu den Faktoren, die über den Erfolg eines Geschäftsmodells entscheiden können. Deshalb muss eine Nachhaltigkeitsstrategie immer auch alle Unternehmensbereiche mit einbeziehen.

Daniela Matysiak

www.kyoceradocumentsolutions.de

WÜRDEN SIE IHREN DRUCKERANBIETER WECHSELN, WENN DIESER FINANZIELL ZU IHRER NACHHALTIGKEITSSTRATEGIE BEITRAGEN WÜRDE?

79 %
Ja, ich würde wechseln!

12 %
Ich weiß es nicht

9 %
Nein, das würde ich nicht

Quelle: KYOCERA Document Solutions

HERAUSFORDERUNG DIGITALISIERUNG

MIT NO-CODE TROTZ FACHKRÄFTEMANGEL PROJEKTE UMSETZEN

Mit No-Code-Plattformen können individuelle Anwendungen zur Digitalisierung verschiedener Prozesse ohne Programmierkenntnisse erstellt werden. Damit sind Unternehmen bei der Software-Entwicklung weniger abhängig von Fachkräften. it management sprach mit Thorsten Winternheimer, CEO Necara GmbH, über Lösungen, die den Zugang zu digitaler Transformation und Software-Entwicklung erleichtern und diese als Kernkompetenz im Unternehmen etablieren.

it management: *Herr Winternheimer, nach einer aktuellen Studie des Bitkom ist die Zahl der unbesetzten Stellen für IT-Kräfte 2021 in Deutschland auf 96.000 gestiegen – das ist ein Zuwachs von 12 Prozent. Inwiefern können Low-Code- und No-Code-Plattformen zur Lösung dieses Problems beitragen?*

Thorsten Winternheimer: Diese Zahlen zeigen deutlich, dass wir uns in einem wachsenden Arbeitnehmermarkt befinden. Wegen der großen Nachfrage werden die IT-Fachkräfte immer teurer. Da

setzen sich dann eher große Firmen durch, die besonders zahlungskräftig sind. Der Mittelstand, der ja sowieso schon Schwierigkeiten mit der Digitalisierung hat, geht oft leer aus. Low-Code-Plattformen sind eine Möglichkeit, um vorhandene IT-Kräfte und Programmierer zu entlasten. Prozesse werden dabei über ein grafisches User Interface zusammengesetzt. So wird weniger eigener Code benötigt. Entwickler erzielen dadurch schnellere Ergebnisse und sind dem hohen Arbeitspensum besser gewachsen. Mit No-Code wird dieser Ansatz einen Schritt weiter gedacht. Viele Firmen haben eben kaum ITler, die sie entlasten können. Da muss die Schwelle zur Softwareentwicklung niedriger sein. Mit No-Code ist das komplett ohne eigenen Code, also im Prinzip auch ohne Programmierkenntnisse möglich. Mit fertigen Codebausteinen werden individuelle Anwendungen zusammengesetzt, die dann direkt einsetzbar sind. Dadurch gibt es nicht mehr Fachkräfte, aber Unternehmen können ihre Digitalisierungsprojekte trotzdem umsetzen.

it management: *Eine andere Möglichkeit wäre doch auch der Einkauf von fertigen Software-Lösungen für die verschiedenen Belange. Welche Vorteile hat No-Code demgegenüber?*

Thorsten Winternheimer: Fertige Software, auch Standardsoftware genannt, ist meist eine bedeutende Kostenstelle - besonders wenn man für unterschiedliche Unternehmensbereiche Lösungen braucht. Das summiert sich auf. Mit dem Erwerb solcher Software ist es oft noch nicht getan, da sie ja auch an die individuellen Unternehmensstrukturen angepasst werden muss. Dafür sind oft auch wieder Fachkräfte nötig. Wenn man die Anpassung geschafft hat, bleiben die Strukturen aber nicht immer genau so bestehen. Moderne Unternehmen entwickeln sich stetig weiter - und mit ihnen die Prozesse. Es sind also immer wieder Modifizierungen notwendig, um effizient zu bleiben. Mit No-Code ist das kein großes Problem mehr, weil Angestellte in den

MODERNE UNTERNEHMEN ENTWICKELN SICH STETIG WEITER – UND MIT IHNEN DIE PROZESSE.

Thorsten Winternheimer,
CEO, Necara GmbH, www.saas.do

Fachabteilungen ihre eigenen Prozesse mit wenigen Klicks anpassen können. Anders als bei Standardsoftware sind die Einsatzmöglichkeiten von No-Code dabei nicht begrenzt. Wenn man eine Idee hat, kann man sie meist in wenigen Tagen oder gar Stunden mit einer neuen Applikation umsetzen. Das geht einfach schneller und macht auch mehr Spaß als sich mit Standardsoftware herumzuschlagen.

it management: *Nun gibt es ja schon eine Reihe von No-Code-Plattformen. Die Anforderungen in verschiedenen Branchen unterscheiden sich. Wie findet man da die richtige Plattform für sein Unternehmen?*

Thorsten Winternheimer: Am wichtigsten ist, dass die Plattform für den professionellen Gebrauch und komplexe Szenarien im Backoffice geeignet ist. Die Nutzung ist oft über die Cloud oder On-Premises im eigenen Rechenzentrum möglich. Bestenfalls geht beides. Ich persönlich rate auch grundsätzlich zu einer Plattform, die nicht auf bestimmte Branchen oder Unternehmensbereiche spezialisiert ist. So verbaut man sich nicht von vornherein Möglichkeiten und kann trotzdem technisch aus den Vollen schöpfen. Nur weil eine Software vielseitig nutzbar ist, heißt das nicht, dass sie in einzelnen Bereichen keine Top-Performance erbringen kann. Prozesse, Strukturen, Geschäftsfelder - das alles verändert sich - manchmal schneller als uns lieb ist. In der Coronakrise konnten nach meiner Erfahrung vor allem die Unternehmen den Schaden am besten begrenzen, die besonders anpassungsfähig aufgestellt waren. Software ist dabei längst zur wichtigsten Ressource geworden. Mit einer flexiblen No-Code-Plattform ist man für alle Eventualitäten gewappnet.

it management: *Was sind unter den vielen Möglichkeiten denn typische Anwendungsbeispiele?*

Thorsten Winternheimer: Es gibt einige Anwendungen und Systeme, die fast jedes Unternehmen ab einer gewissen Größe in irgendeiner Form braucht - angefangen bei einem ERP-System zur Ressourcenplanung. Da ist der Unterschied zwischen Standard- und Individualsoftware besonders groß. Das Fraunhofer Institut IAIS hat tausende IT-Leiter und CIOs nach den größten Schwächen ihrer ERP-Systeme befragt. Die Top 3 sind demnach die Kosten, fehlende Benutzerfreundlichkeit und hohe Komplexität. Mit No-Code kann man da gegensteuern, weil man schnell und einfach maßgeschneiderte ERP-Systeme für die individuellen Bedürfnisse bauen oder Bestandssysteme erweitern kann. Ähnlich sieht es im Vertrieb mit CRM-Systemen aus. Die größten Zeitfresser in Unternehmen sind oft Kleinigkeiten, die sich mit No-Code leicht automatisieren lassen. Die Rechnungserstellung beispielsweise oder Zeiterfassung; außerdem Monitoring, Datenerfassung, Qualitätsmanagement. Die Plattform fungiert dabei als Middleware, die alle Anwendungen zusammenhält.

it management: *Immer mehr Unternehmen setzen zur Modernisierung und für mehr Flexibilität in der IT auf Cloud Computing. Zur Vernetzung von Unternehmensanwendungen gewinnen deshalb webbasierte Anwendungsschnittstellen an Bedeutung. Wie konfiguriert man aber solche Schnittstellen ohne Code?*

Thorsten Winternheimer: Tatsächlich funktioniert das API-Management im besten Fall recht ähnlich wie die Entwicklung von Anwendungen - per Drag-and-Drop. Mit einem grafischen Element kann man Rahmenbedingungen für die Schnittstelle festlegen. Das Ganze lässt sich über eine Datenmaske spezifizieren. Die Schnittstelle kann dann per API-Call automatisiert angesteuert werden. So können alle Anwendungen im Unternehmen miteinander kommunizieren und Daten austauschen. Das wäre sonst ein Job, der manuell sehr viel Zeit kostet. Wenn sich an der Infrastruktur irgendetwas ändert, können auch die Schnittstellen jederzeit mit wenigen Klicks angepasst werden. Dadurch ist ein orchestrierter Datenstrom im gesamten Unternehmen möglich und man kann den Verwaltungsaufwand drastisch verringern. Eine hoch-automatisierte IT-Landschaft bildet das wichtigste Grundgerüst für jedes Kerngeschäft. Wer das jetzt berücksichtigt, macht alles richtig.

it management: *Und in Zukunft?*

Thorsten Winternheimer: ...werden wir sehen, wie sich immer mehr Unternehmen daran beteiligen. Auch der Handel im B2B-Sektor wird zunehmend automatisiert, weil Auftragsdaten über APIs ausgetauscht werden oder man Anwendungen für Handelspartner zur Nutzung bereitstellt. Manche sprechen bereits von einer API-Economy. Low- und No-Code-Anwendungen werden immer weiter verbreitet sein. Da sind sich Marktforscher und Experten einig. In den nächsten zehn Jahren werden Fachkräfte wohl immer noch knapp sein, aber vielversprechende Alternativen gibt es bereits jetzt.

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

RANSOMWARE

SICHERE DATENSPEICHERUNG IN UNSICHEREN ZEITEN

Martina Emminger, Channel Account Manager, iTernity

Omar Kohl, Senior Software Architect, iTernity

Wie können sich Unternehmen umfassend vor Ransomware-Angriffen schützen? Ransomware-Immunisierung erfordert mehrere Sicherheitsebenen. Da die Attacken immer raffinierter werden und längst auch Backups ins Visier geraten sind, reicht der einfache Einsatz einer Backup-Software nicht mehr aus.

Was Sie im Webinar erwartet:

- Wie Sie Ihre Daten dank Unveränderlichkeit (Immutable Storage mit WORM, S3, Object Lock) und einer minimierten Angriffsfläche effektiv gegen Cyber-Angriffe absichern können
- Wieso die Speicherinfrastruktur ein zentraler Baustein im Kampf gegen Ransomware ist und wie Sie die Sicherheit Ihrer geschäftskritischen Daten und Backups maximieren
- Wie Sie mehr aus Ihrer Speicherinfrastruktur herausholen: IT-Aufwände senken, Gesamtkosten halbieren, Datenwachstum bewältigen u.v.m.

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

Let's talk about Digital Health

26.–28. April 2022

Messegelände Berlin

GOLD Partner

CGM CompuGroup Medical · Dedalus HEALTHCARE SYSTEMS GROUP · ID Information und Dokumentation im Gesundheitswesen · medatixx Damit die Praxis läuft. · Meierhofer · nexus/ag · T… HEALTHCARE SOLUTIONS

SILBER Partner

3M · arvato BERTELSMANN · ascom · Cerner · D·M·I · Hewlett Packard Enterprise · i-SOLUTIONS HEALTH · m.Doc Smart Health Evolution · Meona · NUANCE · PHILIPS · RZV · SIEMENS Healthineers · Smartifyit! · Thieme · VISUS · vitagroup HEALTH INTELLIGENCE

DMEA Connecting Digital Health

Jetzt informieren auf dmea.de

In Kooperation mit: BVMI Berufsverband Medizinischer Informatiker e.V. · gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Unter Mitwirkung von: KHIT · CIO-UK

Veranstalter: bvitg

Organisation: Messe Berlin 200 Jahre Gastgeber von Welt

KONTROVERSTHEMA: TWO SPEED IT

HOPP ODER TOP? WAS IST RICHTIG, WAS FALSCH? **(TEIL 2 VON 2)**

Teil 1 konzentrierte sich auf die Vorteile verschiedener Entwicklungsgeschwindigkeiten innerhalb der IT und auf erste Erfolgsfaktoren. In Teil 2 werden nun weitere Erfolgsfaktoren aufgezeigt und in Advocatus Diaboli-Manier die Gegenpositionen skizziert.

Erfolgsfaktor: Vorgehensmodell für A und C

Ein Erfolgsfaktor ist das Vorhandensein von Vorgehensmodellen für die beiden Vorgehensweisen. In der Regel findet man nur ein starres, klassisches Vorgehensmodell vor, das verbindlich für alle eingesetzt werden muss. Hier fehlt es oft an der erforderlichen Flexibilität.

Ideal ist es, wenn es nur ein flexibles Vorgehensmodell gibt, das an die Erfordernisse des jeweiligen Projektes angepasst werden kann. Analog zu einem stufenlosen Schaltgetriebe wird dabei zu Projektbeginn die gewünschte Ausprägung des Projektes festgelegt:

- Welche Artefakte werden erstellt?
- Wann sind die Artefakte abzuliefern?
- Welche Quality-Gates müssen durchlaufen werden?
- Was sind die Qualitätsanforderungen an den jeweiligen Quality-Gates?

Wenn die Regularien es erlauben über geeignete Definitionen auf der einen Seite ein Projektvorgehen nach Wasserfall oder V-Modell und auf der anderen Seite ein Projektvorgehen nach Scrum oder Kanban einzustellen, dann sind die Regularien in der agilen Welt angekommen und eine gute Grundlage für die Software-Entwicklung.

Erfolgsfaktor: Mentalität der Teams

Wenn wir in einem Unternehmen zwei Geschwindigkeiten haben, dann wird sich dies auch in mehreren Teams manifestieren. Ein Schnitt, bei dem in einem Team zwei verschiedene Geschwindigkeiten eingesetzt werden, bringt eine neue Komplexität mit sich und wird hier erst einmal nicht weiter betrachtet.

Damit ist es wichtig, dass die Teams die passende Mentalität mitbringen:

- Die Mitglieder der A-Teams sind daran interessiert, Neues auszuprobieren und sich schnell in neue Technologien einzuarbeiten.
- Die Mitglieder der C-Teams sind daran interessiert, das Bewährte– Applikationen und Vorgehensweisen– zu erhalten und gegen unnötige Veränderungen zu schützen.

Wenn jemand in einem Team eingesetzt wird, das seiner Mentalität nicht entspricht führt das zu Frustration und Demotivation und ist einer positiven Arbeitsatmosphäre abträglich. Also müssen die Teams so zusammengestellt sein, dass die

Mentalität der Teammitglieder dem jeweiligen Vorgehensmodell entspricht.

