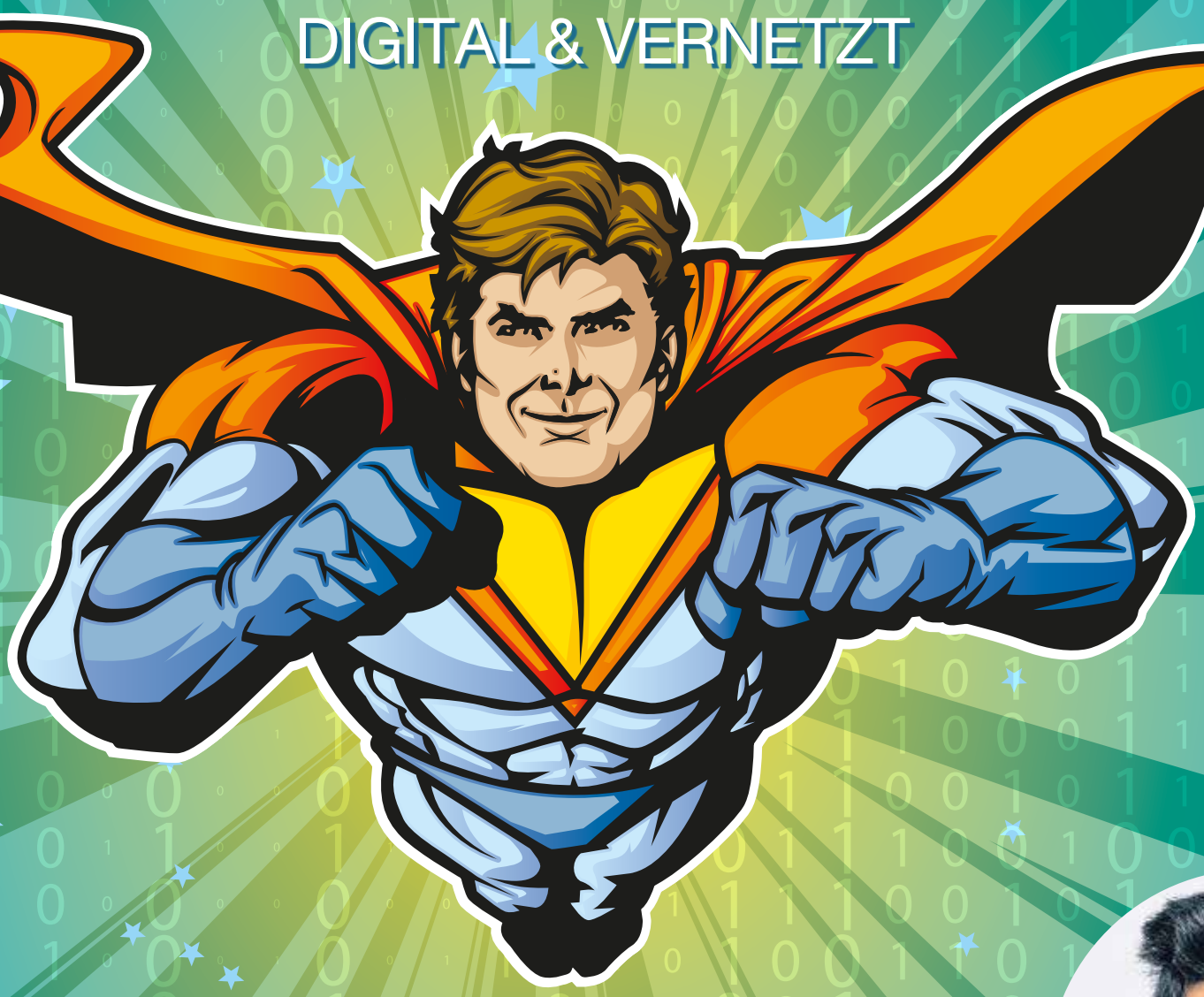
IT-SICHERHEIT Schützen Sie sich und Ihr Unternehmen. **S. 04**

BRANDSCHUTZ So vermeiden Sie gefährliche Situationen. **S. 10**

EINBRUCHSCHUTZ Langfinger schlagen immer zu – schützen Sie sich. **S. 11**

ZUKUNFT SICHERHEIT

DIGITAL & VERNETZT



PHILIPP KALWEIT

Deutschlands begehrtester Hacker spricht im Interview über sein Verständnis von Sicherheit.

Timo Mitsch
Dass Sprachassistenten uns regelmäßig abhören, ist bekannt. Trotzdem wird dies zu selten hinterfragt. Das sollten wir überdenken!

Simon Eichler
Sicherheit ist für viele von uns ein grundlegendes Bedürfnis und sollte in jeder Situation gewährleistet sein, egal ob zu Hause oder in der digitalen Welt.

Tanja Bickenbach
Cyber-Resilienz im Unternehmen erfordert wirkungsvolle und schnelle Reaktionen auf Cyberattacken. Wir werfen einen Blick auf wichtige Schlüsseltechnologien.

Sicher vernetzt

Die Vernetzung von Geräten und Smart Devices schafft mehr Lebenskomfort und viele Effizienzvorteile. Bereits im Jahr 2021 sollen deshalb etwa 25 Milliarden IoT(Internet of Things)-Geräte mit dem Internet verbunden sein, prognostizieren Marktforscher von Gartner. Dazu gehören Kameras, Thermostate, Türöffnungsanlagen, Lichtanlagen und Diagnosegeräte, aber auch Verkehrs- und Finanzinfrastruktur sowie Maschinen. Sicherheit ist dabei oberstes Gebot.

Eine Studie der zu Gartner gehörenden CEB stellt fest: Fast 20 Prozent aller befragten Unternehmen haben in den vergangenen drei Jahren mindestens einen IoT-basierten Angriff beobachtet. Für das Vertrauen in die vernetzte digitale Infrastruktur ist es daher umso wichtiger, dass die IoT-Devices der Wirtschaft, aber auch das vernetzte Smart Home vor Manipulationen durch Hacker wirksam geschützt sind.

Smart und sicher vernetzt

Maschinen, Anlagen, Logistik und Produkte kommunizieren und kooperieren im Internet der Dinge direkt miteinander. Unternehmen müssen ihre vernetzten Anlagen und Steuerungssysteme professionell schützen. Aber auch Freiberufler und Privatnutzer sollten ihre IT-Sicherheit nicht vernachlässigen. Hier gilt es, ein Bewusstsein für die Notwendigkeit von IT-Security zu schaffen. Gemeinsam mit Experten für die Ermittlung und Analyse von Schadsoftware auf IoT-Devices des unabhängigen AV-TEST Instituts hat der Internetverband eco deshalb Bausteine für adäquate IoT-Security entwickelt.

Eine Cyber-Abwehrstrategie sollte das Bewusstsein aller Nutzer schärfen. Ziel ist es, Security aus einem Guss zu schaffen. Das beginnt in Unternehmen mit eindeutigen Verantwortlichkeiten über die gesamte Sicherheitsinfrastruktur. Dies gilt von der Beschaffung der Geräte bis hin zur Planung, Implementierung und zum Betrieb. Gerne zitiert ist das Beispiel einer Webcam,

Alexander Rabe
Geschäftsführer eco – Verband der Internetwirtschaft e. V.

> Maschinen, Anlagen, Logistik und Produkte kommunizieren und kooperieren im Internet der Dinge direkt miteinander.

die vom Hersteller standardmäßig so ausgeliefert wurde, dass jeder Internetnutzer darauf zugreifen kann. Als Überwachungskamera out of the box montiert, konnte dadurch jeder Dieb online auskundschaften, ob die Luft rein ist.

Sicherheits- und Vertrauensfunktionen von Anfang an mitzudenken, ist Schadensprävention. Zu Security by Design gehören technische Mindestsicherheitsstandards. Auf Geräte, die sich nicht updaten lassen, sollte generell verzichtet werden. Ein Schnäppchen vom Discounter erweist sich sonst schnell als gefährliche Zeitbombe. Idealerweise funktioniert Security auch ohne Beteiligung der Nutzer, beispielsweise durch automatische Updates.

Nicht nur jeder PC, sondern auch das Netzwerk sollte mithilfe geeigneter IT-Sicherheitslösungen geschützt sein, die alle IoT-Devices überwachen.

KI untersucht Anomalien im Datenstrom

Künstliche Intelligenz (KI) und maschinelles Lernen können künftig die Cybersicherheit weiter verbessern. KI erkennt beispielsweise Anomalien von Angriffsversuchen, um diese schon in ihrer Ausführung abzuwehren. Bei traditionellen Systemen ist es selbst für die Experten zum Teil sehr herausfordernd, aus dem täglichen Grundrauschen bedeutsame Hinweise herauszufiltern. Ihnen kann KI helfen, etwa durch eine Analyse von Metadaten inklusive deren Herkunft – selbst bei neuartigen Angriffen, die bislang nicht in den Security-Systemen codiert wurden. ■

Follow us facebook.com/Mediaplanet_Stories @MediaplanetGER @Mediaplanet_germany Please Recycle

Project Manager: **Timo Mitsch, Simon Eichler** Head of Key Account Management: **Tanja Bickenbach** Senior Business Development Manager: **Carolin Babel** Vertriebspartner: **Frankfurter Allgemeine Zeitung, 27.09.2019** Geschäftsführung: **Richard Båge** (CEO), **Philipp Colaço** (Managing Director), **Franziska Manske** (Head of Editorial & Production), **Henriette Schröder** (Sales Director) Designer: **Ute Knuppe** Druck: **Frankfurter Societäts-Druckerei GmbH & Co. KG** Mediaplanet Kontakt: **redaktion.de@mediaplanet.com** Coverfoto: **Andrey Suslov/shutterstock**

Als SPONSORED und GASTBEITRÄGE gekennzeichnete Artikel sind keine neutrale Redaktion der Mediaplanet Verlag Deutschland GmbH.

