11 AUSGABE 2018
15. JAHRGANG

Report (+) PLUS

AUF NUMMER SICHER

Datenschutz & IT auf dem Prüfstand.
Wie sich Unternehmen schützen können
und was Sicherheit kosten darf.

10 Daten-schutz-Aktivist Max Schrems im Gespräch über Erfahrungen mit der DSGVO

P. B. B. VERLAGSPOSTAMT 1170 WIEN, VERTRIEBSKENNZAHL GZ 02Z034501, EINZELHEFTPREIS: EUR 4,–

TRUSTED USER ODER CYBER THREAT?

Durch den stetigen Anstieg von Online-Vertragsabschlüssen und Transaktionen treten vermehrt Fälle von Identitätsdiebstahl und vorsätzlichem Betrug auf. Mit dem **Fraud Prevention Kit** überprüft und analysiert CRIF anhand ausgewählter Kriterien in Echtzeit den Antrag Ihres Kunden auf bekannte Betrugsmuster. Damit erhalten Sie sofort die Information, ob es sich um einen möglichen Betrugsversuch handelt oder nicht.

- **Frühzeitige Erkennung von Betrugsversuchen**
- **Vermeidung von Forderungsausfällen**
- **Eindeutige und sichere Identifikation**
- **Umfassende Device Erkennung und Identifizierung**
- **Verifizierung von Antragsdaten in Echtzeit**

crif.at
marketing.at@crif.com

CRIF
Together to the next level

EIN WORT VOM

EDITOR

ANGELA HEISSENBERGER
Redakteurin Report(+)PLUS

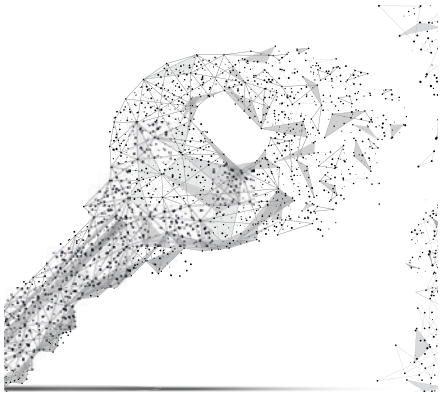
GEFAHRENZONE IT

Löchrig wie ein Schweizer Käse – so schätzen viele Sicherheitsexperten die IT heimischer Unternehmen ein. Veraltete Programme, fehlende Backups und ungesicherte Daten machen es Kriminellen nur allzu leicht, in Systeme einzudringen. Gefahr droht auch durch Lücken in der Hard- und Software; mittels KI-Technologie sollen diese, wie Forscherteams prophezeien, schon bald geschlossen werden.

Die größte Schwachstelle bleibt somit der Mensch. Sorglosigkeit und unzureichende IT-Kenntnisse hebeln die beste Sicherheitstechnik aus. IT-Forensiker berichten von immer raffinierteren Methoden, mit denen das Vertrauen der Mitarbeiterinnen und Mitarbeiter über viele Wochen und Monate erschlichen wird. Treffen kann es Unternehmen jeder Branche und Größe. Einsparungen beim Sicherheitsbudget und chronisch unterbesetzte IT-Abteilungen machen jedoch vor allem KMU verwundbar, die das Risiko jahrelang unterschätzt haben.

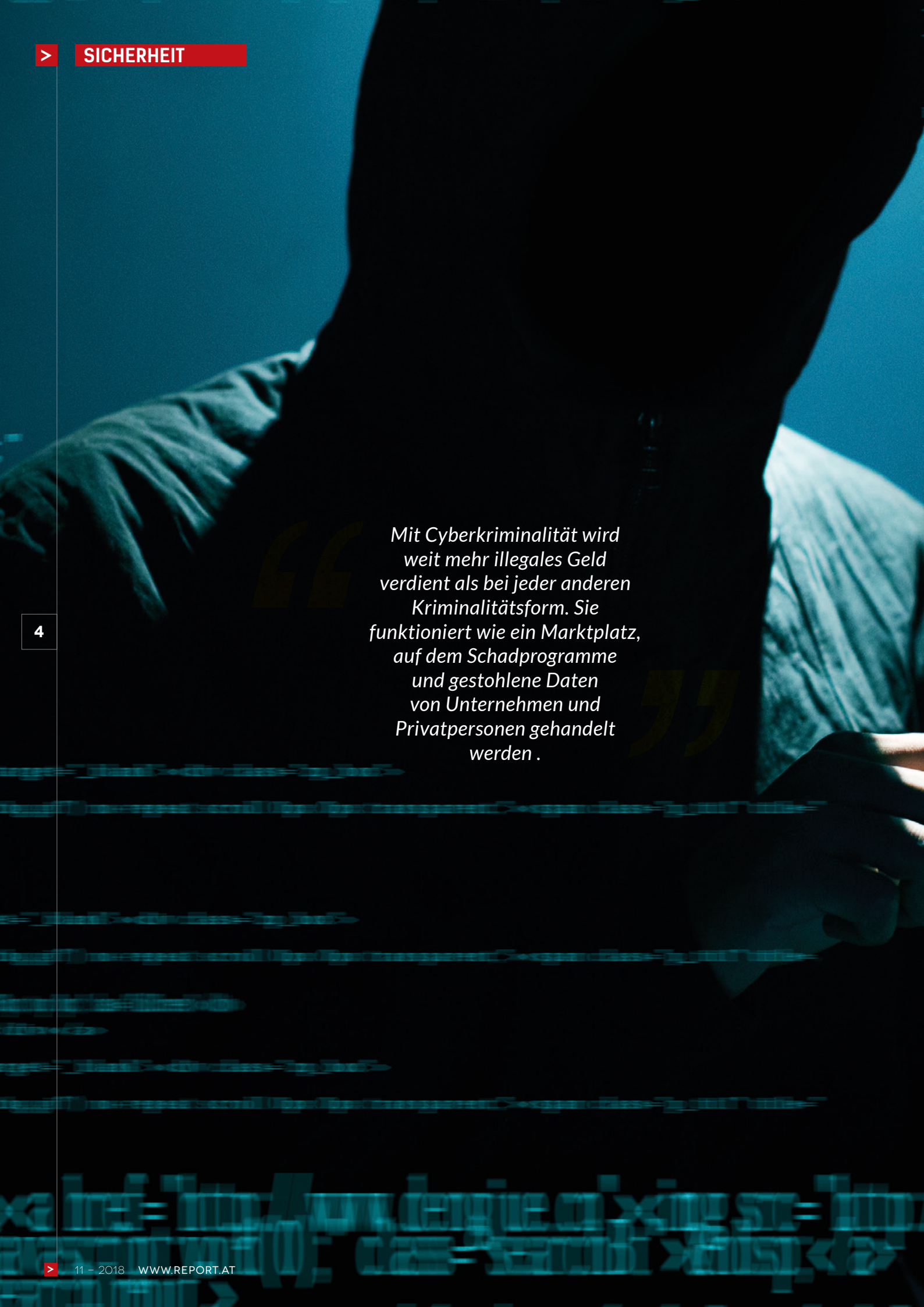
Report(+)PLUS richtet den Fokus auf Best-Practice-Beispiele, die sich in der Praxis bewährt haben. IT-ExpertInnen aus Wirtschaft und Wissenschaft kommen ebenso zu Wort wie VertreterInnen von Behörden. Welche neuen Technologien und Lösungen uns in Zukunft erwarten und wie Sie Ihre Daten besser schützen können, lesen Sie in diesem Schwerpunktheft.

REPORT PLUS DAS UNABHÄNGIGE WIRTSCHAFTSMAGAZIN



IMPRESSUM

Herausgeber/Chefredakteur: Dr. Alfons Flatscher [flatscher@report.at] **Verlagsleitung:** Mag. Gerda Platzer [platzer@report.at] **Chef vom Dienst:** Mag. Bernd Affenzeller [affenzeller@report.at] **Redaktion:** Mag. Angela Heissenberger [heissenberger@report.at], Martin Szelgrad [szelgrad@report.at] **AutorInnen:** Mag. Karin Legat, Mag. Rainer Sigl **Layout:** Report Media LLC **Produktion:** Report Media LLC, Mag. Rainer Sigl **Druck:** Styria **Medieninhaber:** Report Verlag GmbH & Co KG, Lienfeldergasse 58/3, A-1160 Wien **Telefon:** (01) 902 99-0 **Fax:** (01) 902 99-37 **E-Mail:** office@report.at **Web:** www.report.at



Mit Cyberkriminalität wird weit mehr illegales Geld verdient als bei jeder anderen Kriminalitätsform. Sie funktioniert wie ein Marktplatz, auf dem Schadprogramme und gestohlene Daten von Unternehmen und Privatpersonen gehandelt werden .

UNTERSCHÄTZTE RISIKEN

HUNDERTPROZENTIGEN SCHUTZ VOR CYBERKRIMINALITÄT WIRD ES NICHT GEBEN, DARIN SIND SICH FACHLEUTE EINIG. INTERDISZIPLINÄRE FORSCHERTEAMS ARBEITEN MIT HOCHDRUCK AN TECHNOLOGIEN, DIE ANGRIFFE UND SCHÄDEN MINIMIEREN SOLLEN. DAS SICHERHEITSBEWUSSTSEIN IN DEN UNTERNEHMEN IST INDESSEN NOCH NICHT SEHR AUSGEPRÄGT.

VON ANGELA HEISSENBERGER

Trotz aller Fortschritte, die Forscher und IT-Entwickler bei der Erkennung und Abwehr von Angriffen machen, mutet die Aufgabe wie jene des antiken Helden Sisyphos an. Ein herkömmliches Virenschutzprogramm erkennt mehr als 400 Millionen Malware-Signaturen. Täglich kommen aber tausende neue hinzu.

Ein noch größeres Problem sind jedoch Cyberattacken, die in vielen kleinen Angriffen über einen langen Zeitraum erfolgen und kaum Spuren hinterlassen. Sogenannte Advanced Persistent Threads (APTs) sind Schadprogramme, die speziell auf das attackierte Unternehmen zugeschnitten sind, über ein Schlupfloch eindringen und sich tief im System einnisten. Ein APT bleibt oft über Monate, manchmal sogar Jahre unentdeckt, da es seine Anwesenheit vor bekannten Erkennungsverfahren verschleiern kann. Meist werden auf diese Weise Daten ausspioniert und wichtige Dokumente oder Patentunterlagen an fremde Server gesendet.