Erfolgsfaktor für Two-Speed-IT ist die Exit-Strategie

Two-Speed-IT kann ein Mittel sein, kurzfristig mehr Agilität in eine Organisation mit einem etablierten, klassischen Software-Entwicklungsmodell zu bringen. Mittel- bis langfristig kann ein Unternehmen es sich nicht leisten, unbewegliche Unternehmens-IT zu unterhalten. Der Markt ist und bleibt in den meisten Branchen in Bewegung. Dem muss die IT gerecht werden.

Deshalb ist es wichtig, sich dessen bewusst zu sein und frühzeitig in Richtung einer Exit-Strategie für die Two-Speed-IT zu steuern. Dabei ist der Ausweg nicht der Erhalt der Vorgehensweisen der C-Komponenten, sondern diejenige der A-Komponenten. Damit kann man über kurz oder lang mit der gesamten IT in der heute immer schnelllebigeren Welt ankommen.

Aber, es gibt auch eindeutig nur in eine Richtung tendierende Meinungen. Warum das so ist, erfahren sie hier.

Ist das Ende von Two Speed IT die Lösung?

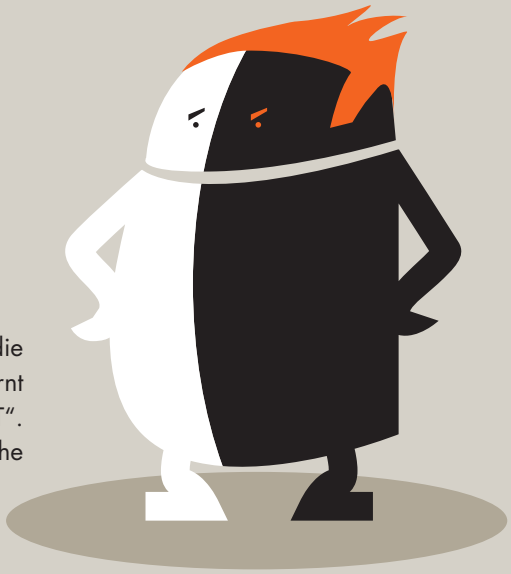
Eine klare Position zur IT der zwei Geschwindigkeiten vertritt die Boston Consulting Group. 2016 verkündeten Hanno Ketterer, Benjamin Rehberg, Christian N. Schmid und Djon Kleine in einer Expertise „The End of Two-Speed IT" zu dem Thema das Ende der zwei Geschwindigkeits-Methode für die IT.

Ihre Argumentation, nachzulesen im englischen Original auf BCG-Website, die wir hier in Auszügen wiedergeben, blickt zurück auf das Jahr 2012, als etablierte Unternehmen begannen, die Digitalisierung im Unternehmen voranzutreiben. Für BCG war das ein Konzept, das als „IT der zwei Geschwindigkeiten" oder eben auch nach unseren oben genannten Schlagworten bekannt wurde. Sie sahen es als eine Art notwendiger Kompromiss. Wenn IT-Organisationen digitale Initiativen unterstützen wollten, mussten sie schneller, flexibler und kooperativer arbeiten. Doch das Management betrachtete diese Methoden, die auf den 2001 im Agilen Manifest dargelegten Grundsätzen beruhten, oft als unerprobt und vielleicht sogar als ein wenig eigenwillig. Mit der IT der zwei Geschwindigkeiten wollte man sagen: „Keine Sorge, ihr könnt die neuen Techniken für neue Bereiche wie die Digitalisierung nutzen und den traditionellen Ansatz für geschäftskritische Kernfunktionen.

Damals, so die Autoren, sei das eine gute Idee gewesen, aber die Zeiten hatten sich geändert. Heute ist die IT der zwei Geschwindigkeiten ein Kompromiss, den sich die Unternehmen nicht mehr leisten können. Die Zukunft der IT ist eine einzige Geschwindigkeit: All-Agil. Das liegt nicht nur daran, dass sich Agilität bei

> TWO-SPEED-IT KANN EIN MITTEL SEIN, KURZFRISTIG MEHR AGILITÄT IN EINE ORGANISATION MIT EINEM ETABLIERTEN, KLASSISCHEN SOFTWARE-ENTWICKLUNGSMODELL ZU BRINGEN. MITTEL- BIS LANGFRISTIG KANN EIN UNTERNEHMEN ES SICH NICHT LEISTEN, UNBEWEGLICHE UNTERNEHMENS-IT ZU UNTERHALTEN.
>
> Dr. Gerd Neugebauer, Senior IT-Architekt, Iteratec GmbH, www.iteratec.com

> „EINE TRENNUNG DES IT-TEAMS – WIE VON DER BIMODALEN IT GEFORDERT – WÜRDE AUCH DEN CHANGE-PROZESS MASSIV BEHINDERN."
>
> Fazit CapGemini-Studie



zahllosen Start-ups und großen Technologieunternehmen bewährt hat – und zwar für alle Arten der Softwareentwicklung, digitale und nicht-digitale gleichermaßen. Das liegt nicht nur daran, dass sich agile Methoden auch nahezu allen Branchen durchgesetzt haben. Und es liegt nicht nur daran, dass die heutigen Unternehmen bei der Implementierung von Agile auf ausgereifte Playbooks zurückgreifen können. Es liegt vor allem daran, dass die IT der zwei Geschwindigkeiten erhebliche Herausforderungen für Unternehmen schafft - oder schaffen wird -, die sie weiterhin einsetzen.

Das Ende der bimodalen IT

CapGemini kommt in seiner Studie „Agilität überall – Das Ende der bimodalen IT" im Fazit zum gleichen Ergebnis: Letztendlich seien zwei Technologiestrategien nicht praktikabel. Im Kern hänge die bimodale IT mit ihren zwei Geschwindigkeiten einem verfehlten technikzentrierten Modell an, das die Komplexität erhöht und die Backend-Systeme von den Geschäftsfunktionen isoliert. Forrester-Analysten sehen das ähnlich. In der Studie „The False Promise Of Bimodal IT" warnt Forrester vor einer „Zwei-Klassen IT". Wenn zwei unterschiedliche IT-Bereiche miteinander um Budget, Ressourcen, Skills und die Aufmerksamkeit des Business kämpften, sorge dies für Unruhe, eine erhöhte Komplexität und hohe Kosten, so die Forrester-Analysten.

Es komme zu Konflikten und Verwirrung, und vor allem könne es die Fähigkeit des Unternehmens, Kunden zu gewinnen, beeinträchtigen – ganz abgesehen davon, dass sich die klassische IT mit ihren Backend-Systemen zurückgesetzt und vernachlässigt fühle, da sie nicht direkt zum Wertschöpfungsprozess beitrage.

Im Endeffekt läuft die gesamte Kritik an der bimodalen IT darauf hinaus, dass auch die operativen IT-Systeme kontinuierlich organisatorisch re-engineert und an den Marktbedürfnissen ausgerichtet werden müssen. Entsprechend sollte die ganze IT agil umstrukturiert werden.

Was also tun? In der bereits 2017 durchgeführten Studie „Designing IT Setups in the Digital Age" des Beratungshauses A.T. Kearney und des Fraunhofer FIT (Institut für Angewandte Informationstechnik) sprechen sich die befragten Top-Manager mehrheitlich gegen eine bimodale IT aus. Stattdessen raten sie, das gesamte Unternehmen zu transformieren, nach dem DevOps-Prinzip zu arbeiten und cross-funktionale Teams zu bilden. Große IT-Dienstleister wie Capgemini unterstützen Unternehmen bei dieser Transformation. Sie verfügen über die erforderlichen Ressourcen und das Know-how, um Anwender bei diesem Transformationsprozess zu begleiten – und ihre IT fit zu machen für die Anforderungen des 21. Jahrhunderts.

Fazit

Zum einen haben neue Technologien wie die Cloud oder API-Management-Plattformen viele Überlegungen hinsichtlich Neuentwicklung, aber auch Updates, Pflege und Wartung von Anwendungen obsolet gemacht. Businessprozesse und die Notwendigkeit der Interoperabilität von Anwendungen tun ihr übriges.

Außerdem zwingen Rahmenbedingungen die Unternehmen heute die Situation anders zu bewerten. Außer von der Unternehmensgröße und Branche wird der Faktor Mensch bei den Überlegungen meist unberücksichtigt gelassen. Personalknappheit einerseits und fehlende Skills bei den Mitarbeitern können in zwei ähnlich positionierten Unternehmen die Entscheidung ganz anders ausfallen lassen. Und wie die Diskussion zeigt: Was heute richtig erscheint, kann morgen schon wieder ganz anders aussehen. „Panta rhei", grob übersetzt bedeutet das: Alles ist im Fluß! Und das trifft den Sachverhalt auf den Punkt.

Ulrich Parthier

Quellen:https://explore.iteratec.com/blog/erfolgsfaktoren-fuer-eine-two-speed-it
https://www.bcg.com/de-de/publications/2016/software-agile-digital-transformation-end-of-two-speed-it
https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2018/07/Capgemini_WP1-bimodaleIT.pdf

CLOUD-NATIVE COMPUTING

SOFTWARE ENGINEERING VON DIENSTEN UND APPLIKATIONEN FÜR DIE CLOUD

Cloud-native Computing – Software Engineering von Diensten und Applikationen in die Cloud; Nane Kratzke, Carl Hanser Verlag GmbH & Co. KG, 12-2021

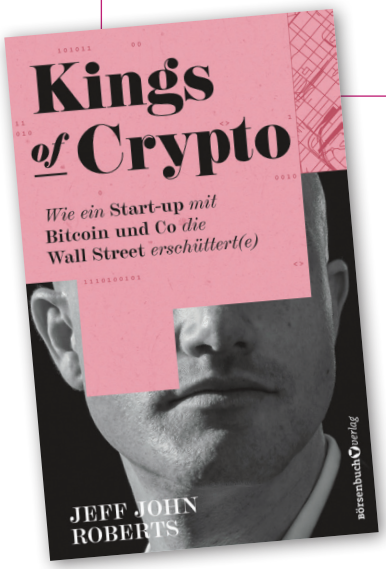
Märkte verändern sich immer schneller, Kundenwünsche stehen im Mittelpunkt – viele Unternehmen sehen sich Herausforderungen gegenüber, die nur digital beherrschbar sind. Um diese Anforderungen zu bewältigen, bietet sich der Einsatz von Cloud-native-Technologien an. Dabei reicht es jedoch nicht aus, einen Account bei einem Cloud-Anbieter anzulegen. Es geht auch darum, die unterschiedlichen Faktoren zu verstehen, die den Erfolg von Cloud-native-Projekten beeinflussen.

Das Buch beleuchtet den Cloud-native-Wandel aus unterschiedlichen Perspektiven: von der Unternehmenskultur, der Cloud-Ökonomie und der Einbeziehung der Kunden (Co-Creation) über das Projektmanagement (Agilität) und die Softwarearchitektur bis hin zu Qualitätssicherung (Continuous Delivery) und Betrieb (DevOps). Anhand von realen Praxisbeispielen wird gezeigt, was bei der Umsetzung in unterschiedlichen Branchen gut und was schlecht gelaufen ist und welche Best Practices sich daraus ableiten lassen. Dabei wird auch die Migration von Legacy-Code berücksichtigt.

IT-Architekten vermittelt dieses Buch zudem das grundlegende Wissen, um Cloud-native-Technologien und die DevOps-Kultur in ihrem Projekt oder im gesamten Unternehmen einzuführen.

KINGS OF CRYPTO

WIE EIN START-UP MIT BITCOIN UND CO DIE WALL STREET ERSCHÜTTERT(E)



Im Krypto-Universum spielen sich Dramen darüber ab, welche Kryptowährung sich gegenüber anderen durchsetzt. „Kings of Crypto" taucht tief in diese Dramen ein: Star-Kryptojournalist Jeff John Roberts verfolgt den Aufstieg, den Fall und die Wiedergeburt von Kryptowährungen anhand der Erfahrungen der wichtigsten Akteure weltweit.

Im Mittelpunkt seines Buches stehen die Story des Silicon-Valley-Unternehmers Brian Armstrong und der turbulente Höhenflug seines Start-ups Coinbase, das heute die führende US-Kryptowährungsbörse ist. Scharfsinnig beobachtet und brillant recherchiert enthüllt Roberts diese Erfolgsgeschichte – von der einfachen Bude zum Milliardengeschäft. Dabei vermittelt er die ganze Faszination, aber auch die Abgründe der Kryptowelt.

Kings of Crypto – Wie ein Start-up mit Bitcoin und Co die Wall Strett erschüttert(e); Jeff Jjohn Roberts, Kulmbach Verlag, 02-2022

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
02. MAI 2022

MANAGED SERVICES: Den Dienstleister wechseln?
INDUSTRIAL IOT: Bessere Entscheidungsfindung
DIGITALISIERUNG: Mehr als nur IT

DIE AUSGABE 04/2022
VON IT MANAGEMENT
ERSCHEINT AM 31. MÄRZ 2022

INSERENTENVERZEICHNIS

it management

Snom (Teaser)	U1
it Verlag GmbH	U2, U4
ams.Solution AG	3
DSAG	7
operational services	15
Messe Berlin	29
E3 Magazin / B4B Media	U3

it security

it Verlag GmbH	U2, U4
HiScout GmbH	3
DriveLock SE (Thought Leadership)	8

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

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Carina Mitzschke, Silvia Parthier (-26)

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Daniela Matysiak, Carina Mitzschke, Dr. Gerd Neugebauer, Silvia Parthier, Ulrich Parthier, Michael Steinberg, Stephan Vanberg, Sven-Ove Wähling, Thorsten Winternheimer

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. 29. Preisliste gültig ab 1. Oktober 2021.

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

Digitale Transformation:
Wie ECM und DMS dabei helfen

15. März 2022 | *Digitalevent*

Daten sind das neue Öl aber Informationen sind das neue Gold.
Es steckt in **E**nterprise **C**ontent **M**anagement Systemen und wartet darauf, seinen Beitrag zur Digitalen Transformation zu leisten. Die Referenten informieren Sie praxisnah und kompakt.
Besuchen Sie unser kostenloses Event und profitieren Sie von deren Erfahrung.

Highlights aus der Agenda

Keynote

Mythen und Irrglauben zu GoBD, DSGVO und Co.
Berhard Zöller, Geschäftsführer, Zöller & Partner GmbH

Information Governance/Information Management.
Dr. Ulrich Kampffmeyer, Geschäftsführer,
PROJECT CONSULT Unternehmensberatung Dr. Ulrich Kampffmeyer GmbH

Collaboration/New Work/Digital Workplace

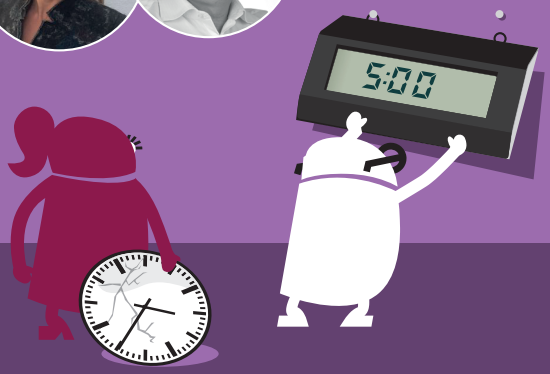
Willkommen in der Content Cloud
Michael Mors, General Manager Central Europe, Box Inc.