Mit Strategie zu mehr Schutz

Ohne IT-Technologie funktioniert unsere Welt heute nicht mehr: Das Eigenheim ist als Smart-Home vernetzt und auch ganze Unternehmensbereiche sind inzwischen komplett digitalisiert. Wie gelingt jedoch der Schutz, wenn gleichzeitig gefährliche Cyberattacken zunehmen? Eine mögliche Antwort darauf sind eine risikobasierte Analyse sowie neue Technologien, um Angreifern immer wieder die Stirn zu bieten und fehlende Fachkräfte zu kompensieren.

Gastbeitrag, Computacenter

Wenn Unternehmen heute wettbewerbsfähig bleiben wollen, müssen sie auf digitale Prozesse und Strategien setzen – und das passiert längst nicht mehr nur in der klassischen Office-IT. Informationstechnologien dringen seit einigen Jahren verstärkt in Bereiche vor, die bislang wenig oder gar keine Berührungspunkte damit hatten. Die meisten kommen mittlerweile auch nicht mehr ohne innovative Technologien wie Cloud Computing oder Machine Learning aus. Diese Entwicklung bringt riesige Chancen mit sich. Je weiter sie allerdings fortschreitet, desto komplexer gestalten sich IT-Infrastrukturen und desto schwieriger wird ihr Schutz.

Gefahr durch Cyberangriffe

Neue Technologien durchdringen und optimieren unseren beruflichen wie privaten Alltag immer stärker. Gleichzeitig kann diese Digitalisierung auch eine Gefahr werden, wenn es zu gefährlichen Cyberangriffen kommt.

Heute kann sich kein Unternehmen mehr einen größeren Sicherheitsvorfall leisten. Dabei vergrößern und verändern sich die Angriffsflächen ständig und es braucht regelmäßige, individuelle Risikoanalysen. Viele Unternehmen schätzen die Gefahren nicht richtig ein. Sie orientieren sich meist an statischen Compliance-Standards, berücksichtigen aber nicht ihre individuelle Situation: Welche Angreifer haben es auf das eigene Unternehmen abgesehen, welche Daten sind am stärksten gefährdet und wo liegen die Schwächen bei der Absicherung?

Sicherheit in jedem IT-Projekt

Zentral ist daher, die Security von Anfang an mitzudenken, um für die nötige Sicherheit zu sorgen – und das in jedem IT-Projekt. Konkreter heißt das: Jedes IT-Projekt ist auch ein Security-Projekt. Insgesamt müssen Unternehmen ihre klassischen Sicherheitsansätze verbessern und gleichzeitig neue Methoden integrieren. Dabei sollte im ersten Schritt die Prävention im Vordergrund stehen, um die Anzahl der Vorfälle von vornherein zu reduzieren. Dies erleichtert dann auch die Detektion und Reaktion auf tatsächliche Angriffe.

Mehr Sensibilität bei Mitarbeitern

Je nach Ergebnis der individuellen Risikoanalyse müssen dann Unternehmen ihre Security-Maßnahmen priorisieren: Das schwächste Glied ist weiter der Benutzer, der E-Mails und deren Inhalte falsch behandelt. Ihn für mehr Bewusstsein und Sensibilität zu schulen, ist ein wesentlicher Punkt. Hinzu kommen ausreichende technische Schutzmaßnahmen. Auch die Adminstrator- und VIP-Rechte sollten Unternehmen eingrenzen und kontrollieren. Wenn Hacker auf diese Konten Zugriff erhalten, können sie heute praktisch alle Daten und Anwendungen des Unternehmens manipulieren. Aber auch Social Engineering stellt eine große Gefahr dar, insbesondere bei Mitarbeitern mit Geld-Überweisungsrechten. Alle Lösungen und Produkte der IT müssen idealerweise in die vorhandene Landschaft integrierbar sein. Nur dann funktionieren sie optimal und ihr Management ist handhabbar. Folgerichtig haben Best-of-Breed-Ansätze ausgedient und werden immer häufiger durch „Best-integrated"-Konzepte ersetzt.

Detektion und Reaktion

Nachholbedarf zeigen viele Firmen neben der Prävention aber auch bei Detektion und Reaktion, denn Hacker gehen immer ausgeklügelter vor. Zwar gibt es für jede Angriffsmethode eine technische Security-Lösung, dennoch besitzen viele Unternehmen keinen ausreichenden Schutz. Oft sind organisatorische Aspekte der Hemmschuh für eine strategische Cyber Defence. Daher ist es ratsam, Abwehrmaßnahmen in überschaubaren Teilprojekten anzugehen und alle Beteiligten von Beginn an einzubinden.

Schutz der Geschäftskontinuität

Hauptziel aller Cyber-Defence-Aktivitäten ist der Schutz der Geschäftskontinuität. Dazu müssen die IT-Welt, die Business-Welt und die reale Welt der Anwender aufeinander abgestimmt werden. Während die Mitarbeiter im Security Operations Center (SOC) die IT-Welt meist perfekt verstehen, berücksichtigen sie die Geschäftsprozesse oft nicht. Sie müssen wissen, wie die Organisation aufgestellt ist, wer zu welchen Bereichen Zugang hat und welche Dienstleister eingebunden sind. Um das begrenzte Budget zielgerichtet einzusetzen, sollten betriebliche Prozesse bekannt sein und auch, welche davon unternehmenskritisch, also besonders schützenswert sind. Cyber Defence ist also eine unternehmensweite Aufgabe. Enge Zusammenarbeit ist ihr Schlüssel zum Erfolg.

> Kein Business kann heute überleben, wenn die IT nicht sicher ist. Dazu muss die Security bei jedem IT-Projekt ganzheitlich von Anfang an mitgedacht werden.
>
> **Jan Müller**
> Director Secure Information bei Computacenter

Strategische Cyber Defence

Die Realität sieht häufig anders aus: Viele Unternehmen wissen nicht, was sie mit ihren Sicherheits-Tools erreichen wollen, gegen wen sie sich schützen möchten und wie hoch ihr präventives und detektives Schutzlevel sein soll. Dazu sollten Firmen zunächst den Status Quo ermitteln, um sich einen Gesamtüberblick zu verschaffen, Problemzonen zu kennen und auf dieser Basis gezielt Lösungen anzuschaffen. Nur so ist die Cyber Defence wirksam und die Investitionen lohnenswert.

Hilfe mit neuen Technologien und Automatisierung

Da zudem überall Fachkräfte fehlen, können langfristig neue Technologien helfen: Viele Routineaufgaben lassen sich automatisieren. Aber erst dann, wenn diese genau beschrieben und erprobt sind. Dies trifft speziell auf Cyber-Defence-Aufgaben zu, die Schritt für Schritt in eine Automatisierung überführt werden können. Machine Learning erleichtert zum Beispiel die Absicherung deutlich, da hier viele Daten in kurzer Zeit analysiert und daraus mögliche Gefahren abgeleitet werden. Angesichts der Datenflut und des Fachkräftemangels wäre dies mit Menschen gar nicht möglich.

Lösungen für das Industrial Internet of Things

Einsetzbar sind neue Technologien auch in der Industrie, wo jede Minute Stillstand Geld und Reputation kosten kann: So lassen sich zum Beispiel bei Netzwerk-Segmentierung und Zugangskontrolle die bewährten Standard-Lösungen meist mit wenig Aufwand anpassen. Auch die Anforderungen in den Bereichen Predictive Maintenance, Remote Access oder Cyber Defence unterscheiden sich nicht grundsätzlich, sondern nur im Detail. Außerdem können Lösungen zum Einsatz kommen, die im laufenden Prozess Anlagen und Geräte überwachen und im Bedarfsfall in Echtzeit alarmieren. Somit lassen sich drohende Störungen schon erkennen, bevor die Anlage ausfällt. ■

Digitalisierung – ein Zusammenspiel aus Mensch und Technik

Die digitale Transformation ist mehr als eine technische Frage. Wenn die Mitarbeiter den notwendigen Wandel aktiv mitgestalten, wird er gelingen.

Wie Studien des Bundesverbands Digitale Wirtschaft (BVDW) bestätigen, wird die digitale Transformation nur dann erfolgreich sein, wenn motivierte und qualifizierte Kollegen sich für digitale Innovationen und Veränderungen begeistern.