Die Schadsoftware kann aber auch das System gezielt manipulieren. Der Schaden ist immens – Experten gehen davon aus, dass der Gewinn, der durch Cyberkriminalität erzielt wird, den Gewinn aus internationalen Drogengeschäften bereits übersteigt. »Cyberangriffe auf Unternehmen sind längst keine Seltenheit mehr – sie sind an der Tagesordnung«, bestätigt Gottfried

Noch scheint es, als wären die Täter stets zwei Schritte voraus. Das könnte sich bald ändern.

Tonweber, Director IT Advisory bei EY Österreich. »Selbst die Unternehmen, die noch keinen Angriff registriert haben, könnten betroffen sein, ohne etwas davon mitzubekommen. Unternehmen, die erst reagieren, wenn das Kind in den Brunnen gefallen ist, handeln fahrlässig: Der Schadensfall kann schnell verheerende Auswirkungen haben.«

>> Sorgenkind IoT <<

Noch scheint es, als wären die Täter stets zwei Schritte voraus. Das könnte sich bald ändern. Wissenschafter an den technischen Universitäten und Fachhochschulen arbeiten in ständigem Austausch mit Unternehmen mit Hochdruck an der Entwicklung innovativer Lösungen, die IT-Sicherheit auf einen höheren Level heben sollen. »Der Schutz kritischer Infrastrukturen ist in Europa wichtiger denn je«, sagt Thomas Brandstetter, Dozent am Department Informatik und Security der FH St. Pölten und Organisator der internationalen Fachtagung »IT-Security Community Exchange« (IT-SECX). »Digitalisierung ist ein Kernthema auch für die Industrie geworden. Industrieunternehmen vernetzen ihre Anlagen immer stärker und statten diese stärker mit Softwarekomponenten aus, um Daten zu generieren und mit diesen den Betrieb zu verbessern. Das öffnet Einfallstore für Schadsoftware und ist eine große Herausforderung für die IT-Sicherheit.«

Claudia Eckert, AISEC: »So wie der Mensch eindeutig identifizierbar ist, gibt es auch eine Art Biometrie für Objekte.«

Spätestens in fünf bis zehn Jahren werde es »selbstregulierende Architekturen« geben, die proaktiv eine Bedrohung verhindern, zeigt sich Claudia Eckert, Leiterin des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit (AISEC) und Professorin an der TU München, zuversichtlich. »Hacking ist auch ein kreativer Akt«, sagt die Informatikerin – und genau das diese Unberechenbarkeit mache Gegenmaßnahmen so schwierig. Alle Varianten eines möglichen Eindringens müssten durchkalkuliert werden. Aber ähnlich wie Schachcomputer auch den besten Spielern längst überlegen sind, sei es nur noch eine Frage der Zeit, bis auch Sicherheitssysteme so ausgereift sind, dass Angreifer keine Chance haben.

ERNSTFALL **CYBERANGRIFF**

1. Risikoanalyse: Vorsorge ist alles. Um gegen Angriffe gewappnet zu sein, sollte klar sein, über welche kritischen Daten das Unternehmen verfügt wo diese gespeichert sind. Mitarbeiterverzeichnisse, Kundendaten, Fahrtenbücher oder Lieferantenlisten finden sich u.a. auch auf mobilen Devices wie Smartphones, Tablets oder digitalen Fotokameras. Auf Cyber Security spezialisierte Experten ermitteln in einer Analyse den Schutzbedarf und mögliche Bedrohungsszenarien. Penetrationstests zeigen auf, wo Sicherheitslücken bestehen.

2. Schutzmaßnahmen: Ein modernes Sicherheitskonzept beinhaltet ein Frühwarnsystem, das verdächtige Anomalien rechtzeitig meldet. Komplexe Cyberattacken torpedieren das Unternehmen an mehreren Stellen über einen längeren Zeitraum in vielen kleinen Angriffen, von denen jeder für sich unbedeutend erscheint, aber Teil einer gefährlichen Strategie ist. Neben technischen Sicherheitslösungen, die alle Unternehmensprozesse umfassen und regelmäßige Updates vorsehen, sind auch organisatorische Maßnahmen unumgänglich. Dazu gehören Zugangsregelungen und Verhaltensrichtlinien ebenso wie klare Zuständigkeiten. Ein Notfallplan legt fest, welche Maßnahmen in welcher Reihenfolge ablaufen und wer wann zu informieren ist. Die Sicherheitsstrategie sollten laufend überprüft werden und fester Teil der Mitarbeiterschulungen sein.

3. Meldung: Sind personenbezogene Daten von Kunden, Lieferanten oder Mitarbeitern betroffen, muss laut DSGVO innerhalb von 72 Stunden eine Meldung an die zuständige Datenschutz-

Foto: iStock, Andreas Heddergott

behörde erfolgen. Strafrechtlich relevante Angriffe werden an die Polizei gemeldet. Weiters sind jene Personen zu benachrichtigen, deren Daten möglicherweise in falsche Hände gelangt sind.

4. Krisenmanagement: Nach einer Attacke tritt der im Vorfeld akkordierte Notfallplan in Kraft. Sicherheits- und Datenschutzbeauftragte, Mitarbeiter der IT-Abteilung, des Rechenzentrums und der betroffenen Abteilungen, Betriebsrat und Geschäftsführung sollten sofort einen Krisenstab bilden. Auch die Beiziehung externer IT-Forensiker empfiehlt sich. Statt einfach den Stecker zu ziehen, versuchen Spezialisten, die Angreifer mittels sogenannter »Honeypots« – vielversprechender Fake-Informationen – abzulenken und sie nach Möglichkeit ausfindig zu machen. Gleichzeitig werden zusätzliche Barrieren installiert, um besonders sensible Datenbereiche zu schützen.

5. Dokumentation: Zur Verfolgung und Evaluation eines Cyberangriffs ist ein Protokoll hilfreich, das alle Informationen zu den damit verbundenen Vorgängen enthält, z.B. Zeitpunkte und Kontaktpunkte der jeweiligen Ereignisse, Personen und Verbindungen nach außen, Schadensfeststellung der betroffenen Konten, Systeme, Netze und Dienste.

Das Internet der Dinge stellt Forscher und Techniker vor besondere Herausforderung. Damit sich die tausenden im Internet vernetzten Objekte wechselseitig identifizieren können, braucht es für die Industrie praktikable, skalierbare Verfahren. Das AISEC entwickelte eine Methode, die Produktionsmaschinen mithilfe eines Kryptografie-Chips von Infineon eine zusätzliche Sicherheitsstufe vorschaltet. Ähnlich wie der Mensch anhand des Fingerabdrucks identifizierbar ist, gibt es auch eine Art Biometrie für Objekte, die sich aufgrund physikalischer, nicht nachbaubarer Eigenschaften unterscheiden. ▶

Am Austrian Institute of Technology (AIT) entwickelten Wissenschafter eine patentierte Lösung, die auf Ansätzen aus der Bioinformatik basiert. Das selbstlernende Tool kann häufig auftretende Muster in Logfiles und Ereignissen entdecken, klassifizieren und clustern und somit bekannte »gute« Aktivitäten von unbekannten schädlichen Aktivitäten in betrieblichen IT-Infrastrukturen unterscheiden.

Samuel Brandstätter, avedos: »Bedrohungen, die nur schwer zu greifen sind, werden öfter unterschätzt.«

Die Erfolge auf dem Gebiet der künstlichen Intelligenz bringen zugleich Fluch und Segen. Durch die Fortschritte in der Forschung wird Cyber Security im Umgang mit den ständig wechselnden Bedrohungen zwar immer effizienter. »Andererseits stellt KI selbst eine Gefahr dar«, meint Gert Weidinger, KPMG-Partner in Österreich. »Sie bedeutet immer auch Vernetzung und öffnet Tür und Tor für Angriffe und Manipulationen für Hacker.«

> WUNSCH UND WIRKLICHKEIT KLAFFEN WEIT AUSEINANDER. BEI **EINEM FÜNFTEL DER BETRIEBE** BETRAGEN DIE SECURITY-AUSGABEN NUR ZWEI BIS FÜNF PROZENT DES GESAMTEN IT-BUDGETS.

>> An der Wurzel packen <<

»Durch die Digitalisierung und Vernetzung von intelligenten Systemen werden mehr Daten gesammelt – oftmals ohne Ziel – und über unterschiedliche Kanäle bzw. Protokolle übertragen. Dadurch entsteht eine Vielzahl an neuen Angriffsvektoren, die es in einer allumfassenden Sicherheitslösung zu berücksichtigen gilt«, erläutert Marian Percsy, Major Account Manager bei Check Point Software. »Netzwerke industrieller Automations- und Kontrollkomponenten nähern sich zunehmend den klassischen IT-Netzwerken an. Diese müssen ebenso geschützt werden wie die – bis dato vernachlässigten Bereiche – Cloud- und Container-Lösungen sowie mobile Endgeräte. »Heartbleed«, eine Lücke im bis dahin als sicher geltenden Zugangsverfahren SSL, zeigte deutlich, wie verletzbar Systeme sind. Durch einen schwerwiegenden Programmierfehler im Quellcode der älteren Versionen konnten 2014 über verschlüsselte Verbindungen Daten von Clients und Servern ausgelesen werden. Automatische Softwareprüfprogramme, die Programmcodes auf Schwachstellen testen, sind inzwischen Standard. Für Programmierer in der Industrie, die spezielle Software für eingebettete Systeme entwickeln, gewinnen Sicherheitstools im Zeitalter des Internet of Things zunehmend an Bedeutung.

»Security by Design« ist eine Anforderung, die ein entscheidendes Problem an der Wurzel behebt: »95 % der erfolgreichen Angriffe basieren auf schlecht programmierter, schlecht gewarteter oder schlecht konfigurierter Software«, sagt Thomas Tschersich,

Foto: iStock,

Leiter Internal Security & Cyber Defense der Deutschen Telekom. Anstatt erst »ein Pflaster über das Produkt zu kleben, wenn es bereits zusammengebaut wurde«, sollte das Thema Sicherheit bereits bei der Planung mitgedacht werden.