Informationsmanagement-Plattformen müssen intelligent sein
Joachim Bleicher, Sales Engineer DACH, M-Files

Diskussionsrunde

Digitale Transformation:
Was sind aktuell die größten Hürden und wie kann die ECM-Technologie bei der Realisierung helfen?
Annette Stadler, Chefredakteurin, ecmguide.de
Ulrich Parthier, Herausgeber it management, IT Verlag GmbH

SCAN ME



Jetzt anmelden

https://www.it-daily.net/ecm/anmeldung/

#ecmDigital22

itsecurity
MÄRZ 2022

DAS SPEZIAL

IT-SICHERHEITSSTRATEGIEN

DIE SUPPLY CHAIN IN DER RISIKO-BETRACHTUNG

Steffen Ullrich, genua GmbH

INNOVATIONEN & THOUGHT LEADERSHIP
THOUGHT LEADERSHIP

ALLES EINE FRAGE DER SICHTWEISE
AB **SEITE 09**

DriveLock

SYNTHETISCHE IDENTITÄTEN

Die neue Gefahr

DATA LOSS PREVENTION

Gut für den Mittelstand

IT-SIG 2.0 UND S/4HANA

Anforderungen erfüllen

INHALT

COVERSTORY

4 **IT-Sicherheitsstrategien für digitale Infrastrukturen**
Die Supply Chain muss stärker in die Risikobetrachtung einbezogen werden

THOUGHT LEADERSHIP

9 **Thought Leadership**
Alles eine Frage der Sichtweise

IT SECURITY

12 **KRITIS: IT-SIG 2.0 bei S/4HANA mitdenken**
Wie man die Anforderungen des neuen Sicherheitsgesetzes erfüllt

14 **BCM – der Berg ruft**
Was Sie von einer Bergtour über BCM lernen können

15 **Angriff aus der Cloud**
Mit SaaS steigen auch die Risiken

16 **Synthetische Identitäten: Die neue Gefahr**
Aber wie erkenne ich sie rechtzeitig?

18 **Cybersecurity im Energiesektor**
Flexibel und nachhaltig – aber auch sicher?

20 **MHP und LKA BW: Cyber-Security-Risk-Report 2021**
Nachholbedarf bei Risikobewertung und reaktiver Vorfallsbehandlung

22 **Data Loss Prevention**
Ein gutes Mittel für den Mittelstand

IT-SICHERHEITSSTRATEGIEN FÜR DIGITALE INFRASTRUKTUREN

„DIE SUPPLY CHAIN MUSS STÄRKER IN DIE RISIKOBETRACHTUNG EINBEZOGEN WERDEN"

Meldungen über Sicherheitslücken in der IT gehören zum täglichen Brot von Mitarbeitern in den IT-Security-Abteilungen in Unternehmen wie Behörden. Was tun? Steffen Ullrich ist Sicherheitsforscher beim deutschen IT-Security-Hersteller genua. Im Interview mit it security-Herausgeber Ulrich Parthier äußert er sich zum Dilemma und zeigt Lösungsansätze auf.

Ulrich Parthier: *Solarwinds, Proxylogon, Log4Shell, 2021 war erneut äußerst herausfordernd für IT-Verantwortliche. Wie bewerten Sie das vergangene Jahr?*

Steffen Ullrich: Es war ein unruhiges Jahr, in welchem wir erleben mussten, wie fragil und anfällig geschäftskritische Infrastrukturen gegen Cyber-Angriffe über vertrauensvoll eingesetzte Fremdsoftware sind. Bei Solarwinds handelte es sich um eine Backdoor in kritischen Netzkomponenten, die durch einen staatlichen Angreifer platziert wurde. Proxylogon war eine Lücke in der kommerziellen Software MS Exchange, Log4Shell eine Schwachstelle in einer von vielen, auch kommerziellen, Projekten eingesetzten Open-Source-Bibliothek. Alle diese Lücken ermöglichten einem Angreifer die Kompromittierung der internen Firmeninfrastruktur.

Ulrich Parthier: *Wie schätzen Sie als IT-Sicherheitsforscher perspektivisch die weitere Risikoentwicklung ein?*

Steffen Ullrich: Die Probleme werden noch deutlich wachsen, sowohl von der Menge als auch der Kritikalität. Mit der zunehmenden Digitalisierung von Geschäftsprozessen geht eine starke Erhöhung von Komplexität einher: vielfältigere Software, Dienste und Hardware mit mehr Features, stärker vernetzt über Standorte, Clouds und Home Office hinweg. Dies bewirkt eine abnehmende Kontrolle und Beherrschbarkeit der Infrastrukturen und entsprechend steigende Fragilität. Gleichzeitig wachsen die Abhängigkeiten von einer korrekten Funktion digitalisierter Geschäftsprozesse und die Anforderungen an Verfügbarkeit, Zuverlässigkeit und Datensicherheit.

Ulrich Parthier: *Ein zunehmendes Problem sind Supply-Chain-Angriffe. Woran liegt das?*

Steffen Ullrich: Der größte Teil der heutigen Infrastrukturen beinhaltet Komponenten aus einer Vielfalt von Quellen. Bei Software sind es teilweise Open-Source- und teilweise Closed- Source-Komponenten, die selber wiederum aus weiteren Komponenten aufgebaut sind. Das Netz an Abhängigkeiten ist oft unüberschaubar, komplex und fragil. Die Qualität der einzelnen Komponenten ist sehr unterschiedlich und man muss von bestehenden Sicherheitslücken ausgehen, die evtl. auch schon von Angreifern ausgenutzt werden. Ein einfaches Patchen bei erkannten Lücken ist nicht möglich, weil gepatchte Versionen von Komponenten sich nicht unbedingt genauso verhalten wie die vorherigen Versionen. Wenn es denn überhaupt Patches gibt, weil oftmals tief im Inneren Komponenten stecken, die schon lange nicht mehr gepflegt werden. Und das ist nur die Problematik der Bugs. Daneben gibt es durchaus auch gezielt eingebaute und gut versteckte Backdoors. Auch hier werden die Probleme nur größer.

Ulrich Parthier: *Wie können IT-Verantwortliche mit dieser Unsicherheit umgehen?*

> DER WERT VON SICHERHEIT ALS BEWAHRER DER PRODUKTIVITÄT WIRD OFT ERST DANN KLAR, WENN MAN DIREKT VON EINEM CYBER-ANGRIFF BETROFFEN IST.
>
> Steffen Ullrich, Sicherheitsforscher, genua GmbH, www.genua.de

Steffen Ullrich: Man sollte davon ausgehen, dass eine eingesetzte Software unsicher ist und die damit zusammenhängenden Risiken minimieren, zum Beispiel durch eine Beschränkung der Kommunikation. Auch eine solide Segmentierung und Mikrosegmentierung schränkt die Bewegungsfreiheit eines Angreifers im Netzwerk deutlich ein und reduziert dessen Ausbreitung sowie die verursachten Schäden. Grundsätzlich muss die Supply Chain insgesamt stärker in die Risikobetrachtung einbezogen werden. Das bedeutet, es sollten potenzielle Schäden betrachtet und Mitigationsmaßnahmen zur Schadensbegrenzung entwickelt werden.

Ulrich Parthier: *Und mit Blick auf die Komponentenauswahl?*

Steffen Ullrich: Es ist grundsätzlich wichtig, bei der Auswahl der eingesetzten Komponenten hohe Sorgfalt walten zu lassen. Das betrifft die Fremdsoftware oder gemanagte Infrastruktur der IT genauso wie die Softwarekomponenten bei der Entwicklung. Hier hilft es nicht, nur auf den jeweiligen Hersteller zu vertrauen, sondern auf unabhängige Sicherheitsuntersuchungen zu achten, zum Beispiel im Rahmen von Zertifizierungen, Zulassungen oder Penetrationstests. Fundierte, unabhängige Beurteilungen und Analysen können das Vertrauen in IT-Security-Lösungen signifikant stärken. Sie erhöhen auch den Druck auf Zulieferer bezüglich Qualität, Zuverlässigkeit und Sicherheit, sowohl mit Blick auf Produkte und Dienstleistungen als auch auf interne Arbeitsprozesse und Infrastrukturen.

Ulrich Parthier: *Mitarbeiter in IT-Abteilungen scheinen Getriebene der Cyber-Kriminellen zu sein. Was hindert uns daran, mehr proaktiven Schutz zu erreichen? Haben wir zu viele „IT-Verwalter" anstelle von Strategen und Visionären?*

Steffen Ullrich: IT-Sicherheit und Datenschutz kosten erst einmal nur Zeit und Geld, für die es keinen spürbaren Gegenwert gibt. Im Gegenteil: Ein mehr an Sicherheit wird oft hinderlich bei der Arbeit oder als Verlangsamung von Prozessen empfunden. Entsprechend werden oft nur die Minimalanforderungen erfüllt, die die Compliance erfordert. In diesem Umfeld können sich Strategen und Visionäre kaum entfalten. Der Wert von Sicherheit als Bewahrer der Produktivität wird oft erst dann klar, wenn man direkt von einem Cyber-Angriff betroffen ist. Dies steigert dann allerdings die Akzeptanz für Visionen und Strategien, die einen solideren, proaktiven Umgang mit dem Problem bieten.

Ulrich Parthier: *Was ist aus Ihrer Sicht der richtige Weg, um aus einer primär reaktiven, getriebenen Rolle zurück in eine gestaltende, kontrollierende Rolle zu gelangen?*

Steffen Ullrich: Eine proaktive Absicherung des Netzes bedeutet, die Kommunikation auf das Erwartete zu beschränken, statt, wie oft der Fall, beliebige Kommunikation innerhalb eines Netzes zu erlauben. Je präziser und granularer die Restriktionen sind, desto schwieriger ist es für einen Angreifer, in die Infrastruktur einzudringen beziehungsweise sich dort auszubreiten. Die Restriktionen können durch eine Positionierung von Zugriffskontrollen an neuralgischen Stellen im Netz erfolgen, sei es direkt vor einem abzusichernden Dienst, vor einem sensitiven Netzbereich oder vor einer besonders anfälligen Maschine. Die Umsetzung ist schrittweise möglich, zum Beispiel für besonders sensitive Dienste zuerst oder erst grobgranular und dann schrittweise verfeinernd.

Ulrich Parthier: *Wir müssen ja unterscheiden zwischen strategischem und operativem Handeln. Das Thema proaktives Handeln zählt zum strategischen Teil. Dort wird im Rahmen einer IT-Sicherheitsstrategie gerade das Thema „Zero Trust" hoch gehandelt. Wie kann Zero Trust für mehr Schutz sorgen?*

Steffen Ullrich: Der Begriff ist tatsächlich schon mehr als zehn Jahre alt, gewinnt aber zunehmend an Relevanz. Der

Grundidee liegt ein Perspektivwechsel zugrunde: Statt zu versuchen, ein komplettes Netz abzusichern, konzentriert man sich auf die Absicherung der Endpunkte einer Kommunikation sowie des Datentransfers dazwischen. Konkret bedeutet das eine auf Applikationen fokussierte Zugriffskontrolle, bei der die Zugriffsentscheidung basierend auf den Sicherheitseigenschaften des zugreifenden Clients und den Sicherheitsanforderungen des Dienstes basiert. Jeder Dienstzugriff kann so eigenständig behandelt werden, unabhängig von der Sicherheit des darunterliegenden Netzes. Das bedeutet nicht, dass Netzsicherheit irrelevant wird. Im Sinne einer Defense in Depth ist es sinnvoll, sich nicht alleinig auf die Funktionsfähigkeit einer einzelnen Komponente zu verlassen.

> JE EINFACHER ES WIRD, EINE MÖGLICHST GRANULARE, PROAKTIVE SICHERHEIT ZU BEKOMMEN UND BEIZUBEHALTEN, DESTO WIRKSAMER KÖNNEN WIR ANGREIFER ABWEHREN.
>
> Steffen Ullrich, Sicherheitsforscher, genua GmbH, www.genua.de

? Ulrich Parthier: *Werfen wir noch einen Blick auf die operativen Probleme. Sie manifestieren sich in Angriffsvektoren wie log4j2, Proxylogon, Solarwinds, IaaS (Cloud), AI als Blackbox. Helfen hier Ansätze wie Konsolidierungen, Zertifizierungen oder eine Reduktion von Features, um die Angriffsfläche zu verringern?*

Steffen Ullrich: Viele Features und eine hohe Flexibilität erhöhen die Komplexität und vergrößern die potentielle Angriffsfläche. Eine Reduktion auf das tatsächlich Benötigte erhöht die Beherrschbarkeit aber auch die inhärente Sicherheit von Software. Je weniger Features oder Feature-Kombination existieren, desto verständlicher ist das Design und desto einfacher kann umfassend getestet werden. Zertifizierungen tragen neben der unabhängigen Überprüfung durch Dritte auch zu einem verständlichen, sicheren und robusten Design bei, weil dies auch eine Zertifizierung vereinfacht. Konsolidierungen hingegen sind zwiespältig: Zum einen können sie helfen, die vorhandene Sicherheits-Expertise und -Technologie besser zu konzentrieren. Zum anderen entsteht ein höchst lukratives Ziel für Angreifer, das entsprechend mit signifikant mehr Aufwand geschützt werden muss.

? Ulrich Parthier: *Sie arbeiten seit 2001 bei der genua GmbH als Softwareentwickler und Sicherheitsforscher. Wo sehen Sie aktuell die interessantesten Forschungsansätze um die IT sicherer zu machen?*

Steffen Ullrich: Cyber-Sicherheit ist ein riesiges Feld mit vielen wichtigen Problemen. Ich sehe enorm viel Potenzial in der Nutzung von Künstlicher Intelligenz als Unterstützung für die Verteidiger, aber leider auch als Hilfe für den Angreifer. Wir haben in der IT seit Langem einen Wettlauf zwischen den Fähigkeiten von Abwehr und Angriff. Dieser wird sich durch KI eher noch beschleunigen. Wichtig finde ich es daher, KI zu nutzen, um komplexe Infrastrukturen besser zu beherrschen und proaktiv abzusichern, statt einfach nur auf Angriffe zu reagieren. Im BMBF-geförderten Forschungsprojekt Wintermute gehen wir genau diesen Möglichkeiten nach, und zwar der Frage, wie KI den IT-Administrator bei der Lagebeurteilung, Definition und Durchsetzung von Sicherheits-Policies in komplexen Netzen unterstützen kann. Ebenfalls mit besserer Beherrschbarkeit beschäftigen sich Forschungen im Bereich der User Experience und Usability sowie zum Management komplexer Informationssysteme. Je einfacher es wird, eine möglichst granulare, proaktive Sicherheit zu bekommen und beizubehalten, desto wirksamer können wir Angreifer abwehren.