Wissen und Weiterbildung

Ein Thema sind dabei Fähigkeiten und Kompetenzen der Mitarbeiter. Das Zauberwort lautet peopleIT. Gerade in aufwendigen Projekten wie bei der digitalen Transformation ist es unabdingbar, dass Menschen und Technik in Einklang gebracht werden und das gesamte Team mitspielt.

Nicht zu vergessen dabei ist die Unternehmenssicherheit als kritischer Bestandteil der digitalen Transformation: Die beste Technologie reicht nicht aus, wenn die Angestellten und Führungskräfte die Wichtigkeit des Themas Informationssicherheit nicht verinnerlichen. Dafür sind Aus- und ständige Fortbildung dringend anzuraten, denn mit der umfassenderen Digitalisierung vergrößern sich auch die Angriffsmöglichkeiten durch Social Engineering, Hacker und Co.

Teams und Kompetenzen

Teambildung ist wichtig, und es braucht für Innovationen Kollegen aus den Bereichen Design, IT und Produktmanagement, die eng zusammenarbeiten und die nötigen Freiheiten haben. Vieles ist für Fachabteilungen erklärungsbedürftig und etlichen Kollegen fehlt das Verständnis gegenüber Veränderungen. Daraus können Widerstände entstehen. Ein weiteres mögliches Hindernis: Unternehmen suchen händeringend die nötigen Fachkräfte für ihre Digitalisierungsstrategie.

Der beste Rat in dieser Situation: Wenden Sie sich an kompetente Partner, die bereits Digitalisierungsprojekte durchgeführt haben und aussagekräftige Referenzen vorweisen können. Besonders sinnvoll ist es, wenn diese Partner über gute Beziehungen zu weiteren Spezialisten verfügen, die ihre eigenen Fachkompetenzen im Projektverlauf einbringen können. Dann müssen Sie sich nicht nur auf Ihre eigenen Kräfte verlassen, sondern können kompetenten Rat für peopleIT und Unternehmenssicherheit in Anspruch nehmen.

Mentaler und technischer Wandel

Vor dem technischen Wandel steht daher immer ein mentales Umdenken. Idealerweise integrieren Verantwortliche top-down ihre Mitarbeiter und Technik in ein neues Digitalisierungsvorhaben. An dieser Stelle müssen die zentralen Abteilungen IT, Fachabteilungen und Human Resources an einem Strang ziehen. ■

Geschrieben von Dominik Maaßen

Kooperation für mehr Services mit der Cloud

Wie gelingt es Unternehmen, während der digitalen Transformation den richtigen Weg in die Cloud zu finden, die neue Businesslösungen erst möglich macht – ohne Kompromisse bei der IT-Sicherheit? Einen Ansatz, ihren Kunden dafür die passende Unterstützung zu bieten, haben die Unternehmen Proservia und Maincubes gefunden und kooperieren dafür erfolgreich.

Gastbeitrag, Proservia & maincubes

FOTO: ISTOCK / RIDOFRANZ

Basis der Zusammenarbeit ist das gemeinsame Verständnis, dass IT-Sicherheit ein wesentliches Fundament aller Unternehmensteile und Projekte sein muss und eine ganzheitliche Betrachtung erfordert. Auf diese Weise werden die Partner den immer komplexeren Cyber-Angriffen als auch der erhöhten Komplexität durch hybride Landschaften, Konnektivität und Automation bei Ihren Kunden gerecht.

Mensch im Mittelpunkt

Mit über 1.000 IT-Experten alleine in Deutschland, verteilt auf über 14 Standorte, liefert Proservia bereits in einem eigenen Service-Modell individuelle Lösungen, die IT und Personalthemen kombinieren.

Als IT-Tochter des Personaldienstleisters ManpowerGroup konzentriert es sich dabei auf die Herausforderungen der digitalen Transformation, bei denen Menschen eine Rolle spielen: also am Arbeitsplatz, als Anwender von IT-Infrastrukturen und Plattformen und in der Unternehmensorganisation.

Sicheres Rechenzentrum

Maincubes wiederum stellt seinen Kunden mit je einem Rechenzentrum in Frankfurt und Amsterdam ein Netzwerk hochverfügbarer Datacenter unterschiedlicher Größe und Ausprägung in Europa zur Verfügung. Maincubes ist Teil des deutschen Immobilieninvestors und -entwicklers Art-Invest. Das Rechenzentrum von Maincubes in Frankfurt wurde ausgezeichnet mit dem Deutschen Rechenzentrumspreis und ist „Made in Germany“. Aufgrund seiner hohen Leistungsfähigkeit eignet sich das Datacenter für High Performance Computing und bietet damit beste Voraussetzungen für die heutigen Anforderungen des Marktes.

Über seine digitale Plattform secureexchange können Kunden und Partner von maincubes außerdem weltweit IT-Dienstleistungen wie IoT-, (Cyber-) Security- sowie Connectivity- und Cloud-Services zur Erweiterung ihrer Geschäftsmöglichkeiten nutzen. Maincubes-Services sind daher sicher, effizient und nutzerfreundlich – so haben Daten ein sicheres zu Hause.

Innovative Cloud-Lösungen

Dank der Kooperation der beiden Firmen erhalten die Kunden von Proservia nun Zugriff auf eine hochsichere, verfügbare und skalierbare Rechenzentrums-Infrastruktur. Sie ermöglicht zahlreiche Connectivity-Optionen über alle Cloud-Lösungen hinweg. Maincubes kann dagegen auf das breite Spektrum von IT-, Personal- und Beratungsleistungen von Proservia zurückgreifen. Die Kundenanforderungen für Cloud-Lösungen werden dabei technisch, organisatorisch sowie business-seitig betrachtet. So lassen sich praktikable Ansätze und Migrationsszenarien von Public- über Hybrid- bis hin zu individuellen Private-Clouds gestalten. ■

IT-Security mit LastPass:

Kontrolle und Komfort in einer Komplettlösung

SPONSORED

IT-Teams müssen Unternehmen heute trotz immer mehr Geräten, Gefahren und Vorschriften schützen – und das, ohne die Produktivität der Mitarbeiter zu beeinträchtigen. Modernes Identitätsmanagement braucht deshalb Lösungen für höchste Sicherheit, übersichtliche Kontrolle und einfache Bedienung.

Genau dafür bietet LastPass seine Business-Produktlinien an, ein Identity- und Access-Management-Paket, das Unternehmen jeder Größe gerecht wird. Es ist auf die zahlreichen Herausforderungen bei der Verwaltung von Zugriff und Identitäten ausgerichtet.

Mehr Flexibilität dank Single-Sign-On-(SSO)-Technologie

So können Firmen mit LastPass Enterprise immer alle Zugangspunkte sichern, denn die Lösung verfügt über Single-Sign-On-(SSO)-Technologie mit einem robusten Katalog von über 1.200 integrierten Anwendungen. Das vereinfacht nicht nur die Bereitstellung von Cloud-, mobilen, älteren und lokal installierten Anwendungen, sondern beinhaltet auch die bestehenden marktführenden Passwortmanagementfunktionen von LastPass.

Mehr Sicherheit mit Multifaktor-Authentifizierung

LastPass MFA wiederum kombiniert biometrische und kontextuelle Faktoren: Mitarbeiter bestätigen ihre Identität mit Gesicht, Fingerabdruck, Stimme oder Iris. Das Gerät verifiziert sie darüber hinaus hinter den Kulissen anhand versteckter Faktoren wie Standort oder IP-Adresse – ohne dass der Mitarbeiter ein Passwort eingeben muss. Das stellt sicher, dass die richtigen Benutzer zur richtigen Zeit und ohne zusätzliche Komplexität auf die richtigen Daten zugreifen.

Clevere Komplettlösung

LastPass Identity schließlich ist eine Kombination aus beiden: Es umfasst Passwörter, Authentifizierung und alle verwendeten Anwendungen und ermöglicht detaillierte Kontrolle und einen reibungslosen Zugriff. Mit LastPass Identity hat die IT eine ganzheitliche Sicht auf die Aktivitäten der Mitarbeiter von einem einzigen Dashboard aus.

Gerade für kleine und mittlere Unternehmen mit begrenzten Ressourcen ist es besonders wichtig, diese Art der Komplettlösung zu verwenden, die Schlüsselkomponenten kombiniert und den Nutzen der Investitionen in die Identitätstechnologie maximiert.

Verbesserter Sicherheitsstandard

Mit solchen praktischen wie etablierten Lösungen von LastPass können Unternehmen unabhängig von Größe und Ressourcen schnell und einfach eine erschwingliche, flexible Identitätslösung einsetzen – und den Sicherheitsstandard moderner Arbeitsplätze deutlich verbessern. ■

Von Gerald Beuchelt, CISO LogMeIn

Sicher mit dem Multifaktor

Unternehmen, die IT-Security auf modernen Stand bringen wollen, vertrauen auf Multifaktor-Authentifizierung als moderne Methode des Identitätsmanagements. Sie erhöht die Sicherheit erheblich – und ist bei passender Lösung für die Mitarbeiter gleichzeitig einfach zu bedienen.

Angesichts zunehmender Cyberkriminalität steht die Sicherheit der IT bei Unternehmen ganz oben auf der Agenda. Allerdings helfen die besten Firewalls oder Antivirentools nichts, wenn der Mitarbeiter durch sein Verhalten zum schwächsten Glied in der Kette wird.