>> DSGVO als Motor <<

Derzeit lautet die Devise vieler Unternehmen noch, kein einfaches Ziel zu sein. Cyberkriminelle versuchen mit massiven Angriffen, den größtmöglichen Schaden zu erzielen. Art, Größe und Branche des Unternehmens sind für sie zweitrangig. Je besser sich ein Betrieb schützt, desto uninteressanter wird er für Täter. Es gibt genügend andere lohnende Ziele, die über keinen mehrstufigen Schutz, moderne technologische Lösungen, aktuelle Systeme und Passwort-Manager verfügen. Globale Cyberattacken wie Petya oder Wannacry rufen die Gefahren kurzfristig in Erinnerung, dennoch ist »123456« noch immer das beliebteste Passwort der Welt. Nicht weniger fahrlässig handelten die 1.464 Mitarbeiter des öffentlichen Dienstes in Australien, die sich mit »password123« einloggten.

Die seit Mai 2018 geltende Datenschutzgrundverordnung (DSGVO) und die EU-Richtlinie zur Netz- und Informationssicherheit (NIS) sorgten in vielen Unternehmen für Verunsicherung, trugen aber maßgeblich zu einer breiteren Publizität des Themas Datensicherheit bei.

»Nicht-zielgerichtete Attacken (beispielsweise durch Ransomware) haben aufgrund der Vielzahl an betroffenen Geräten und dem einhergehenden Schaden für großes Aufsehen gesorgt. Diese Art von Attacken stellt jedoch nur einen Bruchteil der gesamten Cyberangriffe dar«, erklärt Check Point-Manager Marian Percsy. Grundsätzlich könnten alle Organisationen, ungeachtet des Betätigungsfeldes und der Größe, potenzielle Opfer von Cyberangriffen werden, so Percsy: »Vorwiegend von Interesse sind jedoch Organisationen mit sensiblen bzw. wertvollen Informationen, die im Rahmen von zielgerichteten Attacken anvisiert werden. Solche Vorfälle werden durch gesetzliche Vorgaben wie die DSGVO und die daraus resultierenden Meldepflichten sichtbarer. Datensicherheit ist folglich nicht mehr alleiniges Thema der IT.«

Marian Percsy, Check Point: »Datensicherheit ist nicht mehr alleiniges Thema der IT.«

Die gute Nachricht: Rund die Hälfte der befragten Unternehmen will das Budget für Cyber Security im kommenden Jahr zumindest leicht aufstocken. In jedem fünften Betrieb ist man sogar der Meinung, es sollte mehr als 10 % des IT-Budgets ausmachen.

Wunsch und Wirklichkeit klaffen jedoch noch weit auseinander, weiß KPMG-Partner Andreas Tomek: »Die Vorstellung vom idealen Budget weicht stark vom realen ab.« Bei rund einem Fünftel der Unternehmen beträgt das Security-Budget lediglich 2 bis 5 % des IT-Gesamtbudgets.

Die klassische Prävention in Form von Firewalls, Proxies oder Virenscannern kann strategische Angriffe aber bestenfalls erschweren. »Technik kann und muss gegen technische Schwachstellen schützen. Die erforderliche Komplexität steigt parallel zur wachsenden IT-Infrastruktur in Unternehmen«, erklärt Samuel Brandstätter, CEO der avedos GRC GmbH. »Darüber hinaus sind aber auch organisatorische und menschliche Schwachstellen relevant, gegen die technische Lösungen nur bedingt hilfreich sind.«

Das Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27001 bezieht deshalb alle wichtigen Entscheidungsträger mit ein. Besonderes Augenmerk liegt auf laufenden Verbesserung der Security Policies. Trotz der damit verbundenen Aufwertung seiner Position trägt die Verantwortung letztlich aber nicht nur der CIO, so avedos-Chef Brandstätter: »Dies kann keine alleinige Aufgabe des Sicherheitsverantwortlichen oder der IT sein sondern muss in der Organisation verankert sein.« ■

(+) PLUS: Die DSGVO wird von vielen positiv für den europäischen Wirtschaftsraum gesehen. Dennoch stellt sich für Unternehmen die Frage, ob dadurch nicht datenbasierende Geschäftsmodelle von Haus aus verhindert werden.

Max Schrems: Das sehe ich nicht so. Nehmen wir als Beispiel Onlinewerbung. Sie kann auch ohne die Nutzung personenbezogener Daten betrieben werden. Es gibt heute 20 bis 30 verschiedene Arten von Online-Targeting und nur ein gewisser Teil braucht tiefe Nutzerprofile. Da stellt sich schon die Frage, wie sehr das notwendig ist – wenn auf der anderen Seite in die Grundrechte der Konsumenten oder Bürger eingegriffen wird.

(+) PLUS: Warum ist Datenschutz besonders aus Konsumentensicht wichtig?

Schrems: In dieser Diskussion mag der Bereich Werbung noch relativ harmlos erscheinen, wir sehen zunehmend aber auch Anfragen und Probleme beim Kredit-Scoring – wenn jemand keinen Handyvertrag bekommt, wenn etwas falsch in einer Datenbank eingetragen ist. Ein weiteres schönes Beispiel ist auch »Personalised Pricing«, bei dem Menschen verschiedene Preise für ein und dieselbe Sache vorgesetzt bekommen – je nach dem, ob dahinter vielleicht meine Termininformationen mit meinen Anfragen bei der Fluggesellschaft verknüpft werden; je dringender, desto teurer das Ticket. Das wird zwar noch nicht gemacht, steht aber auf der Liste der Möglichkeiten für Umsatzsteigerungen ganz oben. Jene Unternehmen, die über mehr Informationen als andere am Markt verfügen, können praktisch ihre eigenen Regeln bestimmen.

Aber Direktmarketing wird auch weiterhin bei einem legitimen Interesse möglich sein. Ein Beispiel sind Verlage, die ihre Abonnenten anrufen, um eine Aboverlängerung zu bewerben. Das heißt gleichzeitig nicht, dass ein Unternehmen wie Google die letzten zehn Jahre Web-History seiner Nutzer sammeln darf. Das Koppelungsverbot ist ebenfalls etwas, das bislang brutal ignoriert wird. Es ist klar gesetzlich geregelt, dass ein Dienstebetreiber die Zustimmung der Nutzung der Anwenderdaten nicht erzwingen darf – nach dem Motto: Wenn du den AGBs nicht zustimmst, wirst du von meinem Dienst ausgeschlossen. Es muss eine Freiwilligkeit ohne Nachteile gegeben sein.

Und noch einmal betont: Hier geht es vor allem um die Großen, die dadurch Vorteile gegenüber vielen kleineren Unternehmen bekommen. Und ich habe den Eindruck, dass die Strafandrohung von vier Prozent des Umsatzes bei Verletzungen für die ganz großen Player offenbar nicht hoch genug sind. Sie kalkulieren mehrjährige Rechtsstreite ein und agieren einfach etwas zum europäischen Rechtsrahmen versetzt weiter.

DIE NGO

Im November 2017 gründete Max Schrems die Datenschutz-NGO NOYB – Europäisches Zentrum für Digitale Rechte. NOYB steht dabei für »none of your business«. Die Initiative geht gegen Datenschutzverletzungen von Unternehmen auf europäischer Ebene vor und bemüht sich um die Zusammenarbeit mit Organisationen in allen EU-Ländern.

(+) PLUS: Verstehen Sie die Aufregung, die rund um den 25. Mai in der Wirtschaft geherrscht hat?

Schrems: Bei vielen der Regelungen, die ja nicht ganz neu sind, stellt sich schon die Frage, wo diese Panik herrührt. Aber es gibt natürlich auch eine Beratungsindustrie, die gut davon lebt. In einigen Punkten wäre das österreichische Recht sogar strenger als die DSGVO gewesen – zumindest am Papier. Es ist ja stets an der Durchsetzung gescheitert. Andere Punkte der DSGVO wiederum schie-

Foto: Lukas Beck

»Früher im Bereich der Verschwörungstheorien angesiedelt«

Datenschutzaktivist Max Schrems ist Vorstand von NOYB – European Center for Digital Rights. Er spricht über Erfahrungen mit der DSGVO und erklärt, warum diese auch wichtig für die heimische Wirtschaft ist.

ßen übers Ziel hinaus. Aber Unternehmer, die sorgsam mit personenbezogenen Daten umgehen und Datenschutz ernst nehmen, haben keinerlei Probleme mit der DSGVO. Ist die Verarbeitung von Daten für die Vertragserfüllung notwendig, braucht es auch keine Zustimmungserklärung.

(+) PLUS: Viele der Unternehmen waren also unterversorgt, was das Wissen um die DSGVO betrifft?

Schrems: Die meisten hatten ein halbes Jahr vor Inkrafttreten des Gesetzes – also eineinhalb Jahre nach seinem Beschluss – ihren Anwalt zum ersten Mal dazu befragt. Nun ist Datenschutzgesetzgebung generell sehr komplex und der DSGVO-Gesetzestext meiner Meinung nach nicht besonders klar formuliert. Es ist ein juristisches Spezialgebiet. Das hatte zur Folge, dass wir in den vergangenen Monaten so viele Zustimmungserklärungen gesehen hatten. Man geht lieber auf Nummer sicher.

(+) PLUS: Wie gut funktioniert eigentlich die Zusammenarbeit der Datenschutzbehörden in den unterschiedlichen EU-Ländern?

Schrems: Wir haben gerade einen internationalen Fall eines Unternehmens mit europäischen Hauptsitz in Irland, bei dem in dem Kooperationssystem im Sinne der DSGVO die irische Datenschutzbehörde zuständig ist.

Unsere Erfahrung bislang ist, dass dort Anträge einmal abliegen – innerhalb von bald sechs Monaten haben wir gerade einmal eine Bestätigung erhalten, dass es angekommen ist. Wir wollen mit NOYB prinzipiell prüfen, wie gut die Kooperationsmechanismen auf Behördenebene funktionieren. Viele der Dinge, die in Brüssel auf dem Papier überlegt worden sind, müssen nun in der Praxis bestehen.

(+) PLUS: Welche weiteren Schritte haben Sie mit NOYB vor?

Schrems: Wir betreiben Aufbauarbeit für »Strategic Ligitation« für Datenschutzverletzungen auf europäischer Ebene. Dazu gehören die Recherche zu Gesetzestexten, die Analyse von Verfahrensrechten in den Mitgliedstaaten und auch die Kontaktaufnahme zu anderen NGOs. Nach den Beschwerden von NOYB gegen Facebook, WhatsApp, Instagram und Google stehen in Kürze weitere Projekte zur Durchsetzung an, über die ich aber noch nicht sprechen kann.