Weiter Forschungsthemen betreffen zum Beispiel die Gefahr durch unsichere Prozessoren, die vergleichsweise schwache Trennung von Mandanten in Cloud-Umgebungen und die neuen Herausforderungen durch Quantencomputer. Hierfür untersuchen wir neuartige quantenresistente Algorithmen sowie ihre Umsetzung in VPN-Standards und Implementierungen. Das ist Gegenstand des Forschungsprojekts QuaSiModO, in dem wir als Verbundkoordinator agieren. Die Erkenntnisse aus unseren Forschungsprojekten fließen im Übrigen bereits in unsere Produktentwicklung ein, unter anderem in Form von quantenresistenten Signaturen für unsere VPN-Lösungen oder intelligente Machine-Learning-Algorithmen für unseren cognitix Threat Defender.

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

LIVE WEBINAR
AM 10.03.2022
UM 10:00 UHR

SENSIBLE DATEN

DER AUSTAUSCH MUSS NICHT SCHWIERIG SEIN

Björn Röckle, FTAPI Branchenexperte für Fertigung, Dienstleistung, Handel, Steuern & Recht, FTAPI Software GmbH

Für viele Unternehmen ist es nach wie vor eine Herausforderung große oder sensible Daten einfach und zugleich sicher sowie datenschutzkonform mit externen Empfängern auszutauschen. Viel zu oft versenden Mitarbeiter Dateien ungeschützt per E-Mail oder nutzen unsichere File-Sharing-Lösungen.

Doch dabei schwingt ein gewisses Risiko mit. Erfahren Sie, wie Unternehmen einfach und komfortabel ihre wichtigen Daten sicher austauschen können.

Was Sie im Webinar erwartet:

- Erleben Sie durchgängige Ende-zu-Ende-Verschlüsselung ohne komplizierte Zertifikate
- Es entsteht keinerlei administrativer Aufwand für die Nutzer beziehungsweise Ihr Unternehmen
- Kein Medienbruch: nachtlose Outlook-Integration

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

LIVE WEBINAR
30.03.2022
10:00 UHR

BACKUP-AS-A-SERVICE

DATENSICHERHEIT FÜR DIE CLOUD-ÄRA

Was sind die wichtigsten Überlegungen bei der Evaluierung einer Cloud-Datensicherungslösung?

Um sicherzustellen, dass sie die benötigten Dienste zum richtigen Zeitpunkt erbringt, sind zwei zentrale Eigenschaften eines modernen Cloud-Dienstes entscheiden:

- Das System arbeitet konsistent und ausfallsicher
- Ihre Geschäftsprozesse werden nicht unterbrochen

Druva bietet einen SaaS-basierten Ansatz, um Backup-Daten, Rechenzentrums-, Cloud- und Endpoint-Workloads zu schützen und zu verwalten. Datenausfallsicherheit wird über eine einzige Plattform gewährleistet, die mehrere Regionen und Clouds abdeckt: 0 Prozent Infrastruktur, 100 Prozent Cloud. Die Vorteile: Datensicherheit wird vereinfacht, Datenverwaltung rationalisiert, Kosten und Komplexität reduziert. Durch die Nutzung der Lösung als DextraData as-a-Service-Angebot verringern Sie zudem Aufwand und Stress.

Michael Hensche, Principal Architect, DextraData GmbH

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

DIE ZUKUNFT IM BLICK

WAS VERBINDET LEADERSHIP UND INNOVATIONEN? BEIDE BEGRIFFE STEHEN UNTRENNBAR ZUSAMMEN. WENN WIR EINEN BLICK AUF DEN BEREICH IT SECURITY WERFEN, STELLT SICH DIE FRAGE: WAS WIRD IN ZUKUNFT PASSIEREN?

THOUGHT LEADERSHIP

ALLES EINE FRAGE DER SICHTWEISE

Was zeichnet einen Thought Leader im IT Security-Bereich? In welche Richtung entwickelt sich die IT Sicherheit? Über diese und weitere Punkte sprach it security-Herausgeber Ulrich Parthier mit Udo Riedel, CTO und Gründer der DriveLock SE.

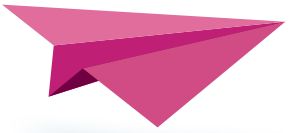
? **Ulrich Parthier:** *Als CTO sind Sie bei DriveLock verantwortlich für Forschung und Entwicklung, Qualitätsmanagement und die Programmierung. Das bedeutet, Ihr Fokus liegt auf der technischen Entwicklung von DriveLock und der Implementierung neuer Technologien in die Software. Was verbindet Sie mit dem Thema Thought Leadership, einem ja eher strategischen Managementthema?*

Udo Riedel: Als CTO ist die Produktstrategie genau mein Thema. Denn als Unternehmen ist es unser Ziel, ein Meinungsführer im IT Security Markt zu sein, während wir den Markt analysieren und zukunftsorientierte Lösungen entwickeln. Der CTO entwickelt die Strategie und bestimmt auch die Außendarstellung in dieser Hinsicht.

? **Ulrich Parthier:** *Wie würden Sie den Thought Leadership-Begriff definieren und welche Sichtweise eignet sich am besten?*

Udo Riedel: Es geht ums Vordenken und Verstehen der Gegenseite. Beim Katz-und-Maus Spiel mit Hackern und Cyberkriminellen schadet es auch nicht – ich sage das jetzt mit einem zwinkernden Auge – selbst eine gesunde kriminelle Energie zu haben. Natürlich ohne diese einzusetzen! So kann man sich in die Gegenseite hineinversetzen und mögliche kriminelle Vorgehensweisen antizipieren. Wir bemühen uns, den Hackern stets einen Schritt voraus zu sein. Wenn wir aus der Vogelperspektive das Gesamtbild betrachten, können wir unser Wissen auch mit unseren Kunden und Partnern teilen.

? **Ulrich Parthier:** *Egal ob Cyberangriffe von außen oder versteckte An-*



griffe von innen, der Mensch ist immer das schwächste Glied in der Kette. Was empfehlen Sie an proaktiven Maßnahmen?

Udo Riedel: Letztendlich sind ungefähr 70 Prozent des Datenverlusts menschlichem Fehlversagen geschuldet – das kann der verlorene USB-Stick sein, oder ein Gerät, das mit dem ungesicherten Heimnetzwerk verbunden wurde. Ein Großteil der Sicherheitsindustrie konzentriert sich aber nur darauf, irgendwelche Angriffe abzuwehren. Deshalb ist „Security Awareness" für uns so ein wichtiges Thema, denn die Beschäftigten müssen fundiert ausgebildet werden. Am besten geeignet sind kurze Schulungsmaßnahmen zum richtigen Zeitpunkt, bei denen die Gefahr visualisiert wird – beispielsweise, wenn ein unbekannter USB-Stick an das Notebook angeschlossen wird. Auf diese Weise findet eine Sensibilisierung für potenzielle Gefahren exakt im kritischen Moment statt und die Mitarbeiter prüfen Gefahrenquellen künftig mit geschulterem Auge.

Ulrich Parthier: *Wie führt man am besten Veränderungsprozesse ein?*

Udo Riedel: Das Thema „Human Performance" wird in einigen Unternehmen nicht kritisch genug betrachtet, um zu einer effektiven Security-Strategie beizutragen. Deshalb ist eine externe Beratung aus anderer Perspektive auf jeden Fall ratsam. Ein Berater kann gegebenenfalls Fehlverhalten oder Lücken in der IT-Sicherheit aufzeigen und entsprechende Tools direkt anbieten. Ein guter Startpunkt ist immer das Coaching, später kommen dann die technischen Maßnahmen dazu.

Ulrich Parthier: *Zum Change gehören Coaching, Sensibilisierung sowie Fehlerkultur und wie man mit diesen umgeht. Welche Maßnahmen haben sich hier bewährt?*

Udo Riedel: Für mich ist Fehlerkultur einer der wichtigsten Begriffe, der oft falsch angegangen wird. Ich bekomme das aktuell bei meiner Tochter mit. Sie bekommt in der Schule beigebracht, wie wichtig es ist, immer einen Schuldigen herauszufinden. Dabei ist das überhaupt nicht wichtig. Fehler passieren – da können wir nichts dagegen tun. Bei uns im Unternehmen sagen wir: Jeder Mensch darf Fehler machen, aber jeden Fehler nur einmal. Schuldzuweisungen sind hier fehl am Platz. Stattdessen versuchen wir herauszufinden, warum der Fehler passiert ist und wie wir ihn beim nächsten Mal vermeiden können.

Was technische Maßnahmen angeht, orientieren wir uns am Swiss Cheese Modell. Jedes System hat irgendwo ein Loch, durch welches ein Angreifer schlüpfen könnte. Je mehr Scheiben Sie übereinanderlegen, desto unwahrscheinlicher ist es, dass diese Löcher sich überlappen.

Ulrich Parthier: *Sie sind ein passionierter Hobby-Pilot. Was haben die Fliegerei und Ihre Erfahrungen zum Thema „Vermeiden von menschlichen Fehlern" gemeinsam?*

Udo Riedel: In der Luftfahrt ist Fehlermanagement seit jeher ein äußerst wichtiges Thema und einige der Stichworte aus dem Bereich Human Performance, die ich vorhin bereits genannt hatte, kommen ursprünglich aus der Berufsfliegerei. Zum Beispiel Fehlerkultur: Autoritätsgefälle sind aus menschlicher Sicht verständlich und typisch, aber auch erfahrene Piloten machen Fehler. Deshalb wurde das Cockpit-Team im Flugzeug auch umbenannt und man spricht nicht mehr von einem Piloten und einem Co-Piloten, sondern von Pilot Flying und Pilot Monitoring. Per Definition sind beide auf eine Ebene gestellt und der Pilot Monitoring kann Fehler ansprechen, die der Pilot Flying macht. Dieses Schema wird mittlerweile auch in anderen Bereichen umgesetzt. Ein besonders prominentes Beispiel ist die Medizin: Ich erinnere mich, eine Statistik gesehen zu haben, laut der 50 Prozent aller Komplikationen nach chirurgischen Eingriffen aufgrund menschlichen Versagens des Arztes herrühren. Die Assistenten trauen es sich möglicherweise gar nicht zu sagen, wenn der Doktor ein Tuch mit einnäht oder einen offensichtlichen Fehler macht. Er sollte es besser wissen, denn er ist ja immerhin Arzt. Nur mit viel Schulung können wir eine gute Fehlerkultur schaffen, in der es nicht

BEIM KATZ-UND-MAUS SPIEL MIT HACKERN UND CYBERKRIMINELLEN SCHADET ES AUCH NICHT SELBST EINE GESUNDE KRIMINELLE ENERGIE ZU HABEN. NATÜRLICH OHNE DIESE EINZUSETZEN!

Udo Riedel, CTO und Gründer, DriveLock SE, www.drivelock.de

verpönt ist, Fragen zu stellen und Fehler anzusprechen.

Technologie – insbesondere das Vertrauen in diese – spielt auch in beiden Bereichen eine wichtige Rolle. In der Fliegerei nennen wir das „Trust your instruments", zum Beispiel wenn eine Wolke gerade das gesamte Blickfeld beeinträchtigt. Auch in der Cybersecurity verlassen wir uns auf unsere Technologien, die uns vor dem Unbekannten zu schützen.

Ulrich Parthier: *Zurück zum Thema Leadership. Was verbindet Leadership und Innovationen?*

Udo Riedel: Für mich gehören die beiden Begriffe untrennbar zusammen. Wenn ich ein Leader sein möchte, dann muss ich innovativ und immer auf dem neuesten Stand sein. Ansonsten steht der „Leader" am Ende irgendwo weit hinten in der Schlange und führt gar nichts an.

Ulrich Parthier: *Wenn wir einen Blick auf den Bereich IT-Security werfen. Was zeichnet einen Thought Leader hier aus?*

Udo Riedel: Nach vorne blicken und sich fragen: Was wird in Zukunft passieren? Wir beobachten aktuell eine zunehmende Industrialisierung der Gegenseite und das dürfen wir als Anbieter von IT Security nicht ignorieren. Wir reden bei der Malware-Industrie mittlerweile von einem Milliardenmarkt, in den Unmengen an Ressourcen investiert werden. Da reichen die Antivirus Software und die Firewall, die 20 Jahre lang gewiss gute Dienste erwiesen haben, einfach irgendwann nicht mehr aus.