Unsicherheitsfaktor Mitarbeiter

Noch immer gehören unsichere Passwörter wie „123456“ oder „Passwort“ zu den beliebtesten bei deutschen Usern. Und auch im weiteren beruflichen Umfeld warten jede Menge Fallen: Zur notorischen Passwort-Faulheit kommt hinzu, dass Mitarbeiter mobile Endgeräte geschäftlich wie privat nutzen – und das rund um die Uhr, über eine Vielzahl an Netzwerken und Standorten hinweg. Sie teilen Passwörter mit Kollegen, bringen Hunderte von Cloudanwendungen mit in die Firma oder verwenden dieselben Zugangsdaten für unterschiedliche Accounts.

Hoher Aufwand für die IT

IT-Abteilungen können angesichts solcher Risiken in den Unternehmen nur verzweifeln. Außerdem hört die Arbeit in Sachen Sicherheit nie auf – ob es um Upgrades veralteter Technologien, Kenntnisse der neuesten Bedrohungen oder effektivere Arten der Mitarbeiterschulung geht. Zudem müssen die Kollegen aus der IT zu viel wertvolle Zeit in passwortbezogene Probleme investieren.

Fakt ist: Jeder Mitarbeiter benötigt seine eigene Identität bei der Anmeldung, die richtig verwaltet werden will. Wer in der IT dafür eine passende Lösung anbieten möchte, muss Sicherheit und Benutzerfreundlichkeit unter einen Hut bekommen.

Fehlende Kontrolle und Transparenz

Zum Schutz vor Angriffen agieren deshalb bis dato viele Unternehmen mit einem einfachen Zwei-Faktoren-Authentifizierungsverfahren (2FA): Dabei wird ein einmalig verwendeter Code per E-Mail, SMS oder Telefonanruf an das Telefon oder einen Computer gesendet. Immerhin bietet die 2FA eine höhere Sicherheit als keine zusätzliche Authentifizierung. Viele Banken setzen sie bereits für Verbraucher und deren Kontonutzung ein.

Für Firmen birgt sie jedoch Einschränkungen: In der Regel handelt es sich um eine Insellösung, die sich nicht in andere Systeme integrieren lässt. Die IT verfügt damit über wenig Kontrolle und Transparenz. Und: 2FA-Lösungen können sich nicht einer Vielzahl von anderen Anwendungsfällen anpassen.

Authentifizierung mit mehreren Faktoren

Ganz im Gegensatz zur sogenannten adaptiven Multifaktor-Authentifizierung. Bei ihr wird mit Methoden der künstlichen Intelligenz überprüft, ob das Gesamtbild passt: Ist es möglich, dass der Mitarbeiter sich in Berlin einloggt und bereits zwei Stunden später von Asien aus erneut auf Daten zugreift? Ist es plausibel, dass der Computer sich in einem völlig anderen Land befindet als das zur Authentifizierung verwendete Smartphone?

Bei einer MFA wird so für jede Anmeldesituation eine intelligente Entscheidung getroffen. Denn es braucht heute neben Benutzername oder Passwort auch Faktoren wie Standort, IP-Adresse oder Geräte als wichtige Komponenten für eine sichere Legitimierung. Fingerabdruck, Stimme oder Gesicht mit ihren einzigartigen Merkmalen können ebenfalls zum Einsatz kommen. So fließt eine Vielzahl an Parametern in die Analyse ein und es entsteht ein individuelles Benutzerprofil, das Anomalien sofort erkennbar macht.

Flexibel und passgenau

Für die IT erhöht sich dadurch die Transparenz deutlich. Flexible Richtlinien für einzelne Applikationen lassen sich einfacher durchsetzen. Zugleich ist eine solche Lösung im Prinzip frei skalierbar und durch den Einsatz vorhandener Hardware kostengünstig umsetzbar. Verschiedene Faktoren zur Authentifizierung bieten mehr Flexibilität und Passgenauigkeit. Wichtig ist jedoch, dass ein MFA-System nicht isoliert arbeitet, sondern sich nahtlos in eine bestehende Infrastruktur einbinden lässt.

Mehr Akzeptanz

Vorteil wiederum für den Mitarbeiter: Auf einem wesentlich höheren Sicherheitsniveau profitiert er trotzdem von einer natürlichen und einfachen Anmeldung. Management von IT-Sicherheit bedeutet nämlich auch Changemanagement. Wichtig ist bei der Einführung, dass Mitarbeiter der Lösung offen gegenüberstehen und lernen, damit effektiv und selbstverständlich umzugehen.

Mit einer benutzerfreundlichen Lösung, die sich an die Arbeitsweisen der Mitarbeiter und die Rahmenbedingungen des Unternehmens anpasst, steigen so die Akzeptanz und das Sicherheitsniveau. Eine flexible und adaptive MFA-Lösung ist damit ein strategisch wichtiges Element einer modernen Security-Landschaft. ■

Geschrieben von Dominik Maaßen

„Umso mehr ich mich mit Sicherheit befasse, umso weniger Angst habe ich vor Risiken“

In unserer digitalen Welt haben mehr und mehr Geräte eine Internetschnittstelle und sind vernetzt. Doch wie sicher sind wir im Internet? Philipp Kalweit ist einer der begehrtesten Auftrags-Hacker. Der junge Hannoveraner berät Banken, Regierungsbehörden und internationale Unternehmen im Thema IT-Sicherheit. Im Gespräch blickt er auf sein Verständnis von Sicherheit und wie wir mit IT-Sicherheit bewusst umgehen sollten.

Womit assoziierst du den Begriff Sicherheit?
Wenn ich an Sicherheit denke, denke ich an Risiken. Sicherheit gibt es dort wo es Risiken gibt und gerade, weil es Sicherheit gibt, gibt es immer weniger Risiken. Wenn ich Sicherheiten habe, muss ich mir keine Sorgen um Risiken machen.

Hat sich deine Wahrnehmung vom Thema Sicherheit durch deine bisherigen Erfahrungen geändert?
Definitiv, ja. Ich merke immer wieder, dass Menschen, die vielleicht nicht so bewandert mit dem Thema IT sind und dementsprechend Risiken und Sorgen nicht einschätzen können, eine größere Unsicherheit in dem Bereich haben. Fehlinformationen oder Gerüchte bekommen eine wachsende Relevanz, da diese dann nicht fundiert bewertet werden können. Umso mehr ich mich mit dem Themenfeld befasse, umso weniger ist die Angst vor Risiken vorhanden.

Wird man selber immer vorsichtiger, wenn man im Beruf die Sicherheit von Kunden sicherstellen möchte?
Ganz im Gegenteil. Man schätzt Risiken ganz anders ein und bewertet sie meistens nicht so kritisch. Sicherheit ist relativ. Es bedarf sie überall dort, wo es Risiken gibt. Umso größer diese dann sind, umso höher muss der Sicherheitsstandard sein. Die Sicherheit ist dynamisch genau wie das Risiko selbst. Die meisten Menschen können Risiken und Sicherheit nicht so gut einschätzen und tendieren daher dazu, die Sicherheit zu übertreiben.

Wird IT-Sicherheit im privaten Umfeld zu wenig hinterfragt?
Ja, wir leben in einer Welt, in der Digitalisierung jeden Bereich in unserem Leben betrifft. Man kann nirgendwo mehr klar zwischen analog und digital unterscheiden. Auch analoge Dinge gehen, selbst wenn passiv, mittelbar mit IT und damit auch IT-Sicherheit einher. Allerdings dauert gesellschaftlicher Wandel sehr lange. Werden neue Technologien auf den Markt geworfen, werden sie schnell verbreitet. Allerdings dauert es deutlich länger diese Dinge in seine Ideologie zu implementieren und sich in der Gesellschaft auf die neuen Möglichkeiten einzustellen. Wir nutzen Dinge, auf die wir in der Gesellschaft noch nicht vorbereitet sind. Der aktuelle Stand in der Technologie ist interessant. Wir können jetzt nicht sagen, was in Zukunft sein wird. Wir sollten eine Datensparsamkeit in unserem Verhalten implementieren.

Beim Thema Smartphone beispielsweise wird Herstellern augenscheinlich sehr vertraut, dass diese sichere Produkte bereitstellen. Ist man dort oft zu naiv?
Sicherheit basiert auf Vertrauen. Wenn ein Hersteller Sicherheit verspricht, kann man Vertrauen haben und dadurch Sicherheit aufbauen. Oder man hinterfragt diese Versprechen. Da kommt es auf Medienkompetenz an. Eigentlich ist Sicherheit wenig komplex. Sie basiert auf Grundbausteinen. Beispiel Passwörter: Es gibt unzählige Thesen dazu, was ein sicherer Umgang mit Passwörtern ist. Nimmt man sich einen einfach Satz und nimmt nur die Anfangsbuchstaben in Groß- und Kleinschreibung und die Zahlen als Passwort, ist das eine gute Grundlage. Ein anderes Sicherheitsrisiko sind Updates. Werden Updates nicht ausgeführt, werden die Angriffsvektoren nicht mehr geschlossen.