Wir bringen uns dort ein, wo möglichst effektiv etwas durchgesetzt werden kann. Gerade im Verfahrensrecht tickt jedes Land etwas anders – in manchen Ländern wie in Irland können Verhandlungen empfindlich länger dauern und sind deshalb auch wesentlich teurer. Aufgrund des Kostenrisikos haben einzelne Konsumenten oder Bürger eigentlich keine Chance. Deshalb ist es schon sinnvoll, dass es Verbraucherschutz-Organisationen oder NGOs auf europäischer Ebene gibt.

(+) PLUS: Sind europäische IT-Unternehmen und Dienstleister ebenfalls im Fokus?

Schrems: Wir machen keinen Unterschied, was die Herkunft betrifft. Ich sehe aber schon einen gewissen Unterschied in der Unternehmenskultur. Die krassen Datenschutzverletzungen werden oft von Firmen begangen, die nicht aus Europa kommen. Aber es gibt auch europäische Firmen mit einer sehr amerikanischen Zugangsweise. Da ist der Unterschied dann nicht mehr so groß.

(+) PLUS: Hat der deutschsprachige Raum eine besondere Beziehung zu Datenschutz? Was ist Ihr Eindruck?

Schrems: Als ich vor sieben Jahren begonnen hatte, mich intensiv mit Datenschutz zu beschäftigen, war dieses Thema bei vielen noch im Bereich der Verschwörungstheorien angesiedelt. Das hat sich zum Glück massiv geändert. Datenschutz als Thema ist im Mainstream angekommen. Einen Anteil daran haben auch Verbraucherschutzverbände wie der Verein für Konsumenteninformation in Österreich oder der deutsche Verbraucherschutzverband. In der OGH-Judikatur zu Datenschutzthemen findet man zum größten Teil Klagen durch den VKI wieder. Außerhalb des deutschsprachigen Raums gibt es nur wenige Staaten, in denen die Privatsphäre der Menschen schon vor der EU-Datenschutzgrundverordnung ein Riesenthema war, Norwegen zum Beispiel. ■

DIE GESCHÄFTSLEITUNG INVOLVIEREN

Das Bewusstsein für das Risiko von IT-Angriffen ist bei Führungskräften zwar gestiegen, viele scheuen aber notwendige Ausgaben für IT-Sicherheit. Deshalb ist es wichtig, die Geschäftsleitung umfassend zu informieren und sicherzustellen, dass sie die Tragweite und Notwendigkeit des Themas erkennt und sie für das Projekt zu gewinnen.

ANTI-VIRUS-PROGRAMME

Eine einfache, aber effektive Sicherheitsmaßnahme ist die Installation einer starken Virenschutz-Software auf allen Mitarbeiter-Computern und Mobiltelefonen. Diese Virenscanner suchen die Geräte nach Bedrohungen wie Viren oder Spyware ab, die dann blockiert und entfernt werden.

MITARBEITER SCHULEN

Bewusstsein schützt vor Schaden: Viele Mitarbeiter kennen die Cyber-Risiken nicht. Aus Naivität oder Neugierde werden einem Virus oder Schadprogramm Tür und Tor geöffnet. Schulen Sie Ihr Personal daher im sicheren Umgang mit dem IT-System und stellen Sie einen Cyber-Security-Leitfaden zur Verfügung.

ACHTUNG SMARTPHONES

Auch sämtliche Smartphones in einem Unternehmen müssen gegen Cyber-Angriffe geschützt werden. Denn Viren und Trojaner können sich über E-Mails und dubiose Apps besonders leicht in ein System einschleichen. Laden Sie Apps nur aus den offiziellen App-Stores herunter und sichern Sie Handys unbedingt mit einem Kennwort oder, besser noch, durch eine biometrische Absicherung.

Quelle: Dell, Uniqa

Foto: iStock

Tipps & Tricks

Wie Sie Ihr Unternehmen gegen Cyber-Angriffe schützen

SICHERHEITSSTRATEGIE ENTWICKELN

Welche Ressourcen – personell und finanziell – werden benötigt? Welche Risiken können in Kauf genommen werden? Welche Reaktion sollte auf welchen Einbruch erfolgen? Welche Systeme werden benötigt? Brauchen Sie externe Dienstleister? In der Sicherheitsstrategie sollten solche und andere Fragen geklärt, Erwartungen festgelegt als auch Budget- und Personalszenarien entworfen werden.

VORSICHT W-LAN

Wichtig für alle, die gerne unterwegs arbeiten: Nutzen Sie das öffentliche W-LAN in Cafés, am Flughafen, oder auch im Hotel niemals für sensible Transaktionen wie E-Banking. Vor allem bei unverschlüsselten Verbindungen besteht die Gefahr, dass Passwörter ausgelesen werden.

SICHERE PASSWÖRTER

Wählen Sie für jedes Konto ein eigenes, starkes Kennwort mit Zahlen, Ziffern, Groß- und Kleinschreibung und geben Sie dieses niemals weiter. Default-Passwörter für Software und Hardware sollten immer geändert werden. Spezielle Software-Programme, sogenannte »Passwortmanager«, helfen Ihnen, den Überblick zu bewahren, indem sie Ihre Passwörter verschlüsseln und verwalten.

SICHERHEITSRICHTLINIEN ERARBEITEN

Unternehmensweite Richtlinien sind ein zentraler Bestandteil einer umfassenden Sicherheitsstrategie. Diese Richtlinien müssen auch Compliance- und sonstige juristischen Aspekte , z.B. die DSGVO, berücksichtigen.

REGELMÄßIGE BACKUPS

Erstellen Sie in regelmäßigen Abständen Datensicherungen, um im Ernstfall einen kompletten Datenverlust zu vermeiden und gelöschte Daten wiederherstellen zu können. Speichern Sie dazu wichtige Dokumente und Dateien auf einem externen Datenträger ab und trennen Sie diesen nach der Datensicherung unbedingt vom operativen System.

KONTROLLSCHLEIFEN EINZIEHEN

Nur ein Sicherheitssystem, das ständig hinterfragt wird, ist ein gutes Sicherheitssystem. Behalten Sie neue Gefahren, Best-Practice-Lösungen am Markt oder auch die Veränderung der Organisation im eigenen Unternehmen im Blick. Leistungskennzahlen, sogenannte KPIs, sollten ständig erweitert oder angepasst werden.

40.500

Euro kostet kleinen und mittleren Unternehmen (KMU) durchschnittlich ein Ransomware-Befall. Das durchschnittlich geforderte Lösegeld liegt bei 3.700 Euro, so eine Studie von Datto, die auf den Aussagen von 2.400 IT-Dienstleistern basiert.

870

Laut einer Erhebung des Sicherheitsspezialisten Tenable sind Unternehmen im Durchschnitt mit 870 Schwachstellen pro Tag konfrontiert. Darunter befinden sich 100 Schwachstellen, die nach dem Common Vulnerability Scoring System (CVSS) – einem Branchenstandard zur Bewertung von Sicherheitslücken – als kritisch eingestuft werden.

1/2

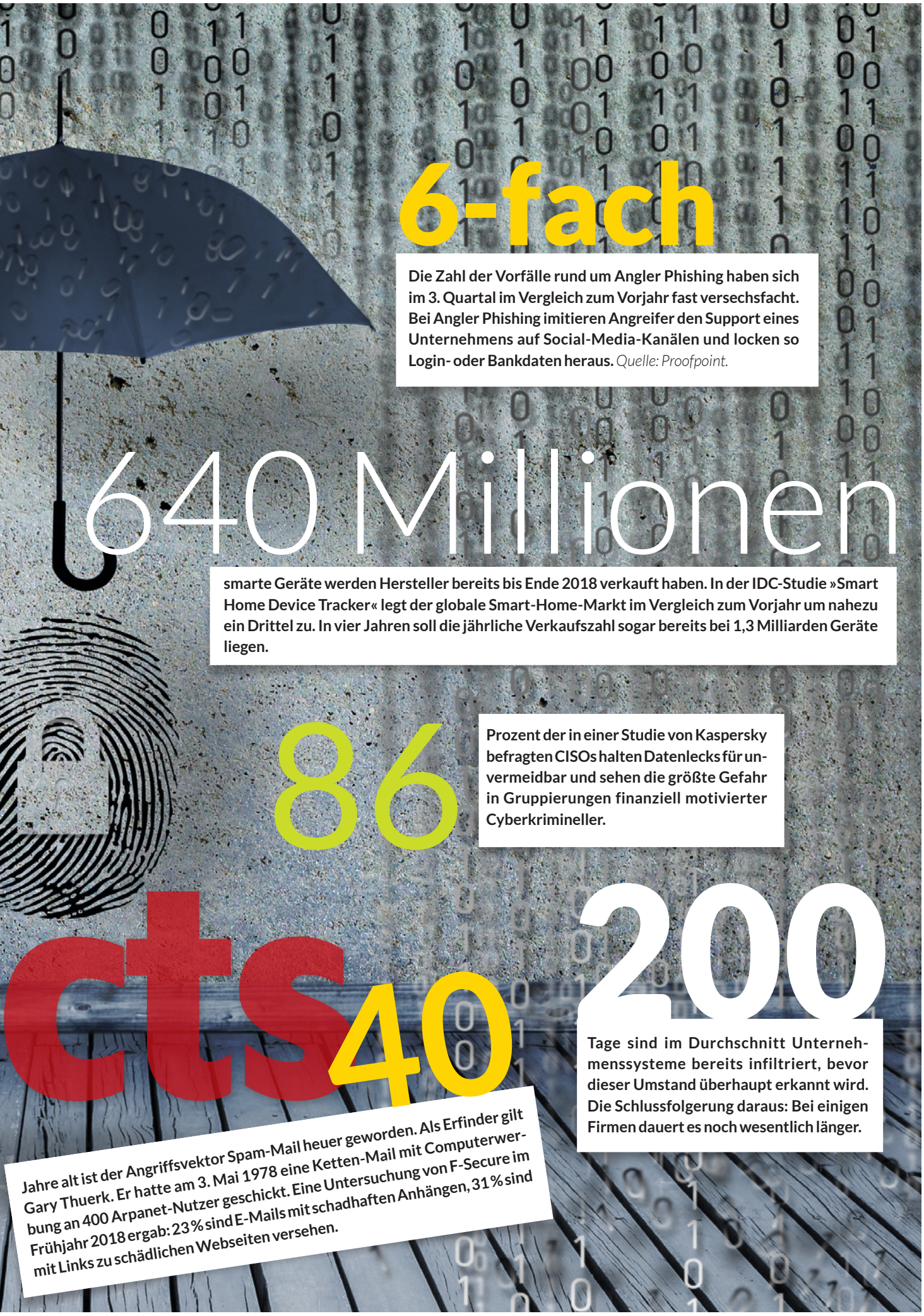
Die Hälfte aller Unternehmen würde ein Katastrophenereignis nicht überleben, schätzt man bei IDC. Laut der Studie »State of IT Resilience« erachten fast alle Befragten die Absicherung ihrer Systems für wichtig oder sehr wichtig, aber nur 7 % halten die von ihnen eingesetzten Technologien für ausgereift genug, um ihre betriebliche Ausfallsicherheit zu gewährleisten.