Ulrich Parthier: *Wie würden Sie Drivelock hier sehen?*

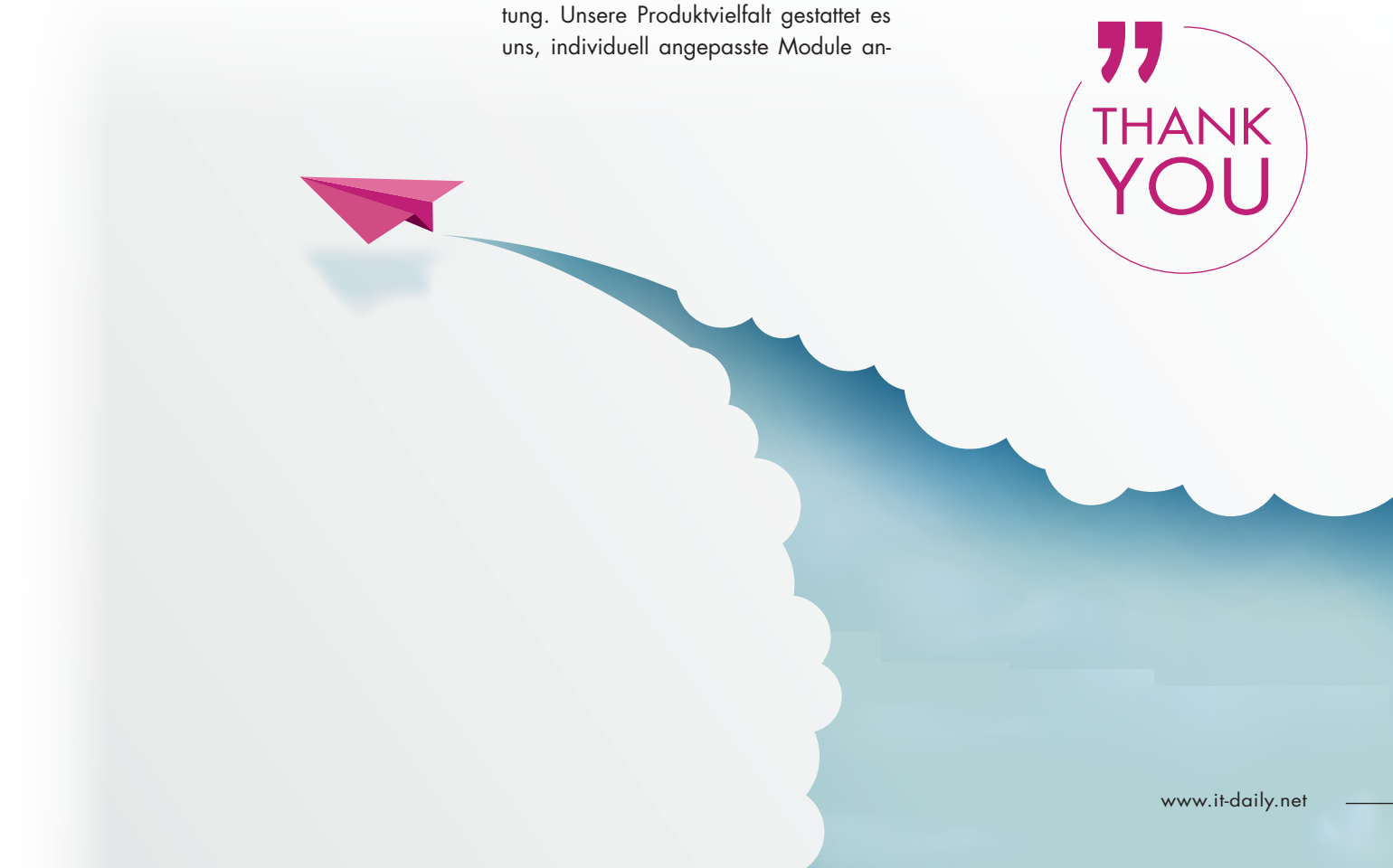
Udo Riedel: Wir sehen das Thema Security ein bisschen anders als die meisten Hersteller, denn uns geht es nicht nur darum, Angriffe abzuwehren. Wir wollen den gesamten Life Cycle von Daten schützen – von der Entstehung bis zur Vernichtung. Unsere Produktvielfalt gestattet es uns, individuell angepasste Module anzubieten, bei denen sich die „Käsescheiben" überlappen, sodass keine Löcher übrigbleiben.

Außerdem steht das Thema Human Performance bei uns im Fokus, wie bereits erwähnt.

Ulrich Parthier: *Letzte Frage - in welche Richtung entwickelt sich die IT-Sicherheit?*

Udo Riedel: Eine große Rolle wird die Sensibilisierung der Menschen spielen. Je besser die Menschen Schadsoftware erkennen, desto weniger effektiv ist diese. Aus technologischer Sicht nähern wir uns immer mehr dem Schweizer Käse Modell an. Die Professionalisierung der Malware-Industrie bedeutet, dass Unternehmen ihre Cybersecurity-Strategie überdenken müssen und andere beziehungsweise mehr Produkte einsetzen werden als bisher.

Ulrich Parthier: Herr Riedel, wir danken Ihnen für das Gespräch!



KRITIS: IT-SIG 2.0 BEI S/4HANA MITDENKEN

WIE MAN DIE ANFORDERUNGEN DES NEUEN SICHERHEITSGESETZES BEIM UMSTIEG AUF S/4HANA ERFÜLLT

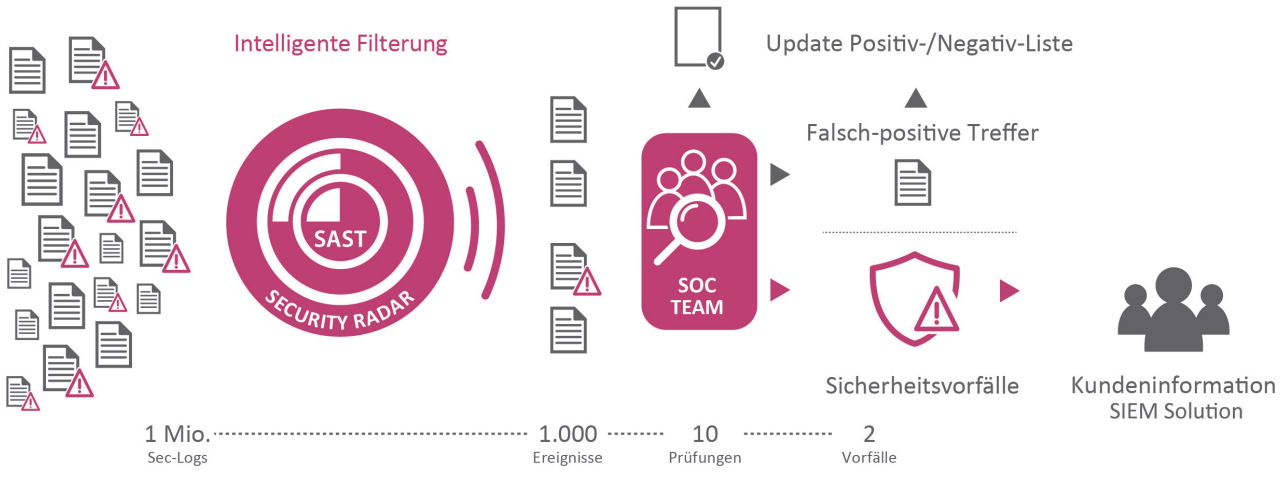
Der renommierte AXA Future Risks Report 2021 nennt als zweitwichtigste globale Bedrohung nach dem Klimawandel und noch vor Pandemien und Infektionskrankheiten die wachsenden Risiken durch Cyber-Attacken. Tatsächlich haben diese laut aktuellem BKA-Lagebericht erheblich zugenommen, sind professioneller geworden und konzentrieren sich oft auf kritische Infrastrukturen (KRITIS). Nicht zuletzt dieser Bedrohungslage begegnet das neue IT-Sicherheitsgesetz. Ralf Kempf, CTO des SAP-Security-Spezialisten SAST SOLUTIONS, erläutert die Herausforderungen für ein erfolgreiches S/4HANA-Projekt unter den Gesichtspunkten des SiG 2.0.

Für SAP S/4HANA haben sich gerade hinsichtlich SiG 2.0 die Sicherheitsanforderungen an KRITIS-Betreiber verändert, Datenbank, User Interface, Gateway, Applikationen und Berechtigungen sind enger zusammengewachsen, der Zugriff auf wichtige Daten ist komplexer geworden – und somit auch schwieriger zu überwachen. Das Sicherheitsgesetz fordert von allen KRITIS-Unternehmen ein detailliertes Business Continuity Planning und Desaster-Recovery-Szenarien, prozessuale, direktive und reaktive Maßnahmen, um schon im Vorfeld die Härtung der Systeme so durchzuführen, wie sie Marktstandard ist. Dabei gilt es, konkrete Vorgaben einzuhalten, wie man KRITIS-Architekturen baut, denn es ist stets zu beachten, dass man Infrastruktur und Prozesse so definiert, dass sie später im Rahmen einer SiG-Abnahme auch prüffähig sind und abgenommen werden. Diese Qualität der Architektur und Prozesse muss zyklisch nachgewiesen werden und setzt ein Umdenken voraus: Man kann nicht einfach weiterverfolgen, was man schon immer auf seine Weise getan hat, sondern muss konkrete Vorgaben erfüllen.

SiG-2.0-Aspekte bereits in Frühphase bedenken

Noch wichtiger als zuvor ist bei Migrationsprojekten daher eine Security-Betrachtung und ganzheitliche Strategie, die alle Themen und Anforderungen vereint. Bezüglich SAP ist der vorgeschriebene Einsatz von Anomalie- und Intrusion-Detection-Systemen (IDS) nach dem „neuesten Stand der Technik" dabei nicht ausreichend: IDS erkennen und konkretisieren Angriffe mithilfe auszuwertender

SAP CYBERSECURITY MONITORING IN ECHTZEIT



Log-Dateien, wobei SAP als weitgehend eigenständiges System oft durch das Erkennungsraster fällt, wenn nicht zusätzlich die Expertise von SAP-Sicherheitsprofis und spezielle Software wie die SAST SUITE zum Einsatz kommen. Diese stellt entsprechende SAP-SIEM-Monitoring-Komponenten bereit und das integrierte Dashboard ermöglicht Transparenz über alle Systeme. Essenziell ist hier also die Einbindung eines SAP-Security-Spezialisten, eine Erkenntnis, die auch für Non-KRITIS-Unternehmen mit hohem Schutzbedarf gilt.

S/4HANA und SiG 2.0 als Chance nutzen

Wie aber gewährleisten Betreiber bei der S/4HANA-Migration das Zusammenspiel zwischen Konzeption und Management ebenso wie zwischen Überwachung, Verwaltung und Auditing? Die Einbettung eines integrierten Sicherheits- und Berechtigungskonzeptes ist weiterhin eine der Kernaufgaben. Technische Systemabsicherung, aber auch Rollen und Berechtigungen gehören 2022 zu den größten Herausforderungen. Aus diesem Grund sollte schon vor der Umsetzung eine ganzheitliche Security-Strategie definiert werden. Ein Migrationsprojekt bietet auch die Gelegenheit, die IT-Sicherheit auf ein neues Level zu heben – mit einer sauber aufgesetzten und ganzheitlich geplanten Security- und Compliance-Strategie. Daher ist die Herausforderung SiG 2.0 auch als Chance zu verstehen, die Sicherheit in SAP-Systemen zu verbessern, Rollenkonzepte effizienter zu gestalten und so S/4HANA mit all seinen Vorteilen nutzen zu können.

Das Beispiel Standardisierung

SiG 2.0 sollten viele Unternehmen als Anlass zur Standardisierung nutzen. Dies ist etwa bei den Versorgern geboten, wo das Business durch die regulatorischen Vorgaben, durch Software und Abläufe hochgradig standardisiert ist: Dinge, die man sehr gut skalieren, wo man im Geschäftsprozess bei Energie, Gas und Wasser, bei der Ver- und -Entsorgung gute Templates bilden, die Schnittstellen harmonisieren und dann diese Template-Modelle bei den Berechtigungen, Benutzern und Prozessen einführen kann. Man vollzieht mit den ersten ein, zwei die Implementierung und wird feststellen, dass am Ende alle sehr ähnlich bis gleich funktionieren. Dies bedeutet neben Kostenersparnis auch einen erheblichen Sicherheitsgewinn. Standardisierung ist zwar eine Herausforderung, zumal auch der menschliche Faktor hinzukommt und sie nicht immer schnell von der Hand geht, aber es ist absolut zielführend, so an eine Infrastruktur heranzugehen und wirklich Bottom-up von der Technik, den Schnittstellen bis ganz nach oben alles so weit wie möglich zu standardisieren.

Problemfelder Komplexität und Fokussierung

Wer sich der Herausforderung S/4HANA und SiG 2.0 stellt, muss auch seitens der Geschäftsführung Ressourcen bereitstellen, was Zeit in der Personalbeschaffung erfordert – und natürlich Geld. Doch ist immer noch in vielen Firmen zu beobachten, dass die Fokussierung und Finanzierung meist stiefmütterlich ist, obwohl dies hier eher geringe Investitionen sind, man braucht wenige gut qualifizierte Mitarbeiterinnen und Mitarbeiter und zusätzliche Expertise in SAP-Sicherheit. Mit SiG 2.0 gilt es jetzt, wirklich zu verstehen, dass diese Maßnahmen nicht mehr fakultativ sind: Verfügbarkeit und Compliance-Anforderungen sind eine zu erfüllende Vorgabe – und diese kostet erst einmal Top-down-Investment.

Besonders die Komplexität hinsichtlich Rollen und Berechtigungen sehen Unternehmen als große Herausforderung der Transformation, obwohl es seit Längerem probate Tools wie die SAST SUITE gibt, mit denen man dies gut managen kann. Hier gibt es weiterhin steigenden Bedarf an Expertise, denn die Sorge vor Kontrollverlust nimmt auch bei Administratoren und Technikern zu: Die Welt wird immer komplizierter und zum Beispiel im KRITIS-Bereich der Ver- und Entsorgung gibt es sehr lange Prozessketten, etwa Messstellen, Messstellenbetreiber, Abrechnungen, die Trennung von Vertrieb und Netz: sehr komplexe Systeme, wo man auch hinschaut. Zudem wird das Outsourcing in die Cloud vorangetrieben, Schnittstellen werden auch hier immer komplexer. Bei diesen Problemfeldern muss man deutlich sagen, IT-Governance-Planung kommt von oben, es muss kein Fünfjahresplan sein, aber wenn dies nicht klar geregelt ist, sind Lücken und Frustration vorprogrammiert.

www.sast-solutions.de

LEARNINGS AUS DEN LETZTEN PROJEKTEN

- Transition so planen, dass die neue Sicherheitsarchitektur SiG-abnahmefähig ist
- Zusätzliche SAP-SIEM-Monitoring-Komponente einbinden
- So weit wie möglich standardisieren
- Zeitersparnis und Sicherheitsgewinn durch Ausprägung der Rollen im Template
- Echtzeitüberwachung für ein ganzheitliches Sicherheitskonzept
- Ausreichende Fokussierung und Ressourcen gewährleisten
- Sorgen um wachsende Komplexität ernstnehmen und externe Expertise nutzen
- IT-Governance-Planung sicherstellen

BCM – DER BERG RUFT!

WAS SIE VON EINER BERGTOUR ÜBER BUSINESS CONTINUITY MANAGEMENT LERNEN KÖNNEN

Quelle: ©cofficevit – Stock.adobe.com

Bei einer schwierigen Gipfelbesteigung geht es wie bei der Einführung eines Business Continuity Management vor allem um die vorausschauende Verhinderung von Notfällen und das Management von Krisensituationen. Was beim BCM trocken und theoretisch erscheint, wird am Beispiel einer Bergtour greifbar und anschaulich. Zögern Sie nicht länger und legen Sie los: Sie werden feststellen, dass jeder kleine Vorbereitungsschritt Ihrer Organisation unmittelbar mehr Sicherheit und Handlungsfähigkeit im Notfall verschafft.