Wie wird Sicherheit in der Zukunft definiert werden?
Die Globalisierung fördert die Vernetzung. Blicken wir auf Technologien wie Smart Home. Alles ist über kurz oder lang gesehen digital miteinander vernetzt. So haben immer mehr Geräte Internetschnittstellen. Dadurch, dass IoT Designs über keine Updates verfügen, ist hier grundsätzlich Gefahrenpotenzial vorhanden. Die zunehmenden, gesammelten Datensätze werden dann interessant, sobald sie effektiv mit Gewinnpotenzial verkauft werden können. Dann ziehen Unternehmen daraus ihre Vorteile. So ist der Datenüberfluss, genau wie IoT, Fluch und Segen zugleich. Die beste Vorbereitung darauf ist Verhaltensänderung. Wir müssen andere Anforderungen an Geräte aufbauen. Gute Kamera oder viel Speicherplatz dürfen nicht wichtiger sein als eine langfristig abgesicherte Update-Verfügbarkeit. Es muss eine gewisse digitale Mündigkeit vorherrschen. Wenn man reflexiv mit den Daten und Medien umgeht, berücksichtige ich automatisch auch die Sicherheitsaspekte. ■

Geschrieben von Lukas Knochel

SPONSORED

Marc Thamm
Underwriting Manager Technology, Media & Communications, Hiscox Deutschland

Digitalisierung muss für alle Beteiligten sicher sein

■ Alle reden von der Digitalisierung, aber nur selten von den Gefahren. Die kennen Sie als Spezialist für IT-Versicherungen sicher am besten. Können Sie uns ein paar aufzeigen?
Eine entwickelte Software ist zum Beispiel fehlerhaft und deshalb steht der Betrieb des Kunden still. Daten gehen bei einer Datenbankmigration verloren. Oder beim Hosting eines Onlineshops kommt es zu einem mehrtägigen Ausfall aufgrund einer Attacke und die zugesagten Erreichbarkeiten werden nicht eingehalten. In diesen Fällen und vielen anderen sind zum Beispiel Nutzungsausfall, Mehrkosten und daher hohe Schadenersatzforderungen möglich. Nicht zuletzt, weil Probleme heute unmittelbar einen sichtbaren Schaden verursachen.

■ Sie haben zusammen mit Bitkom Research rund um dieses Thema mehr als 300 IT-Verantwortliche aus deutschen IT-Dienstleistungsunternehmen in einer Studie befragt. Was hat sie ergeben?
Die Hälfte der IT-Dienstleister hält digitale Risiken für nicht kalkulierbar. Es gibt viel Unsicherheit zu Haftungsfragen, wenn Fehler passieren. Auch Cyber-Gefahren sind ein großes Thema. Gleichzeitig setzen Auftraggeber voraus, dass sich IT-Dienstleister entsprechend absichern. 75 Prozent der befragten Dienstleister geben an, dass ihre Auftraggeber einen Nachweis über eine IT-Berufshaftpflicht fordern. Es herrscht Verunsicherung. Die Auftragszahlen der externen IT-Spezialisten wachsen mit der stetig steigenden Zahl der Digitalisierungsprojekte. Auf der anderen Seite fürchten Freiberufler genauso wie KMU Risiken und Fehler, die sie in ihrer Existenz bedrohen. Die Digitalisierung kann in Deutschland aber nur erfolgreich voranschreiten, wenn sich Auftraggeber wie Auftragnehmer von IT-Projekten sicher sein können, dass die digitalen Risiken abgesichert und somit beherrschbar sind.

■ Die Frage nach der passenden Lösung liegt nahe – welche bietet Hiscox an?
Unsere Lösung Net IT by Hiscox ist speziell auf die besonderen Risiken der IT-Branche ausgerichtet. Die Versicherungsleistungen mit IT-Haftpflichtkomponenten, Cyber- und Sachdeckung sind flexibel kombinierbar. Alle Komponenten vereint decken mit passendem Rundumschutz die branchentypischen Risiken ab. Dank offener Deckung sind alle in der IT- und Telekommunikations-Branche üblichen aktuellen und zukünftigen Tätigkeiten automatisch versichert. Unsere Versicherten brauchen daher nicht kontinuierlich überprüfen, ob sie ihre Versicherung anpassen müssen. ■

Gerald Beuchelt
CISO von LogMeIn/LastPass

Je höher die Akzeptanz, desto besser die IT-Security

■ Mitarbeiter gelten als Schwachstelle der IT-Sicherheit. Woran liegt das?
Ein Beispiel sind schwache und wiederverwendete Passwörter. Sie sind einer der Hauptgründe, warum es immer wieder zu Datenschutzverletzungen kommt. Dabei stehen sich die Nutzer selbst im Weg – sei es im privaten wie im beruflichen Umfeld. Eine Umfrage von LastPass zeigte, dass 59 Prozent der User aus Angst, ihr Passwort zu vergessen, meistens dasselbe oder ein leicht abgeändertes verwenden. Wenn man bedenkt, dass ein Nutzer im Durchschnitt über 100 Konten besitzt und immer wieder dasselbe Passwort nutzt, ist klar, worauf das hinausläuft: Einmal geknackt, stehen den Cyberkriminellen alle Konten offen.

■ Wie kann man das in Firmen ändern?
Neben den technischen Tools braucht es ein entsprechendes Bewusstsein. Mitarbeiter müssen wissen, dass sie selbst im Mittelpunkt der Entwicklung eines Sicherheitsprogramms stehen. Aber sie müssen auch bereit sein, sich auf Veränderungen einzulassen.

■ Welche Erwartungen haben denn die Mitarbeiter und wie holt man sie dabei ab?
Für die Mitarbeiter sollten die Vorteile eines sicheren Umgangs mit Daten für die eigene Arbeit klar erkennbar sein, so dass sie freiwillig mitmachen. Je höher die Akzeptanz bei den Mitarbeitern, desto besser ist die IT-Security. Benutzererfahrung geht hier über alles. Generell wollen sie ein reibungsloses Nutzungserlebnis, das der täglichen Arbeit nicht im Weg steht. Von Apps bis hin zu Web-Logins sollte alles an einem Ort zugänglich sein. Ideal ist die Echtzeitsynchronisation zwischen allen Devices. Denn die Mitarbeiter wollen nicht zwischen verschiedenen Sicherheitslösungen hin- und herwechseln. Berufliche und private Konten sollten entsprechend von überall zugänglich sein.

Teams wiederum wollen Apps flexibel und sicher gemeinsam nutzen, ohne dass die IT Einbußen bei der Rechenschaftspflicht oder Sicherheit in Kauf nimmt. Dann lassen sich zum Beispiel Zugangsdaten sicher und flexibel für andere freigeben und Konten gemeinsam nutzbar machen.

Praktisch ist dabei natürlich immer nur ein Passwort. Bei LastPass können sich Mitarbeiter dafür mit ihren Active-Directory-Zugangsdaten anmelden. Danach überlassen sie LastPass das Erstellen langer Passwörter, sodass jeder Dienst mit einem anderen starken Passwort geschützt ist. Idealerweise braucht es für alle diese Services auch keine internen Schulungen oder externe Dienstleistungen. ■

Sven Meise
CDO/COO, Francotyp-Postalia

Das Gateway für die sichere, digitale Kommunikation

■ Während sich das Internet of Things (IoT) stärker an Endkunden orientiert, kommt das Industrial Internet of Things (IIoT) in der Industrie zum Einsatz. Was ist bei letzterem entscheidend?
Der Datenpool eines privaten Nutzers ist vergleichsweise überschaubar. Sensoren von Industrieanlagen erfassen kontinuierlich riesige Datenmengen verschiedener Maschinen. Sie sind empfindlicher und präziser. Für eine Erfassung müssen die Daten zu lesen und zu vereinheitlichen sein. Unternehmen können auf Basis der Daten Prozesse optimieren, Energie und Kosten sparen und ressourcenschonender sowie zukunftsorientierter produzieren.

■ Diese sensiblen Daten sind leider bei kriminellen Hackern heiß begehrt. Wie können sich Unternehmen schützen?
Um Hackerangriffe zu verhindern, müssen Unternehmen die Daten ihrer Industrieanlagen verschlüsseln, wenn sie sie in die Cloud übermitteln. Dies ist mithilfe von entsprechenden Gateways möglich. Sie regeln die Datenkommunikation der Industrieanlagen mit der Cloud und sichern die Automatisierungssteuerungen vor unautorisierten Zugriffen. Wir bieten dafür eine komfortable End-to-End-IoT-Lösung. Sie wird den hohen Sicherheitsanforderungen industrieller Unternehmen gerecht und stellt Authentizität sowie Integrität der übertragenen Daten sicher.

■ Nicht alle Industrieanlagen sind auf solche Sicherheitsanforderungen von IIoT angelegt, vor allem kleine und mittelständische Unternehmen. Wie können Firmen dennoch passend reagieren?
Für die Nachrüstung und Modernisierung haben wir mit unserer Beteiligung Juconn eine sichere Gesamtlösung entwickelt. Sie verbindet hochsicher dezentrale Anlagen, insbesondere solche mit alten Steuerungen. Das IoT-Gateway von FP erfasst dabei die Daten von Steuerungsanlagen und Außenstationen und überträgt sie hochsicher an die IoT-Cloud-Plattform von Juconn. Diese wertet die Daten aus und visualisiert sie in einem Dashboard, welches die Kunden via Computer, Tablet oder Smartphone einsehen können und stellt sie nachgelagerten Systemen zur Verfügung. Somit können Kunden alle Daten ihrer Steuerungsanlagen zu jedem Zeitpunkt unkompliziert überwachen und auswerten.