1/3

der Internet-Nutzer (34 %) fürchtet sich einer Bitkom-Umfrage zufolge vor Ransomware. Dass diese Angst durchaus berechtigt ist, zeigt eine aktuelle Kaspersky-Studie: Die Anzahl durch Ransomware angegriffener Nutzer stieg im dritten Quartal auf weltweit 259.867 an.

fa

Foto: iStock



6-fach

Die Zahl der Vorfälle rund um Angler Phishing haben sich im 3. Quartal im Vergleich zum Vorjahr fast versechsfacht. Bei Angler Phishing imitieren Angreifer den Support eines Unternehmens auf Social-Media-Kanälen und locken so Login- oder Bankdaten heraus. *Quelle: Proofpoint.*

640 Millionen

smarte Geräte werden Hersteller bereits bis Ende 2018 verkauft haben. In der IDC-Studie »Smart Home Device Tracker« legt der globale Smart-Home-Markt im Vergleich zum Vorjahr um nahezu ein Drittel zu. In vier Jahren soll die jährliche Verkaufszahl sogar bereits bei 1,3 Milliarden Geräte liegen.

86

Prozent der in einer Studie von Kaspersky befragten CISOs halten Datenlecks für unvermeidbar und sehen die größte Gefahr in Gruppierungen finanziell motivierter Cyberkrimineller.

cts 40

Jahre alt ist der Angriffsvektor Spam-Mail heuer geworden. Als Erfinder gilt Gary Thuerk. Er hatte am 3. Mai 1978 eine Ketten-Mail mit Computerwerbung an 400 Arpanet-Nutzer geschickt. Eine Untersuchung von F-Secure im Frühjahr 2018 ergab: 23 % sind E-Mails mit schadhaften Anhängen, 31 % sind mit Links zu schädlichen Webseiten versehen.

200

Tage sind im Durchschnitt Unternehmenssysteme bereits infiltriert, bevor dieser Umstand überhaupt erkannt wird. Die Schlussfolgerung daraus: Bei einigen Firmen dauert es noch wesentlich länger.

»Oft muss man nur ein paar Stellschrauben drehen«

Thomas Masicek ist Head of Security Management und Chief Security Officer bei T-Systems Österreich. Er spricht über Einfallstore, Wirtschaftsspionage und Quick-Wins in der Absicherung von Systemen und Netzwerken.

VON MARTIN SZELGRAD

(+) PLUS: Wie stehen es um die IT-Sicherheit in Österreich? Warum werden Unternehmensnetzwerke und Endgeräte angegriffen?

Thomas Masicek: Die Bedrohungslage ist unverändert dramatisch – mit einer Vielzahl an Angriffen, in denen Schadsoftware zunehmend gezielt eingesetzt wird. Wir beobachten, dass viele Schadcodes vorab getestet worden sind. Diese fertigen Produkte stellen dann das Einfallstor dar, das auf einem Schwarzmarkt gehandelt wird.

Dabei ist Datendiebstahl einer der wesentlichen Treiber. Bei einem unserer Kunden hatten wir Spionageaktivitäten entdeckt. Beschädigt oder zerstört wurde zwar nichts, aber es wurden Informationen abgesaugt. Für einen Technologiekonzern etwa ist das natürlich eine heikle Sache.

(+) PLUS: Im schlimmsten Fall bemerkt man also einen Eindringling nicht?

Masicek: Wenn es die Angreifer gut machen, merken Sie nichts. Vor kurzem hatte sich ein anderes Unternehmen an uns gewandt: Wir stellten fest, dass ein Angreifer über eineinhalb Jahre unbemerkt Daten mitgeschnüffelt hatte. Das Ziel sind normalerweise sensible interne Informationen wie etwa Rezepturen, personenbezogene Daten oder Produktionsdaten, Designinformationen – einfach Daten, die in irgendeiner Form wertvoll sind. Daten sind das Öl der Zukunft und sie können schon heute entsprechenden zu Geld gemacht werden. Das betrifft aber nicht nur Technologieunternehmen. Wir hatten auch Vorfälle in der Verwaltung.

Es ist aber nicht nur dieser unmittelbare Schaden, sondern es betrifft auch das Image eines Unternehmens. Mittlerweile gibt es auch eine Meldepflicht solcher Vorfälle aufgrund der Datenschutz-Grundverordnung – es könnten ja potenziell auch personenbezogene Daten betroffen sein.

Foto: T-Systems

(+) PLUS: Wer spioniert österreichische Unternehmen aus? Der heimische Mitbewerb oder Angreifer aus fernen Ländern?

Masicek: Das ist sehr gemischt und kommt auf das Opfer an. Letztlich entscheidet die Exponiertheit eines Unternehmens über das Risiko, angegriffen zu werden. Je eher sensible Daten und Know-how in einer Organisation liegen, desto stärker droht Gefahr. Die eigenen Finger macht sich da niemand schmutzig. In der Regel hacken Organisationen auf Auftrag durch Dritte. Welcher Auftraggeber dann tatsächlich dahintersteckt, ist nur schwer nachzuvollziehen. Wir haben Lösungen, die es – wenn man die Plattform rechtzeitig etabliert – ermöglichen, Angreifer zurückzuverfolgen. Mit diesen sogenannten »Deception Technologies« werden Aktivitäten eines Angreifers genau beobachtet und es werden auch präparierte Informationen bereitgestellt.

Es müssen aber nicht immer »Targeted Attacks« sein: Sehr oft werden Unternehmen ungezielt Opfer von großflächigen Phishing-Kampagnen, die zufällig auch die eigene Domäne betreffen.

(+) PLUS: 2017 war das Jahr der großen Angriffe mit Ransomware, in denen Festplatten verschlüsselt und Unternehmen erpresst wurden. Ist das vorbei?

Masicek: Die großen Wellen sehen wir nicht mehr, Ransomware gibt es aber weiterhin – mit neuen Versionen und ausgeklügelteren Techniken. Auch heuer hat man wieder von einzelnen Hotelbetreibern lesen können, die mehrmals Opfer wurden. Und auch zu unserem Geschäftsalltag gehören regelmäßig Incidence-Response-Einsätze. Sie schaffen es nur nicht in die Presse.

(+) PLUS: Wie groß ist die eigene Schuld, wenn man Opfer einer Phishing-Attacke wird? Betrifft das eher Unternehmen, die Software-Updates vernachlässigen?

Masicek: Es gibt schon schwarze Schafe ohne Sicherheitsvorkehrungen, die der Meinung sind, Kriminelle würden sich ohnehin nicht für sie interessieren. Die Mehrzahl hat aber standardmäßig abgesicherte Systeme – trotzdem kann etwas passieren. Heutzutage ist es fast nicht möglich, sich rundum vor Angriffen zu schützen. Selbst eine auf dem neuesten Stand gehaltene Virenschutzsoftware am Arbeitsplatz erkennt neue Malware in den ersten ein bis zwei Wochen nach ihrem erstmaligen Auftreten nicht. Ist eine Phishing-Attacke dann noch authentisch gestaltet, ist dem Mitarbeiter letztendlich nichts vorzuwerfen, wenn dieser auf einen falschen Link klickt. Es braucht dann schon die perfekte Absicherung, die auch ein Erkennen von Anomalien miteinschließt. Reine Verteidigung ist heute nicht mehr ausreichend.

(+) PLUS: Was bietet T-Systems dazu für Unternehmen?

Masicek: Das beginnt bei einer Absicherung der Arbeitsplätze mit einer Endpoint-Security-Lösung, die auch Smartphones und Tablets einbezieht. Das heißt: Am Arbeitsplatz wird eine Sicherheitskonfiguration mit entsprechenden Policies gesetzt. Angriffe und Anomalien werden auf den Geräten erkannt und an ein zentrales »Security Operations Center« gemeldet.

Der zweite Teil betrifft das gesamte Unternehmensnetzwerk. Wer kommuniziert mit wem? Welche Daten werden verschickt? Mit einer Anomalie-Kontrolle können Abweichungen erkannt werden. Wir bieten dazu Security-Information- und Event-Management-Systeme, die kombiniert mit Intrusion Detection die Log-Files der Server und den gesamten Netzwerk-Traffic analysieren. Eine klassische Intrusion-Detection-Lösung liefert eine Vielzahl an Alarmen. Das kann manuell nicht mehr abgearbeitet werden. Durch die Korrelation aller Informationen und Vorfälle wird eine kleine Menge qualifizierter Alarme herausgefiltert, die rund um die Uhr von unserem Security Operations Center nachverfolgt werden können. Ein Unternehmenskunde bekommt dann Maßnahmen vorgeschlagen, um ein Problem zu beheben. Damit wird verhindert, dass jemand unentdeckt mehrere Wochen oder Monate Zugriff auf ein Netzwerk hat.