Zuerst werden die Geschäftsprozesse aufgenommen. Diese zeitintensive Arbeit ist, wie das Anlegen der richtigen Kleidung am Berg, unabdingbare Voraussetzung für die spätere Betrachtung der möglichen Schwachstellen und Risiken für die Geschäftsfortführungsplanung.

Die Seilschaft

Dem Zusammenstellen der Seilschaft entspricht die Aufstellung der besonderen Aufbauorganisation (BAO): Hier wird bestimmt, wer in Zeiten eines Notfalls welche besondere Aufgabe wahrnimmt, um bei einem Wettersturz die gesamte Gruppe wieder heil vom Berg zu bekommen.

Die Routenplanung und der Schwierigkeitsgrad, den man sich und den Teammitgliedern zutraut, sind vergleichbar mit dem Anwendungsbereich und dem nun festzulegenden Risikoappetit der Organisation. Die letzte vorbereitende Arbeit ist nun die Zusammenstellung der notwendigen Karten für den Weg – das Dokumentenmanagementsystem wird befüllt.

Der Aufstieg

Hat man all diese Aufgaben zufriedenstellend erledigt, beginnt die Planung des Aufstiegs mit dem Blick in die Wand: Wo sind Trittstellen, welche Passage muss funktionieren, wo sind Schwierigkeiten zu erwarten und wie wahrscheinlich ist es, dass sie den Gipfelsturm verhindern? Im zweiten Schritt wird geprüft, wie weit einen die mitgebrachten Hilfsmittel durch die Schwierigkeiten tragen. Im BCM befinden wir uns damit mitten in der Business Impact Analyse (BIA). Wenn festgestellt wird, dass ein paar Meter Seil mehr notwendig sind, werden diese auf dem Weg zum Einstieg noch besorgt. Der Soll-Ist-Vergleich hat damit ganz selbstverständlich stattgefunden.

Das Risiko

Mit der nachfolgenden Risikoanalyse (Hier gibt es bröseligen Fels am Berg mit Absturzgefahr! Haben wir wirklich genug Steigeisen und Seile?) legen wir die Grundlage für weitere Strategieoptionen und Business Continuity Lösungen, die den Erfolg der Unternehmung trotz der festgestellten Widrigkeiten sicherstellen. Vor dem Einstieg in die Wand wird geprüft, ob die neuen Seile tatsächlich lang genug sind und ob sie auch das volle Gewicht eines Kletterers beim Fall halten. Die Ergebnisse dieser Phase der Übungen und Tests werden ebenfalls in den Soll-Ist-Vergleich einbezogen (Reicht das Seil jetzt wirklich? Wenn ja, dann los!).

Gipfel erreicht

Die erlangten Erkenntnisse werden als Handlungsanweisung in ein Notfallhandbuch geschrieben, damit in einem Ernstfall schnell nachgeschlagen werden kann, wie am besten vorzugehen ist. Beim folgenden Aufstieg erweist sich, ob alles richtig bedacht wurde und ob die Planungen und Maßnahmen ausreichend waren. Bricht der Fels tatsächlich unter den Füßen eines Kletterers weg, so muss das Seil halten. Wenn sich ein Mitglied der Seilschaft verletzt, kann nach der Bergung das vorbereitete Erste-Hilfe-Buch konsultiert werden, um den Notfall der Verletzung in den Griff zu bekommen.

Fazit: Der Weg zu einem erfolgreichen BCM beginnt nicht erst an der Steilwand, sondern mit dem Schnüren der Wanderstiefel. Das HiScout BCM unterstützt Sie zuverlässig bei jedem Schritt.

Daniel Linder, www.hiscout.com

RANSOMWARE UND DIE CLOUD

MIT SAAS STEIGEN AUCH DIE RISIKEN

„JEDES UNTERNEHMEN IST FÜR CYBERKRIMINELLE INTERESSANT."

Michael Scheffler,
Country Manager DACH, Varonis Systems,
www.varonis.com/de/

Es gibt in der Cybersecurity keine absoluten Wahrheiten. Dennoch: Es ist keine Frage ob, sondern wann ein Unternehmen Opfer eines Angriffs wird. Aus diesem Grund ist es ratsam, bei allen Sicherheitsanstrengungen und -initiativen davon auszugehen, dass es Angreifer in die eigenen Systeme geschafft haben. Auf diesen Fall muss man sich vorbereiten und entsprechende Pläne erstellen. Denn auch wenn sich viele dessen nicht bewusst sind: Vorbei sind die Zeiten in denen Unternehmen sagen konnten, dass sie nicht interessant für Cyberkriminelle seien. Heutzutage geht es den Angreifern mehr denn je darum, Daten zu verschlüsseln, um den Betrieb zum Erliegen zu bringen. Waren bis vor kurzem noch fast ausschließlich Unternehmen in regulierten Märkten, zum Beispiel die Finanzbranche oder am DAX notierte Unternehmen das Ziel einer Attacke, ändert sich dies gerade: Jedes Unternehmen verfügt über sensible und wertvolle Daten. Daraus ergeben sich zwei Konsequenzen: Entweder sind Angreifer an diesen Daten interessiert oder sie gehen davon aus, dass Unternehmen bereit sind, für die Entschlüsselung zu zahlen.

Die Cloud wird immer beliebter

Die Zeichen der Zeit stehen längst auf Cloud-Nutzung – mit all ihren Vorteilen und potenziellen Nachteilen oder Gefahren. Zur Tendenz, Dateien übermäßig stark zu teilen, kommt noch ein weiterer Punkt: Die meisten Mitarbeiter gehen davon aus, dass zum Beispiel eine Kollaborationssoftware, die sie täglich nutzen, sicher ist. Bis zu einem gewissen Punkt stimmt das sogar: SaaS-Anbieter schützen ihre Infrastruktur und die angebotenen Lösungen hervorragend. Gemäß dem Prinzip der geteilten Verantwortung sind die Unternehmen jedoch unmissverständlich für die Dateien, die in diesen SaaS-Anwendungen gespeichert werden, verantwortlich und können sich bei einem Verlust oder Missbrauch keinesfalls auf den Anbieter berufen.

Für die Nutzer erscheint die Nutzung verschiedener Cloud-Dienste durch die Integration zwischen Anwendungen und Plattformen mittels API-Verbindungen oft nahtlos. Die Verwaltung der SaaS- und IaaS-Plattformen sowie die einzelnen Sicherheitskontrollen und -warnungen für jede dieser Plattformen erfolgen jedoch meist isoliert. Dies verschafft Angreifern einen Vorteil: Eine Warnung über verdächtige Aktivitäten auf einer Plattform geht im Rauschen des Security-Alltags oft unter, da der nötige Kontext fehlt. Nur wenn man in der Lage ist, einzelne Warnungen über mehrere SaaS-Anwendungen hinweg zu verbinden, lassen sich Angriffe identifizieren. Deshalb ist ein ganzheitlicher Überblick über die verschiedenen Plattformen essenziell.

Es gilt, die Auswirkungen eines kompromittierten Kontos möglichst stark zu reduzieren. Ist man in der Lage, zu weit gefasste Zugriffsrechte zu erkennen und automatisiert zu minimieren, reduziert sich die Anfälligkeit für einen Ransomware-Angriff deutlich. Kommt dann noch die intelligente Analyse des Nutzerverhaltens hinzu, die auffälliges Verhalten wie das reihenweise Öffnen, Kopieren oder Verschlüsseln von Daten erkennt, lassen sich Angriffe nahezu aller Art frühzeitig erkennen und automatisiert stoppen – ganz gleich, ob On-Premises oder in der Cloud. Angreifer nutzen ihr Wissen hinsichtlich der Überberechtigungen und den üblichen Ansätzen der Security-Lösungen (User- oder Rollen-basierte Zugangsberechtigungen) aus. Nur wer die Daten in den Fokus stellt und Berechtigungen managt, wird den Angreifern einen Schritt voraus sein, da man auf diese Weise sofort untypische Datennutzung erkennen und entsprechende Abwehrmaßnahmen einleiten kann.

Michael Scheffler

SYNTHETISCHE IDENTITÄTEN: DIE NEUE GEFAHR

ABER WIE ERKENNE ICH SIE RECHTZEITIG?

Arbeit im Homeoffice, Chatten mit Freunden, Online-Shopping und -Banking – unser Leben spielt sich immer mehr im digitalen Raum ab. Für Cyberkriminelle eröffnet sich dadurch ein Bauchladen nur allzu leicht zugänglicher Daten, aus denen sie fiktive – sogenannte synthetische – Identitäten zusammenstellen können.

Anders als beim Diebstahl der Identität einer real existierenden Person, gibt es beim synthetischen Identitätsbetrug keinen echten Konto- oder Accountbesitzer, dem unerklärliche Kontobewegungen oder unautorisierte Onlineeinkäufe auffallen könnten oder der sich über eine Mahnung wundern würde. Das macht es besonders schwer, diese Masche aufzudecken und ist ein Grund dafür, dass der Betrug mit synthetischen Identitäten sich in kriminellen Kreisen immer größerer Beliebtheit erfreut. Die Gauner kombinieren dabei erbeutete echte Daten mit falschen Informationen und kreieren daraus eine fiktive Identität.

Die dazu notwendigen realen persönlich identifizierbaren Informationen (PII) wie E-Mailadressen, Sozialversicherungsnummern, Reisepassnummern, Angaben zum Wohnort oder Geburtsdaten werden durch Phishing abgegriffen bzw. sind im Darknet verfügbar. Die Betrüger können hier aus dem Vollen schöpfen. Mit Hilfe von Deepfake-Technologie lassen sich sogar Fotos erstellen. Die auf diese Weise neu geschaffene Identität erscheint so täuschend echt, dass bei der Eröffnung eines Bankkontos oder eines Shopping-Accounts meist keinerlei Verdacht entsteht.

Ist das neue Bankkonto mit der Frankenstein-Identität erstellt, können die Betrüger in aller Ruhe einen Kredit beantragen, diesen ausschöpfen und spurlos verschwinden. Im Bereich E-Commerce nutzen sie häufig eine Kombination aus legitimen Zahlungsdaten und falschen Angaben, um über einen längeren Zeitraum hinweg ungestört Transaktionen abzuschließen, ohne dass der Betrug entdeckt wird. Synthetische Identitäten werden auch für Empfehlungsbetrug im Rahmen von Kundenbindungsprogrammen angewandt: Dabei werden neue Konten gefälscht, um Einführungsprämien in Anspruch zu nehmen.

Benutzerfreundlichkeit versus Sicherheit?

Die steigende Anzahl von Geräten, Kanälen und Zugriffpunkten spielt den Cyberkriminellen in die Hände. Zugleich sinkt die Geduld der Verbraucher bei Onlineaktivitäten: Laut einer Studie von Ping Identity laufen Anbieter, denen es nicht gelingt, die richtige Balance zwischen Benutzerfreundlichkeit und Datensicherheit zu finden, Gefahr, ihre Kunden an die Konkurrenz zu verlieren. So gaben 45 Prozent der Befragten an, dass sie bereits einem Onlinedienst den Rücken gekehrt hätten, weil sie das Einlog-

VERHALTENSBASIERTE BIOMETRIE LERNT MIT HILFE VON MACHINE LEARNING STÄNDIG DAZU UND IST IN DER LAGE, SOWOHL DIE IDENTITÄT REGELMÄSSIGER NUTZER ZU IDENTIFIZIEREN ALS AUCH BOTS AN IHREM NICHT-MENSCHLICHEN VERHALTEN ZU ERKENNEN.

Thomas Schneider, Regional Sales Director DACH & EMEA South, Ping Identity, www.pingidentity.com

gen als frustrierend empfanden. 53 Prozent würden zu einem konkurrierenden Onlineangebot wechseln, vorausgesetzt das Identitäts- und Zugriffsmanagement funktioniert dort wesentlich einfacher.

Für Onlineanbieter bedeutet das: Sie müssen den Spagat schaffen, das Betrugsrisiko zu minimieren, ohne ihre Kunden durch umständliche Authentifizierungsmaßnahmen wie CAPTCHA oder das Abfragen von PII abzuschrecken. Möglichkeiten wie Spracherkennung, Fingerabdruck-Scans und Gesichtserkennung sorgen für eine reibungslose Kundenerfahrung, garantieren aber für sich allein genommen keine komplette Sicherheit. Auch Methoden, die auf reinen Verhaltensanalysen beruhen, haben ihre Tücken: Denn menschliches Verhalten ist nicht statisch. So änderten im Zuge der Corona-Pandemie viele Menschen ihre digitalen Gewohnheiten. Sie meldeten sich zu anderen Zeiten oder mit anderen Geräten an und kauften andere Produkte wie beispielsweise Lebensmittel. Doch Fehlalarm bei der Sicherung von Onlineaktionen kann fatal sein. Wird einem Kunden beispielsweise das Benutzerkonto gesperrt, wird ihn das vermutlich für immer verprellen.

Verhaltensbiometrische Daten decken Anomalien auf

Neue intelligente Sicherungsmechanismen überwachen daher bestimmte Muster der Verhaltensbiometrie: Ob im Finanzsektor oder im E-Commerce – sobald ein Benutzer mit einem Gerät oder einer Anwendung interagiert, erzeugt er mit jedem Wischen auf dem Smartphone und mit jedem Mausklick am PC hunderte von eindeutigen Benutzerdaten. Während die Betrugserkennung bislang fast ausschließlich in der Zahlungsphase der Customer Journey eingesetzte, prüft moderne Onlinebetrugserkennung bereits ab dem Login die biometrischen Verhaltensdaten, die durch Interaktionen zwischen Mensch und Gerät, durch Geräteattribute und Kontoaktivitäten generiert werden. Sicherheitsrisiken werden unterbunden, bevor sie Schaden anrichten können.