■ Können Sie ein Beispiel geben, wie Ihre Technologie erfolgreich bei Kunden zum Einsatz kommt?
Unsere IoT-Gateways bieten mit ihren modularen Sicherheitsoptionen beispielsweise viele Vorteile in der reibungslosen Energieversorgung. Sie überwachen dezentrale Außenstationen und verbinden diese abgesichert mit der Zentrale. Störmeldungen werden in Sekunden übermittelt, bevor sie für Ausfälle sorgen. Der gesamte Prozess der Energieversorgung wird also schnell, transparent, effizient und sicher. ■

Wie die Digitalisierung die Versicherungs-branche verändert

Geschrieben von Hanna Bachmann

Versicherungen sind aus unserem Alltag nicht mehr wegzudenken. Kaum ein deutscher Bundesbürger hat nicht mindestens eine Versicherung. Doch Digitalisierung und Generationenwandel stellen auch diese Branche vor neue Herausforderungen und zwingen sie zum Umdenken. Eine Anpassung an die neuen Bedürfnisse einer digitalen Gesellschaft versprechen sogenannte InsurTechs, die mithilfe von technischen Lösungen komplexe Versicherungsprodukte und Abschlussstrecken vereinfachen und kundenfreundlicher gestalten wollen.

Hanna Bachmann
Sprecherin InsurTech-Plattform des Bundesverband Deutsche Startups e.V.

Traditionelle Versicherungspolicen bedienen hauptsächlich klassische Rollenmuster und konservative Lebenskonzepte. Im Zuge des digitalen Wandels kann der Kunde von heute sein Leben jedoch individuell gestalten. Verbraucher schätzen die Vorteile des Onlineshoppings: die unendliche Auswahl, 24/7-Verfügbarkeit und die Möglichkeit einer Bestellung ganz bequem von zu Hause aus. Die Definition von Zielgruppen anhand demografischer Merkmale funktioniert in einer globalisierten Welt mit schier grenzenlosen alternativen Lebenskonzepten nicht mehr. Stattdessen bieten InsurTechs situative Versicherungslösungen, die zu der jeweiligen Lebenssituation des Kunden passen. Hierzu zählen zum Beispiel flexible Vertragslaufzeiten und Versicherungsbausteine, mit denen sich eine Police individuell zusammensetzen lässt.

So kann beispielsweise eine Familie für einen siebentägigen Skiurlaub eine Unfallversicherung für jedes Familienmitglied abschließen und gleichzeitig eine Police gegen Beschädigung und Diebstahl für die Skier oder das Snowboard – genau für die sieben Tage der Reise. Der Vorteil: Der Schutz endet automatisch, die Familie muss nur für die Zeit bezahlen, in der die Versicherung tatsächlich benötigt wird. Eine weitere Möglichkeit, die speziell auf die „Generation Netflix" angepasst wurde, ist die Versicherung im Abo. Kunden können hier die Absicherung für ihr Smartphone oder Fahrrad monatlich kündigen – so, wie sie es von Streaming-Anbietern bereits gewohnt sind.

Auch neue Businessmodelle und Technologien verändern den Alltag des Kunden enorm und bergen neue Risiken, die es abzusichern gilt. Statt zu kaufen, setzt der Kunde vermehrt auf sogenannte Sharing-Anbieter. Sharing Economy und Smart Home sind nur zwei Begriffe, die diese neuen Bedürfnisse untermauern. Hierdurch werden wiederum ganz neue Versicherungslösungen erforderlich, wie etwa Peer-to-Peer-Versicherungen. Auch der Einsatz neuer Technologien und Gadgets, etwa für Smart Homes, setzt besonders in den Bereichen Sachversicherungen und Cybersicherheit neue Lösungsansätze voraus, um den Kunden adäquat gegen Schäden zu schützen.

InsurTechs weltweit haben sich darauf spezialisiert, die Versicherungsbranche an die neuen Bedürfnisse in Zeiten der Globalisierung anzupassen. ■

VERANSTALTUNG

it-sa 2019 – Trends & Innovationen der IT-Securitybranche
8. – 10. Oktober 2019, Messezentrum Nürnberg

Internet-Security-Days (ISDs) des eco – Verband der Internetwirtschaft e. V.
26. und 27. September in Köln

DKM 2019: Treffpunkt der Finanz- und Versicherungsprofis
Vom **22.-24. Oktober** ist die DKM Treffpunkt der Finanz- und Versicherungsbranche. Über 320 Aussteller, mehr als 310 Referenten sowie ein Netzwerk mit über 17.000 Profis zeichnen die Leitmesse aus.

Payment Summit – The Future of Payment in Retail
Strategisches und praxisrelevantes Payment-Wissen für Händler

06.-07. November 2019, Hamburg

Sichern Sie sich jetzt Sonderkonditionen mit dem Ticketcode: PaySum19MP

Mehr Infos und Tickets unter: www.payment-summit.de

Mobile in Retail
Mobile in Retail – Der Digital-Kongress für Retail, Brands und Finance

29.-30. Oktober 2019, Berlin

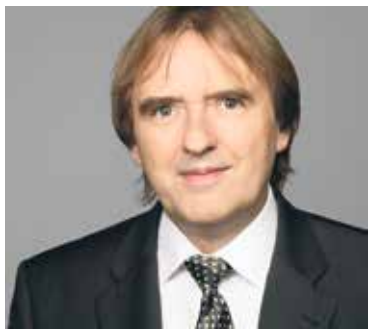
IT-Sicherheit

Die IT und das Internet sind aus unserem Leben nicht mehr wegzudenken! Surfen, E-Mails, WhatsApp, Onlinebanking und soziale Netzwerke wie Xing, Facebook, Instagram, Twitter usw. gehören zum Alltag. Im Rahmen der Digitalisierung werden Prozesse des Berufs- und Privatlebens zunehmend ins Internet verlagert. Die Risiken, die dabei entstehen, sind vielen jedoch unbekannt.

Damit bei der Übertragung von sensiblen Daten, wie beim Online-Shopping oder beim Online-Banking, keiner zum Beispiel Kreditkartenummer oder Zugangsdaten mitlesen kann, benötigen diese Informationen einen besonderen Schutz während der Übertragung. Die Kommunikation im Internet sollte immer verschlüsselt umgesetzt werden. Dies wird daran erkannt, dass die Web-Adresse mit „https“ statt mit „http“ beginnt und an dem kleinen Schlosssymbol in der Statusleiste des Browsers. Die Stärke der Verschlüsselung, die beim Doppelklick auf das Symbol angezeigt wird, sollte mindestens 128 bit betragen.

Nutzung mobiler Geräte

Die Vorteile von mobilen Geräten, wie Smartphones und Tablets, sind bestechend: Über die vielfältigen Schnittstellen (WLAN, Bluetooth, NFC) ist das Internet mit seinen Diensten stets und überall verfügbar. Dadurch ergeben sich auch zusätzliche Angriffsvektoren: Ständig wechselnde, unsichere Umgebungen (Flughäfen, Cafés) erhöhen die Wahrscheinlichkeit des unabsichtlichen Verlustes und des gezielten Diebstahls. Die Gefahr einer Bewegungsprofilbildung ist zu berücksichtigen und die einfache Möglichkeit, in der Öffentlichkeit Einsicht zu nehmen, ist nicht zu unterschätzen. Die Bedrohung von Apps, die Daten auslesen, wird durch das Prinzip „Masse statt Klasse“ und unseriöse App-Stores real. Aber auch die Nutzung von manipulierten Hotspots wird durch ein „schnelles E-Mail-checken“ immer häufiger zum Angriffspunkt, der großen Schaden anrichten kann. Eine Gefahrenquelle für Unternehmen ist die parallele Nutzung von mobilen Geräten für private und berufliche Zwecke, denn die meisten Smartphones werden für den Verbrauchermarkt erstellt. Hier wird von den Anbietern die Strategie verfolgt: Die mobilen Geräte müssen für jeden Nutzer leicht verständlich sein. Von Beginn an sind alle Funktionen zugänglich, möchte der Nutzer mehr Sicherheit, muss er Einschränkungen eigenständig vornehmen – das kann er aber meistens gar nicht. Eine sichere Strategie für Smartphones wäre daher: Es funktioniert erst mal gar nichts und der Nutzer muss die Funktionen, die er für die Erledigung seiner Aufgaben zwingend braucht, freischalten. Dadurch würde die Angriffsfläche auf mobilen Geräten deutlich reduziert!



Prof. Dr. Norbert Pohlmann
Leiter Institut für Internet-Sicherheit

Vorsicht bei Spam-Mails!