Der dritte große Themenblock ist die Absicherung von Netzwerken und Applikationen mittels Next-Generation-Firewalls. Vor allem Applikationen, die von außen erreichbar sind, benötigen entsprechenden Schutz. Das betrifft sowohl Programmierschwachstellen in der Software, die behoben werden, als auch Volumensangriffe – DDOS-Attacken –, die mit den passenden Vorkehrungen abgefangen werden können. Vor allem geschäftskritische Webservices sollten auf diese Weise abgesichert werden. Das beinhaltet auch das kategorische Ausschließen von Prozessen, die nicht ausgeführt werden sollten – beispielsweise eine Datenbank-Eingabe mittels SQL-Injection. Die sollte von Haus aus gar nicht bis zur Applikation gelangen, da sie ein sogenannter Reverse Proxy abfängt und ausfiltert.

(+) PLUS: Ist IT-Sicherheit etwas, das Unternehmen generell an spezialisierte IT-Dienstleister auslagern sollten?

Masicek: Wir sehen, dass sowohl Großkonzerne als auch der Mittelstand dieses Thema nicht mehr zu Gänze selbstständig lösen wollen. Sie haben erkannt, dass das erforderliche Personal nicht mehr verfügbar ist – siehe Fachkräftemangel am IT-Sektor. Wir haben in Österreich mittlerweile eines der größten Teams an IT-Security-Spezialisten und bieten damit auch die nötige Skalierbarkeit, Projekte unterschiedlicher Größenordnungen auch in ganz speziellen Bereichen vollumfänglich realisieren zu können.

Bei uns gibt es für jedes Thema einen Experten. Der Kunde bekommt dadurch ein ganzheitliches Service – in einer Qualität, die das Unternehmen in der Regel nie selbst schaffen würde. Informationssicherheit ist unser Kerngeschäft.

> DIE KOSTEN FÜR IT-SICHERHEIT SOLLTEN ZWISCHEN SIEBEN UND ZEHN PROZENT DES IT-BUDGETS AUSMACHEN. ALLES DARUNTER IST KLAR ZU WENIG.

(+) PLUS: Wie viel darf Informationssicherheit kosten? Was antworten Sie hier Ihren Kunden?

Masicek: In der Regel – je nachdem, in welchem Bereich ein Unternehmen tätig ist, und wie kritisch die IT fürs Geschäft ist – sind es zwischen sieben und zehn Prozent des IT-Budgets. Alles darunter ist klar zu wenig. Da fehlt dann mindestens eine Komponente, die eine Absicherung in Summe unvollständig oder ineffizient macht.

(+) PLUS: Gibt es Quick-Wins in diesem Bereich? Welche Maßnahmen raten Sie Unternehmen zur Absicherung von Daten und Systemen?

Masicek: Man sollte auf jeden Fall zuerst mit einem Security Assessment starten, um die aktuellen Sicherheitsmaßnahmen im Betrieb richtig einzuschätzen. Basierend darauf empfehle ich eine Bedrohungsanalyse mit einem Partner auszuführen, um einen gewünschten Zielzustand abzuklären. Der Weg dorthin ist dann relativ leicht. Es gibt bereits erfolgreiche Beispiele für Umsetzungen und Lösungen am Markt, Best-Practices.

Oft heißt das auch, dass man Bestehendes nicht wegschmeißen muss, sondern nur etwas anpasst. Es sind oft nur ein paar Stellschrauben, die gedreht werden müssen. Viele Unternehmen können dann die Security-Komponenten, die sie bereits im Netzwerk im Einsatz haben, wirksamer betreiben. ■

Schwachstelle Mensch

Technische Schutzmaßnahmen können noch so ausgereift sein – wenn mit Daten, Geräten und Programmen sorglos umgegangen wird, nützen sie wenig. Viele Problemfälle entstehen nicht nur durch Angriffe von außen, sondern auch durch Mitarbeiterinnen und Mitarbeiter selbst.

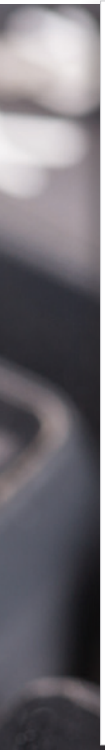
VON ANGELA HEISSENBERGER

Für IT-Sicherheit werden inzwischen enorme Summen aufgewendet. Zum einen wird Malware immer komplexer, schwieriger zu identifizieren und unschädlich zu machen; zum anderen bewirken kürzere Innovationszyklen bei Hard- und Softwarekomponenten, dass zwar stetig Sicherheitslücken geschlossen werden, gleichzeitig aber unzählige neue Schlupflöcher entstehen. Technische Lösungen für Prävention und Abwehr stehen deshalb beim Thema Cyber Security an erster Stelle.

Aus technischer Sicht durchaus nachvollziehbar: Technologien bieten mehr Angriffsflächen, die Angriffe werden immer ausgeklügelter. Das schwächste Glied in der IT ist jedoch der Mensch. Zielgerichtete Angriffe erfolgen fast immer über den »Faktor Mensch«, wie der Security-Anbieter Proofpoint in der gleichnamigen Studie aufzeigt. In der Analyse von Angriffsversuchen bei mehr als 6.000 Unternehmen weltweit wurde die direkte Kontaktaufnahme zu Nutzern als gefährlichste Schwachstelle identifiziert. »Cyberkriminelle finden immer wieder neue Wege, um unsere natürliche Neugierde, Hilfsbereitschaft oder unseren Zeitdruck ausnutzen, um uns zum Klicken zu bewegen«, sagt Werner Thalmeier, Senior Director Systems Engineering EMEA bei Proofpoint. »Unsere Untersuchungen belegen, dass es keine Alternative dazu gibt, Bedrohungen zu stoppen, bevor sie die Benutzer via E-Mail, Cloud-Anwendungen oder soziale Netzwerke erreichen.«

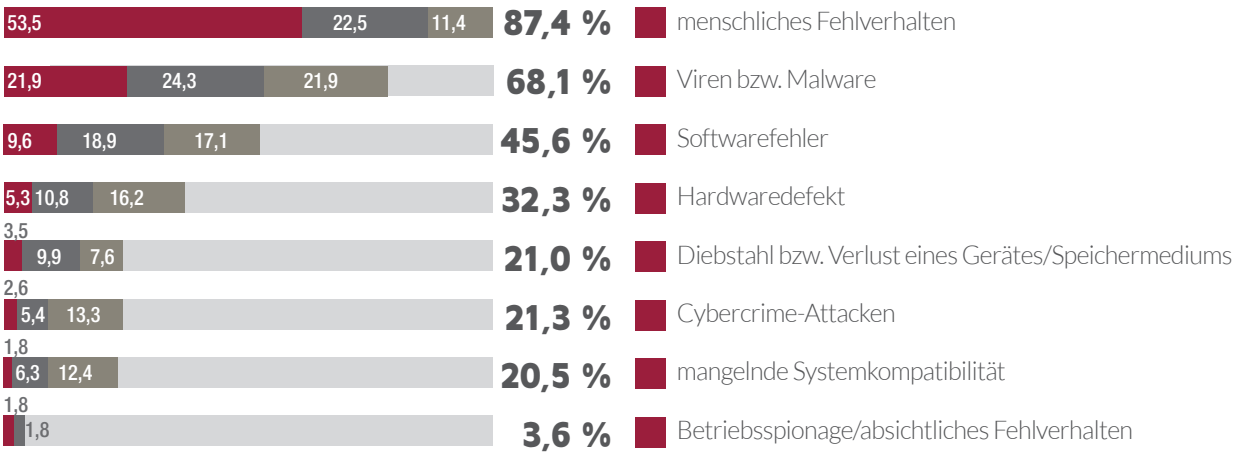
Die E-Mail ist nach wie vor der von Tätern bevorzugte Angriffsvektor. Als bester Köder bei Phishing-Attacken erwies sich ein Bezug zu Dropbox. 80 % der kriminellen Mails verteilten Ransomware und Banktrojaner. Auch die CEO-Fraud-Methode (auch Fake President Fraud) findet noch reichlich Nachahmer. Die Zahl betrügerischer E-Mails, die einen Bezug zu Rechtsberatung in

Foto: iStock



WAS SIND DIE HÄUFIGSTEN PROBLEME IM BEREICH DER IT-SICHERHEIT, MIT DENEN SICH EPU UND KMU KONFRONTIERT SEHEN?

Datenverlust und/oder Ausfall von IT-Systemen durch:



Quelle: UBIT Wien

der Betreffzeile aufwiesen, stieg im Jahresvergleich um 1.850 %. Ab September 2017 stieg infolge des Hypes um Krypto-Währungen der Datenverkehr um entsprechende Botnets um fast 90 % an.

>> Raffinierte Tricks <<

Die Vorgangsweise ist so simpel wie effektiv: Falsche Links in E-Mails oder täuschend echte Social-Media-Accounts laden zur Bestätigung ein – mit nur einem Klick findet die Schadsoftware Eingang ins Unternehmensnetzwerk. Im schlimmsten Fall sind alle Dateien zerstört, Kundendaten gestohlen oder die Täter verlangen hohe Lösegeldzahlungen in Form von Bitcoins, um die blockierten Rechner wieder freizukaufen.

Der raffinierteste Weg, um an Zugangsdaten zu kommen, ist jedoch die Manipulation von Mitarbeitern, die in gutem Glauben und teilweise unter Missachtung der Sicherheitsrichtlinien Passwörter und Interna des Unternehmens an Unbefugte weitergeben. Kriminelle erschleichen sich das Vertrauen über einen längeren Zeitraum, indem sie in vielen harmlosen Anrufen und E-Mails unter falschen Identitäten Insiderwissen signalisieren oder über Smalltalk Gepflogenheiten des Unternehmens ausspionieren. Erst nach mehreren Wochen oder gar Monaten wird die Sache konkreter: Anweisungen für Zahlungen in unterschiedlicher Höhe erfolgen, immer unter dem Deckmantel der Verschwiegenheit – es handle sich um eine dringliche, äußerst diskret zu behandelnde Angelegenheit.

Anrufe von angeblichen Kollegen, Geschäftspartnern oder der Hausbank, die zur Überprüfung nach Kontodaten oder Codes fragen, sollten deshalb ein Alarmsignal höchster Stufe sein, das sofort alle Sicherheitsmechanismen in Gang setzt. Oftmals ist jedoch das Gegenteil der Fall: Der Vorfall wird totgeschwiegen.