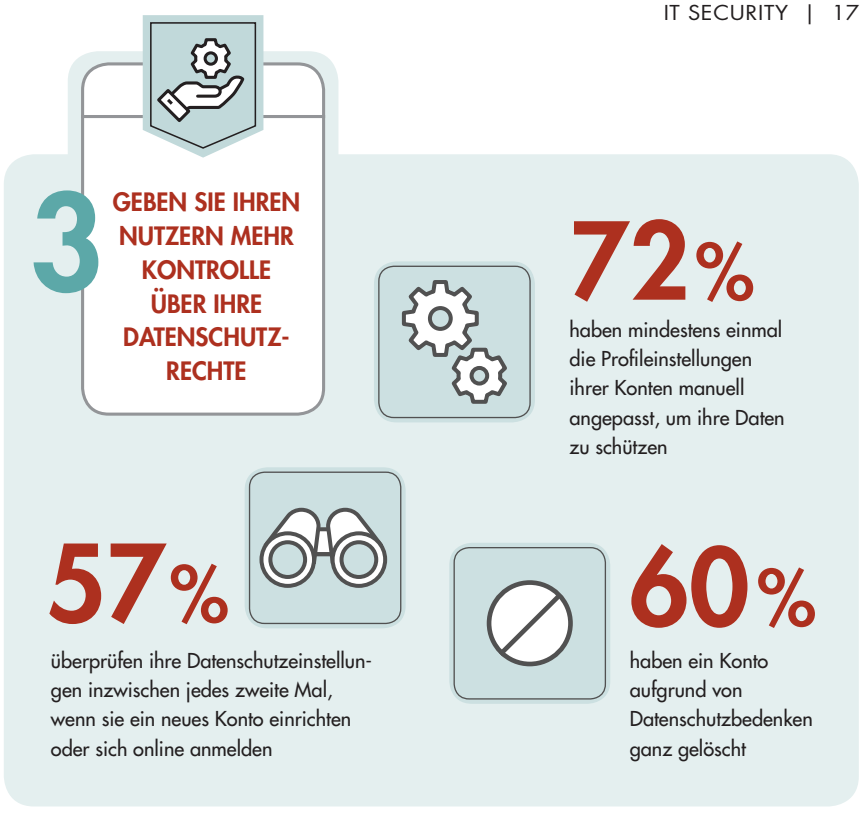
Verhaltensbasierte Biometrie lernt mit Hilfe von Machine Learning ständig dazu und ist in der Lage, sowohl die Identität regelmäßiger Nutzer zu identifizieren als auch Bots an ihrem nicht-menschlichen Verhalten zu erkennen. Die Verwendung von Copy-Paste oder der automatischen Vervollständigungsfunktion beispielsweise, die Geschwindigkeit, mit der auf dem Smartphone getippt oder die Maus über den Bildschirm bewegt wird, können auf den Missbrauch einer Identität hinweisen. Denn ein echter Mensch unterscheidet sich in seiner Art zu klicken oder zu scrollen von Bots, Skripts oder Emulatoren.

Ein normaler Nutzer, der sich neu für einen Account anmeldet, ist nicht mit der Reihenfolge der Felder im Anmeldeformular vertraut und agiert beim Ausfüllen entsprechend langsamer. Weitere Anzeichen für illegale Aktivitäten sind die wiederholte Eingabe eines Anmeldevorgangs mit unterschiedlichen Daten, ein unnatürlich gleichmäßiges, einstudiertes Navigieren zwischen den Seiten oder Abweichungen von der durchschnittlichen Dauer eines Bestelllvorgangs.

Fazit

Cyberkriminelle werden sich auch in Zukunft immer neue und immer raffiniertere Betrugsmaschen ausdenken. Um nicht den Kürzeren zu ziehen, müssen sich die Sicherheitsmethoden der Unternehmen mindestens ebenso dynamisch weiterentwickeln. Mit einer Kombination aus modernem Identitäts- und Zugangsmanagement und Fraud-Prävention durch verhaltensbiometrische Technologien ist es möglich, den Angreifern einen Schritt voraus zu sein.

Thomas Schneider



CYBERSECURITY IM ENERGIESEKTOR

FLEXIBEL UND NACHHALTIG – ABER AUCH SICHER?

Die Energiewende gelingt nur mit größtmöglicher Interoperabilität in den Energienetzen. Die darf nicht zu Lasten der Cybersecurity gehen. Dieser Beitrag erläutert, worauf Unternehmen achten müssen.

2021 war ein gutes Jahr für Hacker. SolarWinds und Log4j waren nur die Spitze des Eisbergs. Den Kriminellen gelangen einige spektakuläre Angriffe, darunter auf kritische Infrastrukturen wie Ölpipelines oder Krankenhäuser, bei denen sie erhebliche Kollateralschäden anrichteten. Die Allianz-Versicherung schätzt, dass die Hackerangriffe im letzten Jahr um mehr als 125 Prozent zugenommen haben. Die Dunkelziffer dürfte hoch sein. Tag für Tag zahlen Betriebe Lösegeld, um wieder an ihre gesperrten Daten zu gelangen, die Öffentlichkeit erfährt meist nichts davon. Das Bundesamt für Sicherheit in der Informationstechnik hat für die Cyber-Sicherheitslage Warnstufe Rot ausgerufen, zuletzt im Dezember 2021.

Die wohl kritischste aller Infrastrukturen befindet sich im Energiesektor. Ohne Strom bricht in einer modernen Gesellschaft alles zusammen – Kommunikations-, Logistik-, Wasser- und Finanznetze, um nur einige zu nennen. Die Hacker wissen das und deshalb nehmen sie Energieversorger und Stromnetzbetreiber vermehrt ins Visier, weil sie dort mit überschaubarem Aufwand maximalen Schaden anrichten und mit Ransomware saftiges Lösegeld erpressen können. Dabei kommt ihnen zupass, dass die Anlagen im Energiesystem nicht mehr voneinander abgeschottet sind. Interoperabilität ist wichtig, damit Komponenten und Akteure im Energienetz Daten und Informationen austauschen können. So soll sich das Elektroauto mit der Photovoltaikanlage verstehen und die wiederum mit dem Stromnetz – ganz gleich, von welchem Hersteller diese Komponenten stammen oder von welchem Energieanbieter man seinen Strom bezieht. Nur so lassen sich Erzeugung und Verbrauch balancieren, auch lokal und bei schwankender Einspeisung von Sonnen- oder Windenergie, sowie über APIs Preissignale optimal nutzen. Das wiederum ist essenziell, um die ambitionierten Ziele des Green Deal zu erreichen. Bis 2030 möchte die EU ihre CO_2-Emissionen um 55 Prozent senken im Vergleich zu 1990.

Teufelskreis durchbrechen

So entsteht scheinbar ein Teufelskreis: Die Energiewende braucht Digitalisierung für mehr Flexibilität, was Interoperabilität erfordert, sie schafft damit aber gleichzeitig zusätzliche Angriffsflächen für Hacker, was die Energiesysteme verletzbarer machen könnte. Erschwerend kommt hinzu, dass Energiesysteme einen Technologie-Mix umfassen mit teils viele Jahrzehnte alte Komponenten, die entwickelt wurden, lange bevor Cybersecurity ein Thema war.

Wie lässt sich dieser Teufelskreis durchbrechen? Ein guter Ausgangspunkt ist der bei IT-Experten wohlbekannte CIA-Dreiklang: Vertraulichkeit (Confidentiality),

Integrität (Integrity) und Verfügbarkeit (Availability). Auf die Energiebranche bezogen heißt Vertraulichkeit zum Beispiel, dass personenbezogene Daten wie ein Lastprofil, aus dem Einbrecher auf Abwesenheit schließen könnten, vor dem Zugriff Dritter geschützt sind. Integrität ist wichtig, damit etwa monatliche Stromrechnungen nicht manipuliert werden können. Und Verfügbarkeit heißt, dass Störungen schnell erkannt und behoben werden. Ein nachhaltiges Energiesystem zeichnet sich demnach nicht nur dadurch aus, dass es die Umwelt wenig belastet, etwa durch geringe CO_2-Emissionen, sondern zunehmend auch dadurch, dass es resilient ist und Störungen es nicht ins Wanken bringen. Cybersecurity leistet dazu einen wichtigen Beitrag.

Aus IT-Perspektive gibt es keinen wesentlichen Unterschied zwischen dem Management von Cyberrisiken in der Energiewirtschaft und anderen kritischen Bereichen wie der Finanzbranche oder dem Gesundheitswesen. Das Wichtigste ist, dass alle Komponenten für sich so sicher wie möglich sind. Viele Risiken lassen sich durch das Orientieren an Best Practices und Benchmarks sowie durch Prozesse mit eingebauter Redundanz und Prinzipien wie Security by Design mindern.

Diese Maßnahmen helfen

Wie das in der Praxis aussieht, erläutert der Report „Interoperabilität & Cybersecurity in der Energiebranche" vom Smart-Grid-Unternehmen gridX. Hier einige Aspekte daraus, die besondere Beachtung verdienen:

- Angriffsfläche minimieren: Im letzten Jahrzehnt wurden laut IEA weltweit neun Millionen Kilometer Stromleitungen gebaut, in diesem Jahrzehnt werden es voraussichtlich 16 Millionen Kilometer sein. Das Netz wächst rasant und damit eigentlich auch die Angriffsfläche. Doch dieser Zusammenhang lässt sich durchbrechen, indem man Zugangspunkte gezielt reduziert. So sollten Entwickler darauf achten, Software-Abhängigkeiten zu minimieren, Ports zu schließen und öffentlich zugängliche Ressourcen auf ein Mindestmaß zu beschränken.

DIE ENERGIEWENDE GELINGT NICHT OHNE INTEROPERABILITÄT UND DIE GELINGT NICHT OHNE CYBERSECURITY.

Andreas Booke,
Co-Gründer und CEO, gridX,
https://de.gridx.ai/

- Cloud first: Cloud-Dienste bieten Energieunternehmen Konnektivität, Skalierbarkeit und Datenanalysen in Echtzeit für mehr Flexibilität, Sicherheit und Agilität. Kritische Infrastrukturen und Cloud – für viele klingt das aber immer noch nach einem Widerspruch. Doch zahlreiche Beispiele aus der Energiebranche zeigen, dass eine zertifizierte Cloud wie von AWS sehr sicher gegen Angriffe ist und es viel seltener zu Ausfällen kommt.
- Automatisierung: Cloud-Umgebungen verändern sich ständig. Sicherheitskontrollen sollten daher automatisiert erfolgen, etwa durch einen Validierungsprozess, der bei Veränderungen automatisch die Sicherheit prüft.
- Infrastruktur als Code: Die gesamte Infrastruktur wird als Code mit modernen Tools wie Terraform, Cloudformation und Kubernetes beschrieben. Außerdem wird dieser Code in der Versionskontrolle gespeichert. Das erlaubt Nachvollziehbarkeit, Reproduzierbarkeit und Transparenz. Das Prinzip der unveränderlichen Infrastruktur reduziert mögliche Sicherheitsrisiken durch Reproduzierbarkeit und die Vermeidung von Konfigurationsabweichungen weiter.
- Verschlüsselt kommunizieren: Wo immer Daten über ein öffentliches Netz übertragen werden, sollte der Verkehr mit modernen Verschlüsselungstechnologien wie TLS 1.3 gesichert sein.
- Vier-Augen-Prinzip: Um menschliches Versagen auszuschließen, müssen immer zwei Personen den Code und die dazugehörige Dokumentation überprüfen und sicherstellen, dass höchste Qualitäts- und Sicherheitsstandards eingehalten werden.

Strategien ständig anpassen

Die Punkte stellen nur einen Auszug aus den Empfehlungen dar. Auf den ersten Blick scheint es sich vor allem um technische Maßnahmen zu handeln. Damit interoperable Technologien aber ihre Wirkung entfalten können, ist es erforderlich, dass Kontrollen nahtlos in die Unternehmensprozesse integriert und mögliche Bedrohungen ständig überwacht und minimiert werden. Und weil sich die Risiken ständig weiterentwickeln, müssen sich auch die Cybersicherheitsstrategien laufend anpassen. Dazu müssen alle Akteure im Energiesektor ihre digitalen Kompetenzen stärken und ihr Bewusstsein für Risiken schärfen.

Fazit

Die Energiewende gelingt nicht ohne Interoperabilität und die gelingt nicht ohne Cybersecurity. Zwar lassen sich Cyberangriffe nie ganz ausschließen, aber Betreiber von Energiesystemen können diese so widerstandsfähig machen, dass sie Angriffen standhalten und sich schnell von ihnen erholen. Dafür braucht es die richtigen Strategien und Technologien – vor allem aber braucht es eine Zusammenarbeit aller Akteure im Energiesektor sowie mit IT-Experten.

Andreas Booke

MHP UND LKA BW: CYBER-SECURITY-RISK-REPORT 2021

NACHHOLBEDARF BEI RISIKOBEWERTUNG UND REAKTIVER VORFALLSBEHANDLUNG

Jedes zweite Unternehmen ist in den letzten zwei Jahren Ziel einer Cyber-Attacke gewesen. Es ist davon auszugehen, dass die Zahl der Angriffe noch weiter zunehmen wird und die Attacken immer vielfältiger werden. Eine vollumfängliche Risikobetrachtung und eine im Voraus geplante und umfangreiche reaktive Vorfallsbehandlung sind geeignete Schritte dieser Entwicklung entgegenzuwirken. Unternehmen in Deutschland haben bei beiden Themen allerdings noch erheblichen Optimierungsbedarf.

Zu diesem Ergebnis kommt unser aktueller Cyber-Security-Risk-Report 2021, der in Kooperation mit dem Landeskriminalamt Baden-Württemberg entstanden ist. Dafür wurden qualitative Interviews mit Experten geführt und 314 Teilnehmende aus Unternehmen unterschiedlicher Wirtschaftsbereiche befragt. Aus der Erhebung des Status quo haben wir Optimierungspotenziale abgeleitet, die in acht Handlungsempfehlungen fließen.

Digitale Assets

Fakt ist, dass bei mehr als der Hälfte der Unternehmen eine vollumfängliche Risikobetrachtung ausbleibt. Auch die Unterstützung durch Behörden wird nicht in vollem Ausmaß genutzt. Und dass, obwohl jedes dritte betroffene Unternehmen einen Schaden in Millionenhöhe verzeichnete. Wir nehmen an, dass vor allem Organisationen mit digitalen Assets betroffen sind: In der Telekommunikationsbranche berichten 82 Prozent der Unternehmen von IT-sicherheitsrelevanten Vorfällen in den vergangenen zwei Jahren. Die Quote im IT-Sektor liegt bei 52 Prozent. In diesen Bereichen gehen wird davon aus, dass ein höherer Digitalisierungsgrad vorhanden ist, wodurch mehr potenzielle Angriffsflächen entstehen.

AUS UNSERER ERFAHRUNG LASSEN SICH IT-SICHERHEITS-VORFÄLLE ZIELGERICHTET BEWÄLTIGEN, WENN SICH ORGANISATIONEN AUF FÄLLE VORBEREITEN.