Unerwünschte Werbe-E-Mails, auch Spam genannt, sind nicht nur nervig, sondern können auch gefährlich werden. Viele E-Mails mit Dateianhang enthalten nämlich Schadprogramme. Es ist wichtig, Dateianhänge nur mit Bedacht zu öffnen, auch bei seriöser Quelle, da der Absender leicht gefälscht werden kann. Bei Unsicherheiten, ob die E-Mail vom richtigen Sender kommt, lieber telefonisch Rückfrage halten! Niemals unbekannte, seltsame oder verlockende Anhänge öffnen! Anwälte versenden keine Abmahnungen/Rechnungen per E-Mail oder Banken fragen nie nach Zugangsdaten per E-Mail, usw.

Zwei-Faktor-Authentifizierung und sichere Passwörter!

Verwenden Sie bei sicherheitskritischen Anwendungen, wie dem Onlineshop oder dem E-Mail-Account immer eine Zwei-Faktor-Authentifizierung. Wenn ein Faktor das Passwort ist, dann muss es sicher sein! Ein sicheres Passwort besteht aus mindestens zehn Zeichen, darunter eine Mischung aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen. Es ist auf den ersten Blick sinnfrei, steht nicht im Lexikon und hat nichts mit dem persönlichen Umfeld zu tun (Namen, Geburtsdaten etc.). Ganz wichtig: Für jeden Dienst muss ein anderes Passwort verwendet werden! Um den Überblick nicht zu verlieren, empfiehlt sich die Verwendung eines digitalen Passwort-Managers. Einige Produkte wie „Keepass“ oder „Password Safe“ können im Internet kostenfrei heruntergeladen werden. Mit diesen Programmen können die Vielzahl der Nutzernamen und Passwörtern verschlüsselt auf dem Endsystem gespeichert werden.

Übersicht: Passwort-Verfahren

Wer sich für Konzepte, Prinzipien, Architekturen von Cyber-Sicherheitssystemen in der Digitalisierung interessiert, sollte sich das Lehrbuch „Cyber-Sicherheit“ genauer ansehen: https://norbert-pohlmann.com/cyber-sicherheit/ ■

Geschrieben von Norbert Pohlmann

Engagierte Wächter

Geschrieben von Heiko Mehrens, Barrington Consulting GmbH

SPONSORED

BARRINGTON CONSULTING

Unternehmen, die sich in ihrer IT sicher aufstellen wollen, stehen vor zahlreichen Herausforderungen: Selbst die besten und hoch angepriesenen Lösungen auf dem Markt können keine hundertprozentige Sicherheit bieten. Dafür sind die Angriffsflächen in Komplexität und Wechselwirkung inzwischen zu groß.

Auch moderne Monitoringsysteme, die mit künstlicher Intelligenz hinterlegt sind, können nicht alle Attacken und Anomalien erfassen. Kleinen Firmen fehlen dafür die Budgets, große Unternehmen müssen aufgrund des Aufwands entsprechende Mitarbeiterkapazitäten vorhalten, bei gleichzeitigem aktuellen Fachkräftemangel.

So umfassender und tiefer integrierte Sicherheitskonzepte sind, nie ist der Personalaufwand zu vernachlässigen, sie umfassend zu betreiben.

Ein ganz pragmatischer Ansatz für dieses Problem ist Security-Awareness: Denn das beste Konzept ist nur so gut, wie es täglich umgesetzt wird. Gerade Angestellte können sich als gefährlichste Sicherheitslücke erweisen, auf der anderen Seite aber die besten Gatekeeper sein. Mit Schulungsmaßnahmen lernen sie, die verschiedenen Sicherheitsbedrohungen während der Arbeit zu erkennen und richtig mit ihnen umzugehen. Sie entwickeln so mehr Verständnis für Daten und IT-Infrastrukturen. Mögliche Themen sind dann der sichere Umgang mit E-Mails, mit mobilen Geräten und Zugriffsrechte entsprechend ihrer Unternehmensrolle. Sinnvoll ist auch, die DSGVO nicht als lästige Gesetzespflicht zu betrachten, sondern viele ihrer Punkte als sinnvoller Vorschlag für richtiges Verhalten.

Entscheidend sind außerdem Schulungen, die nicht standardisiert nach Gießkannenprinzip funktionieren. Relevant ist stattdessen eine Problemanalyse in den einzelnen Abteilungen, die im späteren Training den Bedürfnissen und dem unterschiedlichen Kenntnisstand gerecht wird. Awareness bedeutet Bewusstsein, aber auch Verständnis: Also keine Horrorszenarien aufbauen, sondern Technik und Zusammenhänge am besten so einfach erklären, dass es selbst ein Grundschüler versteht. Erst dann macht die Investition in Sicherheitstechnik Sinn und der Mitarbeiter versteht sich als engagierter Wächter gegen jede digitale Attacke. ■

Dr. Harald Olschok
Hauptgeschäftsführer Bundesverband
der Sicherheitswirtschaft

Sicherheitsarchitektur im Wandel

Deutschland ist nach wie vor eines der sichersten Länder der Welt. Dazu tragen auch die privaten Sicherheitsunternehmen mit ihren rund 265.000 Mitarbeiterinnen und Mitarbeitern wesentlich bei. Sie sind zu einem festen Bestandteil der Sicherheitsarchitektur geworden. Bis vor wenigen Jahren waren die Beschäftigten für die Öffentlichkeit weitgehend „unsichtbar“, weil sie weit überwiegend im Hausrechtsbereich der Auftraggeber eingesetzt waren. Das hat sich stark verändert. Der Schutz von Veranstaltungen, der Einsatz als „City-Streifen“ im privaten oder kommunalen Auftrag, die Begleitung des Öffentlichen Personenverkehrs (ÖPV), Fluggastkontrollen an Verkehrsflughäfen, der Schutz von Universitätsgeländen und Schulen, Friedhöfen, Schwimmbädern im Sommer und Weihnachtsmärkten im Winter haben stark zugenommen. Die Branche agiert immer mehr in öffentlichen Räumen. Dies hat seine Ursache auch darin, dass die Polizei in einer freiheitlichen Gesellschaft nicht in der Lage ist, die Sicherheit jedes Einzelnen und seines Eigentums überall und flächendeckend zu gewährleisten. Gefahren für die Wirtschaft und Gesellschaft drohen unter anderem durch Kriminalität, Terrorismus, Extremismus, kriegerische Konflikte, Spionage und Sabotagehandlungen, Cyberangriffe, Feuer- und Wasserschäden und zunehmend auch durch Klimaveränderungen. Diese Herausforderungen erfordern eine optimale Kombination von Sicherheitsdienstleistungen und moderner Sicherheitstechnik. Videoüberwachungstechnik wird immer leistungsfähiger. Im Brandschutz gibt es hochsensible Früherkennungssensoren für Rauchentwicklung und Brandlokalisierung. In der Zutrittskontrolle steigt die Leistungsfähigkeit von biometrischen Erkennungsverfahren. „Integrierte Sicherheitslösungen“ werden immer wichtiger. Damit steigen auch die Anforderungen an die Qualifikation der Beschäftigten. ■

Geschrieben von Paul Howe

200.000 Brände pro Jahr – viele können vermieden werden

Im Interview spricht Feuerwehrmann Hartmut Ziebs über den richtigen Brandschutz im Haushalt.

Hartmut Ziebs
Präsident des Deutschen
Feuerwehrverbands
FOTO: KATRIN NEUHAUSER/DFV

■ Wie viele Brände gibt es in deutschen Haushalten durchschnittlich pro Jahr und wodurch werden diese meist verursacht?
Die freiwilligen Feuerwehren, Berufsfeuerwehren und Werkfeuerwehren werden im Jahr bei rund 200.000 Bränden und Explosionen tätig – vom Wohnungsbrand über den brennenden Mülleimer bis hin zur Explosion in der Lagerhalle. Wie viele davon in Haushalten sind, ist statistisch nicht erfasst. Zumeist entstehen Brände durch Unachtsamkeit, falsches Verhalten und technische Defekte.

■ Was halten Sie von der Rauchmelderpflicht?
Wir freuen uns sehr darüber, dass unsere jahrelangen Bemühungen zur bundesweiten Umsetzung der Rauchwarnmelderpflicht von Erfolg gekrönt wurden. Die genaue Umsetzung ist jeweils in der Landesbauordnung geregelt. Eine Übersicht und wichtige Tipps zu Installation und Wartung gibt es unter www.rauchmelder-lebensretter.de. Dort gibt es auch Hinweise zum Label „Q“, mit dem das Qualitätsniveau der Rauchwarnmelder am Markt verbessert wird.

■ Wie kann man die Brandgefahr in den eigenen vier Wänden minimieren?
Installieren Sie Rauchmelder in Ihrer Wohnung. Lassen Sie technische Anlagen (Kamin, Therme) warten. Verwenden Sie nur geprüfte Materialien (zum Beispiel bei Mehrfachsteckdosen, Lichterketten et cetera). Überlasten Sie Steckdosen nicht. Schalten Sie nicht benutzte Geräte aus – das spart auch Strom. Passen Sie im Umgang mit offenem Feuer (Kerzen, Ofen) auf; vor allem, wenn Kinder oder Haustiere im Haushalt sind.