Eine intransparente, repressive Unternehmenskultur, in der man keine Fehler machen darf und Weisungen nicht hinterfragt werden, ist der beste Nährboden für betrügerische Angriffe. Mitarbeiter trauen sich nicht, merkwürdige Vorgänge zu melden oder in der Chefetage um Rückbestätigung zu ersuchen, ob die Weisung des Geschäftsführers auch tatsächlich echt ist. Oftmals fühlen sie sich auch geschmeichelt, für ein »Geheimprojekt« zum kleinen Kreis der Wissenden zu gehören. Das österreichische Bundeskriminalamt warnte im Vorjahr vor einem breit angelegten CEO-Fraud: Internationale Ermittlungen wiesen darauf hin, dass bis zu 500 Unternehmen in Österreich ins Visier von Cyberkriminellen geraten waren.

> Nur ein Klick öffnet der Schadsoftware den Weg ins Firmennetzwerk.

>> Teure Lektion <<

Wie aus dem Lehrbuch mutet der Fake President Fraud an, der den oberösterreichischen Flugzeugkomponentenhersteller FACC unfreiwillig in die Schlagzeilen brachte. Die Betrüger hatten eine gefälschte E-Mail-Adresse des damaligen Vorstandschefs und Firmengründers Walter Stephan eingerichtet und vorgetäuscht, es handle sich um eine streng vertrauliche Transaktion für einen Firmenkauf. Zwischen Dezember 2015 und Mitte Jänner 2016 wurden in 18 Tranchen insgesamt rund 52 Millionen Euro auf Konten in der Slowakei, Hongkong, China und Taiwan überwiesen, lediglich ein Betrag von 10,8 Millionen Euro konnte gesperrt werden. Der Schriftverkehr umfasste 48 E-Mails. Die technische Infrastruktur war nicht durch Hacker oder Schadsoftware betroffen. Den Tätern spielte in die Hände, dass FACC aufgrund seiner chinesischen Eigentümer eine besonders verschlossene Unternehmenskultur aufwies. Der mehrheitlich mit Chinesen besetzte Aufsichtsrat setzte zunächst die Finanzvorständin Minfen Gu und wenig später CEO Walter Stephan ab – er habe seine Pflichten schwerwiegend verletzt. ▶

Von einem Betrug mit ähnlicher Vorgangsweise war im August 2016 der deutsche Autozulieferer Leoni betroffen. Auch hier erfolgte kein Angriff auf die IT-Infrastruktur des Unternehmens. Mit gefälschten Dokumenten und Identitäten hatten sich Betrüger das Vertrauen von Mitarbeitern der rumänischen Tochterfirma erschlichen. Die Angreifer verfügten über detaillierte Insider-Informationen, die Zahlungsanforderungen waren von validen Vorlagen des deutschen Mutterkonzerns kaum zu unterscheiden. Rund 40 Millionen Euro landeten auf Konten in China und Hongkong, Leoni verzeichnete einen massiven Gewinneinbruch.

>> Unzureichendes Know-how <<

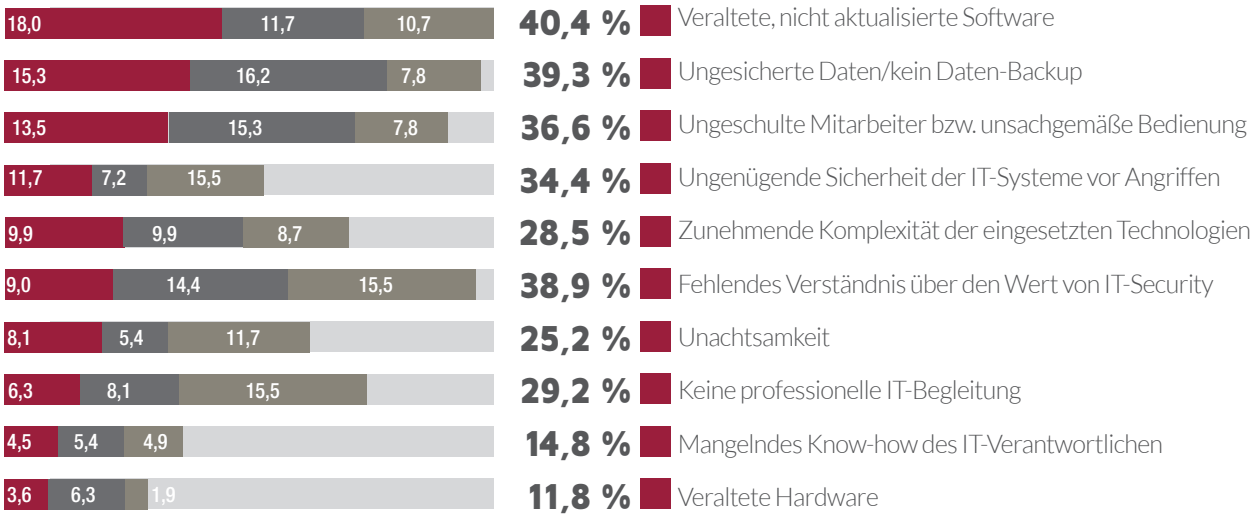
Besonders stark sind mittelständische Unternehmen von Cyberangegriffen betroffen. Während in Konzernen meist eine fundierte Sicherheitsarchitektur existiert, existieren in KMU oft nicht einmal ausreichende Firewalls und Virenscanner. Doch selbst wo diese technischen Minimallösungen vorhanden sind, mangelt es häufig am Bewusstsein der Mitarbeiterinnen und Mitarbeiter, die allzu sorglos mit Daten, Programmen und Rechnern umgehen. »Unterschätzt werden vor allem Bedrohungen, die nur schwer zu greifen sind«, bestätigt Samuel Brandstätter, CEO der avedos GRC GmbH. »Das Szenario, dass von außen versucht wird, an Unternehmensgeheimnisse zu kommen, ist real – man spürt oder sieht es aber nicht.«

IT-FEUERWEHR. Präventive Maßnahmen werden vernachlässigt. 79 % der Unternehmen wenden sich erst nach Eintritt eines Problemfalls an Spezialisten.

In einer Mitgliederumfrage der Fachgruppe für Unternehmensberatung, Buchhaltung und IT (UBIT) der Wirtschaftskammer Wien nannten die befragten IT-Dienstleister menschliches Fehlverhalten und mangelndes Verständnis im Umgang mit IT-Systemen als Hauptgründe für IT-Probleme ihrer KundInnen. »Daten zu sichern und die Software auf dem aktuellen Stand zu halten, sind elementare Maßnahmen für eine sichere IT. Das als Anwender nicht zu machen, ist ungefähr so, wie wenn man einen Motor nicht mit Öl schmiert. Ein Schaden ist dann nur eine Frage der Zeit«, verbildlicht IT-Berufsgruppensprecher Michael Schober, der die Kostenfrage angesichts eines möglichen finanziellen Schadens als Argument nicht gelten lässt: »Bei der IT zu sparen, ist eindeutig die falsche Strategie.«

Dennoch sind veraltete Software, ungesicherte Daten und fehlende Back-ups in vielen Betrieben Alltag. Oft existieren keinerlei Zutrittskontrollen, auch zu sensiblen Datensätzen haben praktisch alle Beschäftigten Zugang. Passwörter werden in Eigenregie gewählt und sind in der Regel viel zu schwach oder auf allen Rechnern identisch. »Bereits mit einfachen Maßnahmen könnten sich EPU und KMU viele Sorgen und Ärger ersparen. Mangelndes Bewusstsein und Ver-

WORIN LIEGEN DIE HÄUFIGSTEN URSACHEN FÜR PROBLEME IM BEREICH DER IT-SICHERHEIT?



Quelle: UBIT Wien

Foto: iStock

ständnis im Umgang mit IT-Systemen erhöhen jedoch das Risiko von IT-Problemen«, so Martin Puaschitz, Obmann der Fachgruppe UBIT. Dazu kommt unsachgemäße Bedienung durch ungeschulte Anwender. So berichten IT-Dienstleister von einer Arztpraxis, in der eine Ordinationshilfe als Administratorin für 20 PCs fungierte. Präventive Maßnahmen werden generell vernachlässigt: Fast 79 % der Unternehmen wenden sich jedoch erst nach Eintritt eines Problemfalls an Experten.

Gefahren drohen auch durch mobile Geräte wie Laptops, Smartphones oder Tablets, die privat und beruflich verwendet werden und ein Umgehen der Sicherheitsmechanismen an der Schnittstelle zwischen Unternehmen und Internet ermöglichen. Jörg Asma, Cybersecurity-Leader bei PwC Europe, ortet zwei gegensätzlich gepolte Haltungen: »überhöhtes Risikoverständnis«, in dem Richtlinien so stark überinterpretiert werden, dass sie dem Business nicht mehr zweckdienlich sind, oder aber ein »kaum vorhandenes Risikoverständnis«, das einem resignativen oder unbekümmerten Gefühl folgt, frei nach dem Motto »Mir wird schon nichts passieren, und wenn doch, kann man eh nichts machen«.

> Vier-Augen-Prinzip als zusätzliche Kontrollfunktion.

Hundertprozentigen Schutz gibt es nicht, denn selbst gut ausgebildeten MitarbeiterInnen unterlaufen mitunter Fehler. IT-Fachkräfte müssen kontinuierlich geschult werden, um jederzeit auf dem aktuellen Stand der Technik zu sein. Die T-Systems-Sicherheitsexperten empfehlen ein konsequentes Vier-Augen-Prinzip – beim Wechsel auf eine neue Software etwa hängt dann die Verantwortung nicht an der Leistung einer einzigen Person. Datenverluste und finanzielle Schäden können durch die zusätzliche Kontrolle minimiert werden.