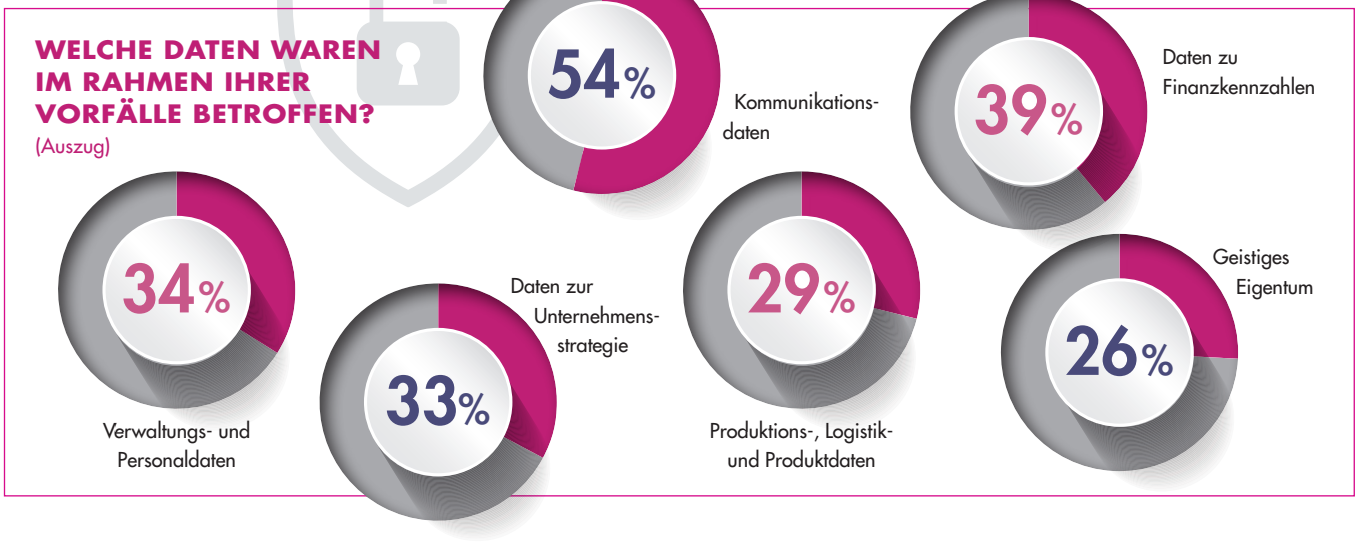
Andreas Henkel, Associated Partner und Focus Topic Lead Cyber Security, MHP, www.mhp.com

Häufigste Schwachstellen

Hacker nutzten vor allem Schwachstellen wie die Konfiguration von Systemen (39%) und auch die jeweiligen Betriebssysteme von Geräten, zum Beispiel Computer, Server, Smartphones und Kopierer (32%) aus, um an begehrte Daten zu kommen. Auch Fremd- und Privatgeräte wurden bei einem Drittel der Unternehmen als Angriffspunkt genutzt. Während bei den kleinen Unternehmen vor allem Fremd- und Privatgeräte sowie Mitarbeiter die häufigsten Schwachstellen sind, gaben die Verantwortlichen von großen Unternehmen die Konfiguration von Systemen sowie Remote-Zugänge als häufigste Ursache für Angriffspunkte an. Ein möglicher Grund dafür könnten die schnell ausgebauten Homeoffice-Lösungen während der Corona-Pandemie sein. Zukünftig wird es entscheidend sein, einen besseren Schutz der Remote-Zugänge zu etablieren, um damit das von dieser Schwachstelle ausgehende Risiko signifikant abzuschwächen.

Umfassende Risikobetrachtung

Aus unserer Sicht zählt eine umfassende Risikobetrachtung zu den wichtigsten Handlungsfeldern, um die Gefahr von Cyber-Security-Vorfällen in den Unternehmen zu minimieren. Bei einer vollumfänglichen Risikobetrachtung sollten verschiedene Aspekte im Vorfeld detailliert betrachtet und analysiert werden. Dazu zählen unserer Erfahrung nach Angriffsziele, aktuelle Bedrohungslagen, Trends und Statistiken, Angriffspfade und werkzeuge sowie potenzielle Angreifer. Nur 40 Prozent der Teilnehmenden haben all diese genannten Aspekte bei der Identifikation der IT-sicherheitsrelevanten Risiken im Blick. Demnach findet eine vollumfängliche Risikobetrachtung in deutschen Unternehmen mehrheitlich keine Anwendung. Wir empfehlen daher die



genannten Aspekte regelmäßig zu validieren. Bei Bedarf sind fehlende Merkmale zu ergänzen. Darauf aufbauend können passende Sicherheitsmaßnahmen abgeleitet und umgesetzt werden.

Präventive Maßnahmen ausbauen

Hierzu zählen insbesondere präventive Maßnahmen, die dazu beitragen sollen, Risiken zu mitigieren. Die positive Nachricht: Mehrheitlich werden die gängigsten Maßnahmen wie Passwortsicherheit (84%), Malware-Schutz (79%), Back-up-Strategien (78%), Anlassbezogenes Monitoring (72%) und Segmentierung und/oder die Rechtevergabe innerhalb von Netzwerken (72%) umgesetzt. Ausbaufähig sind allerdings die Back-up-Strategien und die E-Mail-Kommunikation sowie die Passwortsicherheit.

Passwörter sollten bestimmte Qualitätsanforderungen erfüllen, regelmäßig geändert und idealerweise lediglich für einen Zugang genutzt werden. Empfehlenswert ist außerdem die Multi-Faktor-Authentifizierung, bei der das Passwort durch einen oder mehrere zusätzliche Faktoren ergänzt oder in speziellen Fällen sogar ersetzt wird.

Verbindungen zwischen Back-ups und anderen IT-Systemen sind zu vermeiden. Die Lagerung sollte im Optimalfall an einem anderen Ort erfolgen, um die Daten auch vor natürlichen Gefahren wie Feuerausbrüchen effektiv zu schützen.

Weiter ist die E-Mail-Kommunikation stärker abzusichern, da diese nach wie vor häufig das Einfallstor für Angriffe darstellt. Vor allem Kommunikationsdaten sind mit großem Aufwand zu schützen, da sie am häufigsten Ziel von Angriffen sind. Dasselbe gilt auch für Finanzkennzahlen sowie Verwaltungs- und Personaldaten. Darüber hinaus sollten Daten zur Unternehmensstrategie sowie Produktions-, Logistik- und Produktdaten priorisiert geschützt werden. Regelmäßige Überprüfung der Zugriffsrechte sowie die Kontrolle der Datenablage können eine erste Abhilfe leisten.

Aus präventiver Sicht ist eine hohe Awareness der Mitarbeiter im Allgemeinen unverzichtbar, da sie häufig das primäre Ziel bei Angriffen sind. Wichtig sind deshalb regelmäßige Schulungen, vor allem im Umgang mit Sicherheitssoftware sowie Social Engineering. Bei Social Engineering geben sich Personen unberechtigt als Mitarbeitende eines Unternehmens aus und lassen in deren Namen Anweisungen erteilen – beispielsweise per E-Mail zur Herausgabe von internen Informationen. Eine verstärkte Awareness kann unserer Meinung nach das Risiko eines Social Engineering Vorfalls, der immerhin für jeden dritten Angriff verantwortlich ist, vermindern.

Reaktive Vorfallsbehandlung

Kommt es zu einem Vorfall, müssen die richtigen Schritte eingeleitet werden. Deshalb ist die Planung einer entsprechenden reaktiven Vorfallsbehandlung, durch die schnell auf den Eintritt IT-sicherheitsrelevanter Vorfälle reagiert werden kann, von essentieller Bedeutung. Dabei sollte das Ziel sein, die Betriebsfähigkeit möglichst aufrechtzuerhalten, Sicherheitslücken zu schließen und den Regelbetrieb wieder herzustellen. Wir empfehlen zusätzlich unbedingt, die Polizeibehörde bei IT-sicherheitsrelevanten Vorfällen zu informieren und in die Aufklärung von Cyber-Angriffen aktiv einzubinden.

Pläne zur Meldung des Vorfalls, Reaktionsweisen, Maßnahmen zur Aufrechterhaltung des IT-Betriebs sowie ein Wiederaufbauplan der IT-Systeme sollten in analoger Form vorliegen, um im Ernstfall beispielsweise bei einer Ransomware Attacke und verschlüsselten Daten weiterhin auf diese zugreifen zu können. So können vorgesehene Schritte und Maßnahmen schnell eingeleitet werden.

Aus unserer Erfahrung lassen sich IT-Sicherheitsvorfälle zielgerichtet bewältigen, wenn sich Organisationen auf Fälle vorbereiten. Hierbei hilft nicht nur ein Gefahrenbewusstsein zu entwickeln, sondern auch regelmäßig diverse Worst-Case-Szenarien immer wieder und Schritt für Schritt durchzuspielen. Nur dann fallen potenzielle Lücken auf, die möglicherweise gravierende Auswirkungen auf die Unternehmen haben können.

Andreas Henkel

DATA LOSS PREVENTION

EIN GUTES MITTEL FÜR DEN MITTELSTAND

Cyber-Kriminelle lieben den deutschen Mittelstand. Viele mittelständische Unternehmen hierzulande zählen zu den so genannten Hidden Champions: Unter dem Radar der öffentlichen Wahrnehmung dominieren sie ihren Bereich als Weltmarktführer. Dadurch verfügen sie über einen wahren Schatz an exklusivem Know-how, der Hacker und Wirtschaftsspione magisch anzieht. Sind sie erfolgreich, kann das ganz erhebliche und sogar existenzgefährdende Schäden anrichten.

Verlust von wertvollem geistigem Eigentum droht Unternehmen aber nicht nur durch Kriminelle mit bösartigen Absichten. Auch die bloße Unachtsamkeit eigener Mitarbeiter kann zu einem ungewollten Abfluss sensibler Daten führen. Hidden Champions finden sich in Deutschland vor allem im Maschinenbau und der Automobilindustrie. In diesen Branchen sind sie meist ein Teil von Lieferketten, in denen sensible Informationen wie Konstruktionsdaten in großem Umfang geteilt werden. Gehen solche Daten versehentlich an unautorisierte Empfänger, kann des erhebliche negative Folgen haben.

MIT DLP KÖNNEN UNTERNEHMEN IHRE MITARBEITER VOR FEHLERN BEIM UMGANG MIT DATEN BEWAHREN UND SO GLEICHZEITIG IHR GEISTIGES EIGENTUM SCHÜTZEN.

Carsten Hoffmann, Manager Sales Engineering, Forcepoint, www.forcepoint.com

Geistiges Eigentum sicher verwahren

Um den ungewollten Abfluss wertvoller Daten zu verhindern, steht Unternehmen mit Data Loss Prevention (DLP) ein äußerst wirkungsvolles Instrument zur Verfügung. DLP-Lösungen können schützenswerte Informationen identifizieren und Mitarbeiter vor Fehlern bewahren, indem sie auf potenziell riskantes Verhalten hinweisen. So kann DLP etwa das Versenden, Kopieren oder Ausdrucken extrem sensibler Daten automatisch unterbinden. Damit stellt es sicher, dass geistiges Eigentum nicht versehentlich in falsche Hände gerät.

Obwohl gerade mittelständische Unternehmen aufgrund ihres exklusiven Know-hows besonders von DLP profitieren können, zögern sie häufig, solche Lösungen überhaupt in Betracht zu ziehen. Der Einrichtungsaufwand von DLP ist riesig, deshalb ist diese Technologie nur etwas für Konzerne, aber nicht für uns – so eine häufige, aber unnötige Befürchtung. Entgegen einem weitverbreiteten Mythos müssen Unternehmen für den Einsatz von DLP nicht zwangsläufig umfangreiche Dateiklassifizierungen vornehmen und viele Richtlinien ausarbeiten. Es gibt Lösungen am Markt, die über Schnittstellen auf andere Sicherheitstools zugreifen können, die bereits Datenklassifizierungen vorgenommen haben; und die schon ab Werk ein großes Set aus vordefinierten Richtlinien mitbringen.

Datenschutzverletzungen verhindern

Ein anderes weit verbreitetes Vorurteil: DLP ist ein Tool zur Überwachung der Mitarbeiter. Auch das ist falsch. Es geht nicht darum, jeden Mitarbeiter als potenziellen Datendieb zu behandeln oder zu ermitteln, welche Mitarbeiter sorglos mit Daten umgehen. Es geht darum, versehentliche Datenschutzverletzungen zu verhindern. Dafür müssen DLP-Lösungen keine Daten zentral sammeln. Es reicht völlig aus, wenn sie lokal auf den Endgeräten über die Einhaltung der Richtlinien wachen und Mitarbeiter auf riskantes Verhalten hinweisen. Natürlich sind übergreifende Auswertungen möglich und auch sinnvoll. Diese Auswertungen lassen sich aber anonymisiert durchführen, denn für das Unternehmen ist es unbedeutend, welcher Mitarbeiter versehentlich Daten in die Cloud hochladen möchte, die dort nicht hingehören. Entscheidend ist, dass das DLP ihn davon abhält.

Fazit

Mit DLP können Unternehmen ihren Mitarbeitern im Arbeitsalltag helfen – und so ihre Mitarbeiter wie auch ihr geistiges Eigentum zuverlässig schützen. Keine andere Technologie vermag es, bösartige und versehentliche Datenschutzverletzungen so wirkungsvoll zu verhindern. Davon können auch und ganz besonders die zahlreichen Hidden Champions des deutschen Mittelstands profitieren.

Carsten Hoffmann

SPICKZETTEL DER IT-SECURITY

32 FACHBEGRIFFE SCHNELL UND EINFACH ERKLÄRT

Was ist eigentlich der Unterschied zwischen APT und ATP? Da verhaspeln sich selbst IT-Profis manchmal. Abteilungsleiter und andere Entscheidungsträger verlieren sich gern im Branchenjargon. Doch wenn IT-Sicherheit Teil der allgemeinen Geschäftsstrategie und Risikobewertung werden soll, muss sich die Kommunikation verbessern. Nur so gelingt es, das wichtige Thema in Sitzungen von Vorständen und Geschäftsleitungen zu platzieren.

Gerade deshalb wünscht man sich bei vielen Fachbegriffen der schnelllebigen Welt der IT-Sicherheit einen Blick in ein Wörterbuch, um den Begriff richtig zu verwenden oder anderen schnell und einfach erklären zu können.

Zu diesem Zweck finden Sie in diesem Whitepaper eine Erklärung von 32 hochaktuellen Begriffen der IT-Security. Unser Ziel ist es, mit wenigen Sätzen das Wichtigste zu den Begriffen zu erklären – nicht nur für Fachleute, sondern auch für Laien.

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

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Andreas Booke, Andreas Henkel, Carsten Hoffmann, Daniel Linder, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Michael Scheffler, Thomas Schneider

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

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

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

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 29,
gültig ab 1. Oktober 2021.

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

SAVE THE DATE!

We secure IT

19.05.22 | Digitalevent

#WesecureIT2022