■ Welche Gefahren gehen von Kohlenstoffmonoxid aus?
Kohlenstoffmonoxid ist ein gefährliches Atemgift, das man nicht sehen, riechen oder schmecken kann. Betroffene bemerken nicht, wenn sie Kohlenmonoxid einatmen, denn es gibt keine typischen Symptome wie Husten oder Atemnot. Darüber hinaus kann das Gas mühelos durch Wände oder Fußböden dringen, sodass es auch in Räumen auftritt, in denen sich keine potenzielle CO-Gefahrenquelle befindet. Alle Faktoren zusammengenommen machen CO so heimtückisch. Abhängig von der Konzentration in der Raumluft kann eine Kohlenmonoxidvergiftung zu erheblichen Beschwerden, Bewusstlosigkeit und zu massiven gesundheitlichen Spätfolgen bis hin zum Tod führen.

■ Wie verhält man sich in einem Brandfall?
Überlegen Sie bereits vorher, was Sie im Falle eines Brandes tun: Wenn es ohne Eigengefährdung möglich ist, Löschversuche unternehmen (zum Beispiel Feuerlöschspray oder Feuerlöscher; vorher mit Standort und Bedienung vertraut machen!). Wenn es nicht ohne Gefahr möglich ist und sich der Brand ausbreitet: Andere Menschen informieren (vor allem Kinder, bewegungseingeschränkte Personen!), gemeinsam Räume verlassen und Tür schließen. Wenn es in der Wohnung brennt: Bei der Flucht das Treppenhaus nutzen, NIE den Aufzug! Wenn es im Treppenraum brennt: In der Wohnung bleiben, Türen schließen, am Fenster die Feuerwehr aufmerksam machen. Feuerwehr über kostenfreien Notruf 112 alarmieren – das funktioniert in ganz Europa. Wo bin ich, was ist passiert – diese Informationen fragen die Menschen am Notrufplatz ab. Nicht selbst auflegen, sondern auf Rückfragen warten! Feuerwehr erwarten, nicht eigenständig wieder in Gefahr begeben. Wenn möglich Haustürschlüssel mitnehmen, dann kann die Feuerwehr damit die Tür öffnen.

■ Die Feuerwehr wird klassischerweise bei Feuer gerufen. Bei welchen Notfällen sollte man zudem die 112 wählen?
Die Feuerwehr ist für Brand- und Katastrophenschutz und technische Hilfe zuständig, teils auch im Rettungsdienst unterwegs. Also, bei einem Verkehrsunfall mit oder ohne Verletzten, einem umgefallenen Baum, von dem weitere Gefahr ausgeht (auf Straße, auf Haus), bei nicht beherrschbarem Wassereinbruch im Keller oder in der Wohnung, bei einer verletzten oder akut lebensbedrohlich erkrankten Person: 112 rufen!

Geschrieben von Silvia Darmstädter

Lange Nase für Langfinger

Wer Einbrechern ein Schnippchen schlagen will, setzt ein paar Tipps um, über die wir mit Jens Fritsch, Kriminalhauptkommissar und Fachberater bei der Beratungsstelle Einbruchschutz beim LKA Berlin, gesprochen haben.

Geschrieben von Dominik Maaßen

■ Können Sie uns zu Beginn einen aktuellen Überblick über die Einbruchstatistiken in Deutschland geben?
Wenn wir über private Wohnraumeinbrüche reden, die der Polizei gemeldet werden, lagen die Zahlen bundesweit im Jahr 2006 bei rund 100.000 Einbrüchen. Sie stiegen 2015 auf den Höchststand von knapp 170.000. Seit 2015 gibt es jedoch wieder einen kontinuierlichen Rückgang runter auf unter 100.000.

■ Kennen Sie die Gründe für diesen rapiden Rückgang?
Da gibt es ein ganzes Bündel. Es gab eine Gesetzesverschärfung und Einbrecher haben inzwischen ein größeres Risiko, dass der Richter sie mit Gefängnis bestraft. Das schreckt viele ab. Die Bundesregierung hat den Einbruchschutz massiv gefördert. Generell sind mehr Menschen bereit, sich darüber zu informieren und in Sicherheit zu investieren. Die Polizei berät bundesweit. Hier in Berlin arbeiten Staatsanwaltschaft und Polizei enger und mit mehr Manpower zusammen. Hinzu kommen neue Konzepte des Predictive Policing mit Vorhersage-Software, die Prognosen für wahrscheinliche Einbruchsorte gibt. Die Polizei hat außerdem mehr reisende Täter festgenommen. Für viele ist es inzwischen lukrativer, in anderen Ländern einzubrechen.

Jens Fritsch
Kriminalhauptkommissar und Fachberater bei der Beratungsstelle Einbruchschutz beim LKA Berlin

Tatsächlich gibt es einen Anstieg von Einbrüchen in den Wintermonaten.

■ Es wird Herbst und der Winter steht vor der Tür. Steigt nun auch wieder die Häufigkeit an Einbrüchen?
Tatsächlich gibt es einen Anstieg von Einbrüchen in den Wintermonaten. In den dunklen Jahreszeiten werden Sie als Einbrecher nicht so schnell gesehen. Im Sommer befinden sich Menschen meistens draußen auf der Terrasse oder im Garten. Auch Nachbarn würden dann Verdächtige schneller bemerken. Einbrecher wollen niemanden antreffen und suchen deshalb leere Häuser, die nicht beleuchtet sind. Drei dunkle Häuser nebeneinander in einer Straße sind für die wie ein Sechser im Lotto. Denn dann sind sehr wahrscheinlich auch die Nachbarn nicht anwesend.

■ Welche Stellen am Haus oder der Wohnung sind besonders gefährdet?
Täter agieren ungern auf dem Präsentierteller. Ihre Angriffsfläche ist meistens die Rückseite des Hauses, also die Deckung. Die ist von Fußgängern, Autofahrern oder gegenüber wohnenden Nachbarn nicht zu sehen. Auch Terrassen haben meistens Sichtschutz. Gefährdeter sind Wohnungen im Erdgeschoss. Dort kommen die Täter vor allem durch Fenster oder über die Balkone. Manche Täter steigen aber auch vom Dach auf Balkone oder Dachterrassen.

■ Was würden Sie Verbrauchern raten, wenn sie sich selbst aktiv schützen möchten?
Unsere Empfehlung beruht auf drei Säulen. Bei der Technik gilt immer: Mechanik vor Elektronik. Sorgen Sie für einbruchssichere Türen und Fenster, fast alle lassen sich nachrüsten. Darüber sollte jeder verfügen. Zusatzschlösser und Verriegelungen sind oft elegant und effektiv. Ergänzen kann man elektronische Alarmanlagen. Besser sind Systeme, bei denen ein Notruf bei einer Sicherheitsfirma aufläuft. Bei Leuchten oder heulenden Sirenen, die nach ein paar Minuten stoppen, müssten Nachbarn aktiv werden. Der zweite Punkt ist das eigene Verhalten. Verschließen Sie bei Abwesenheit gekippte oder offene Fenster oder Türen. Dazu kommt drittens die Nachbarschaftshilfe, bei der man sich gegenseitig über Abwesenheit im Urlaub informiert, Briefkästen leert und lieber einmal mehr als zu wenig die Polizei ruft. Aufeinander abgestimmt, ist man mit diesen Maßnahmen sehr weit vorn und minimiert das Risiko. Die Quote der misslungenen Einbrüche steigt weiter auf über 40 Prozent an. Manchmal kann deshalb ein zusätzliches Schloss den Unterschied machen zwischen Drama und gescheitertem Einbruch. ■

VERANSTALTUNG

EINBRUCHSCHUTZMESSE – Polizeilich empfohlene Einbruchschutzmesse

Präsentiert werden einbruchhemmenden Fenstern und Türen nachrüstbare Fenster- und Türsicherungen sowie Sicherheitsschließzylinder.

Neben zertifizierten und polizeilich empfohlenen Ausstellern, bietet die Messe ein informatives Vortragsprogramm, der zuständigen polizeilichen Beratungsstelle.

12. + 13. Oktober in München
im Pressehaus des Münchner Merkur

26. + 27. Oktober in Chemnitz
im Autohaus Schloz-Wöllenstein

www.einbruchschutzmesse.de

RES-Q-EXPO

Die RES-Q-EXPO ist eine Plattform für Aussteller und Fachbesucher aus allen sicherheitsrelevanten Bereichen. Gleichzeitig steht die Messe aber auch allen interessierten Besuchern offen. Gezeigt werden Lösungen zur Rettung und zum Schutz von Menschen für Einsatzkräfte.

27. + 28. September
Fürstenfelder Str. 12, 82256 Fürstenfeldbruck

www.res-q-expo.de

HISCOX VERSICHERT RISIKEN DER DIGITALEN WELT

Versicherungen für den digitalen Wandel.

Mit Wissen und visionärem Mut machen wir digitale Risiken in einer vernetzten Welt managebar, wie mit unserer flexiblen Versicherung für IT-Unternehmen jeder Größe oder der Cyberversicherung bei Hackerangriffen oder Datenverlust.

Mehr erfahren: hiscox.de/digitalewelt

HISCOX

WISSEN VERSICHERT.