>> Bewusstsein schärfen <<

»Sicherheit steht immer Benutzerfreundlichkeit entgegen. Aus diesem Grund ist Sicherheit relativ, denn das System muss zugleich für Nutzer einfach bedienbar sein«, sagt Helmut Leopold, Head of Center for Digital Safety & Security am Austrian Institute of Technology (AIT). »Wenn ein zu geringes Bewusstsein des Bedrohungspotenzials und der möglichen Konsequenzen von Cyberattacken vorhanden ist, werden ein höherer Aufwand in der Bedienung oder höhere Kosten nicht akzeptiert.«

Zugleich gilt es, das Bewusstsein zu schärfen. IT-Sicherheit ist Chefsache und sollte alle Unternehmensbereiche umfassen, auch jene, die von Digitalisierung und Vernetzung bisher nicht betroffen waren. Welche Bedrohungen im Internet lauern, muss aber allen Mitarbeiterinnen und Mitarbeitern klar sein. Klare Verhaltensregeln und Sicherheitsstandards tragen wesentlich dazu bei, die Risiken zu senken. Laut der diesjährigen KPMG-Studie »Cyber Security in Österreich« betrachten allerdings 70 % der Führungskräfte IT-Sicherheit eher als technische Angelegenheit. Angriffe, die sich die Gutgläubigkeit und Neugierde der MitarbeiterInnen zunutze machen, sind somit wohl weiterhin höchst effizient. ■

GEGEN DIE DATENKRAKE, FÜR DEN WIRTSCHAFTS

VON MARTIN SZELGRAD

Das Inkrafttreten der Datenschutz-Grundverordnung mit 25. Mai dieses Jahres hatte das Thema Datenschutz stärker ins öffentliche Bewusstsein gerückt – positiv formuliert. In der Wirtschaft wuchsen die Fragen zu den Regelungen und Pflichten durch die DSGVO zu einem regelrechten Hype, der mit dem Näherkommen der Deadline fast zur Raserei ausartete. »Die meisten hatten ein halbes Jahr vor Inkrafttreten des Gesetzes ihren Anwalt zum ersten Mal dazu befragt. Nun ist Datenschutzgesetzgebung generell sehr komplex«, weist Max Schrems im Interview (Seite 10) auf ein Dilemma hin, das viele betraf: der »Hausanwalt« der Unternehmen war mit den Fragestellungen überfordert. Mit der großen europäischen Datenschutz-Regelung hatten die Unternehmerinnen und Unternehmer auch in Österreich »juristisches Spezialgebiet« betreten.

Aber, so relativiert auch Schrems: »Jene, die sorgsam mit personenbezogenen Daten umgehen und Datenschutz ernst nehmen, haben keinerlei Probleme mit der DSGVO.«

Gut fünf Monate später steht das Abendland immer noch. Die Millionenstrafen, die bei Verstößen drohen, sind bislang ausgeblieben. Doch wenn der Datenschutzstandard davor schon in Österreich und Europa vergleichsweise hoch war, hat der neue Rechtsrahmen mit Sanktionsmöglichkeiten nachgelegt, die auch immateriellen Schaden berücksichtigen. Prompt wurde die DSGVO von Datenschützern als Meilenstein bezeichnet. »Es gibt nun auch neue Tools für die Rechtsdurchsetzung in der Praxis. Sie sorgen dafür, dass das Regelwerk ernst genommen wird«, ist Petra Leupold, Leiterin der VKI-Akademie, überzeugt. »Die großen Player, die auch als Datenkraken bezeichnet werden, sitzen typischerweise nicht in Österreich. Die DSGVO hat nun zur Ausweitung des europäischen Datenschutzes auch auf diese Unternehmen geführt«, argumentiert die Juristin. Eine Niederlassung in Europa sei nicht mehr Voraussetzung, auch US-Anbieter mit hiesigem Geschäft müssen sich an die Datenschutzregeln halten. Es ist eine Erfolgsgeschichte der EU. Der »Gold-Standard« des

RECHTE FÜR KONSUMENTINNEN

Recht auf Auskunft. Auf Anfrage müssen Unternehmen sämtliche personenbezogenen Daten umfassend, kostenlos und grundsätzlich innerhalb eines Monats mitteilen. Dies betrifft Daten, die vom Unternehmen erhoben und verarbeitet werden, zu welchem Zweck sie verwendet werden und an wen sie weitergegeben werden.

Recht auf Datenübertragbarkeit. Bei einem Wechsel eines Dienstleisters können KundInnen personenbezogene Daten transferieren. Damit wird ein Schutz des freien Verkehrs personenbezogener Daten gewährleistet. Erleichtert wird dadurch auch die Kontrolle über die eigenen Daten.

Recht auf Entscheidungen durch eine natürliche Person. Rein auf Algorithmen gestützte Entscheidungsfindungen sind nicht zulässig – etwa bei Scoring-Modellen.

Foto: iStock, VKI

Ansichten und Einsichten zum Hype-Thema rund um die europäische Datenschutz-Grundverordnung. Was die Unternehmen erwartet. Wer Hilfestellungen bietet.

STANDORT

Petra Leupold, Juristin und Leiterin der VKI Akademie, warnt Unternehmen vor der Praxis des – von den großen Social-Media-Plattformen praktizierten – »Forced Consent«: »Wenn die Einwilligung in die Erhebung und Verarbeitung von Daten nicht freiwillig und ohne Zwang geschieht, ist sie unwirksam und unzulässig.«

Datenschutzes könnte zu einem Exportgut der Union werden. »Die Message ist angekommen«, meint Leupold. Man werde nun sehen, wie sich die Konzerne – vor allem im Silicon Valley – verhalten.

>> Unterschiedliche Reaktionen <<

Wellen schlägt das Thema jedenfalls in Übersee, und damit hat die DSGVO teilweise, zumindest indirekt zu tun. Ende Oktober hielt Apple-CEO Tim Cook auf dem Branchentreff »International Conference of Data Protection and Privacy Commissioners« eine Ansprache zum Thema Datenschutz und wählte dabei durchaus drastische Worte. Cook spricht – auch mit Seitenhieb auf die großen Konkurrenten Google und Facebook –von der Entstehung eines »Daten-industriellen-Komplexes« und führt aus: »Unsere persönlichen Daten – von alltäglichen bis hin zu sehr privaten – werden mit militärischer Effizienz als Waffen gegen uns selbst eingesetzt«.

Sind sich nun die Österreicherinnen und Österreicher den Vorgaben und Zielen der DSGVO bewusst? Man könnte sagen: teilweise sind sie es. Gut zwei Monate nach Inkrafttreten der Sanktionsmöglichkeiten waren bei der Datenschutzbehörde bereits so viele Beschwerden eingebracht, wie im gesamten Jahr 2017. Das Anziehen der Höhen der Strafen hat Leupold zufolge aber vor allem das Bewusstsein bei den Unternehmen geschürt. Konnten die maximal 25.000 Euro hohen Pönalen bei gröberen Datenschutzverletzungen früher sprichwörtlich aus der Portokasse bezahlt werden, treiben Höhen von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes mancher Geschäftsleitung die Sorgenfalten auf die Stirn.

> „IM VERGLEICH ZUM FRÜHJAHR HAT SICH DIE SITUATION IN DEN HEIMISCHEN BETRIEBEN ZWAR DEUTLICH GEBESSERT, INSGESAMT IST DAS ABER NOCH ZU WENIG."

>> Stand im Alpenland <<

Es könnte wesentlich besser sein: Einer aktuellen Umfrage des Kreditschutzverband 1870 zufolge hinkt ein Großteil der Unternehmen den gesetzlichen Anforderungen für datenschutzkonforme Unternehmensprozesse und Services hinterher. Sechs von zehn Unternehmen haben die gesetzlichen Vorgaben nicht vollständig erfüllt. Acht Prozent aller Firmen haben aktuell mit der Umsetzung noch gar nicht begonnen. Kurz vor dem Inkrafttreten der EU-DSGVO im Mai 2018 waren es 30 %. Insbesondere die kleinen Unternehmen müssen noch aufholen: Lediglich 38 % agieren so, wie es die neue Verordnung vorsieht.

»Im Vergleich zum Frühjahr hat sich die Situation in den heimischen Betrieben zwar deutlich gebessert, insgesamt ist das aber noch zu wenig. Ein Großteil der Unternehmen hat noch einiges zu tun, bis sämtliche DSGVO-Maßnahmen realisiert sind«, kommentiert KSV1870-Vorstand Ricardo-José Vybiral die Ergebnisse.

Während ungefähr zwei Drittel (67 %) der Großunternehmen bereits sämtliche Kriterien erfüllt haben, weisen Betriebe bis zu einer Größe von maximal 20 Mitarbeitern weiterhin den größten Aufholbedarf auf. ■

»DER DRUCK AUF DIE EINKAUFSABTEILUNGEN IST HOCH«

Die Verschränkung von Datenschutz und IT-Sicherheit ist für Roland Marko, Partner bei Wolf Theiss Rechtsanwälte, das große Thema. Der Experte mit Beratungsschwerpunkt IT-Recht spricht über sichere Geschäftskommunikation und Zertifizierungen.

Roland Marko, Wolf Theiss, ist als Rechtsanwalt auf IT-Recht spezialisiert und als Auditor tätig.

(+) PLUS: Welcher Zusammenhang besteht zwischen Datenschutz und Informationssicherheit?

Roland Marko: Diese Verschränkung ist zum einen gesetzlich vorgegeben. Personenbezogene Daten sind eine Unterkategorie aller Informationen, die in Unternehmen verarbeitet werden. Die Datenschutz-Grundverordnung schreibt insofern auch technische und organisatorische Maßnahmen vor, um ein angemessenes Sicherheitsniveau für die Daten vorzukehren. Man spricht hier von der Trias »Confidentiality, Integrity und Availability«, also von Vertraulichkeit, Integrität und Verfügbarkeit. Dies sind die Eckpfeiler der Daten- und Informationssicherheit. Letztere schließt neben personenbezogenen Daten auch sonstige Unternehmensinformationen, wie insbesondere Geschäfts- und Betriebsgeheimnisse ein, die ebenfalls von einem hohen Wert für Unternehmen sein können.

Zum anderen sehen wir den Zusammenhang auch in den täglichen Abläufen und Systemen in Unternehmen: Von der Stechuhr der Mitarbeiter über diverse Monitoring-Maßnahmen für die IT-Sicherheit im Hintergrund, bis hin zur eigentlichen Personalverarbeitung – das alles ist mittlerweile stark datengetrieben. Und es wird weiter zunehmen, auch in Branchen, die bislang nicht klassisch digitalisiert waren. Der Datenhunger wächst etwa auch in der Bauwirtschaft, wenn zum Beispiel ein Generalunternehmen die Einhaltung rechtlicher Vorgaben durch die Subunternehmer auf der Baustelle dokumentieren muss und selbst dort zunehmend IT-Plattformen und Applikationen eingesetzt werden. Betroffene Unternehmen, die dazu Daten liefern müssen, haben sich dann der Frage zu stellen, was davon aus Datenschutzgründen legitim ist und auch Informationssicherheitsanforderungen genügt.

Übrigens gelten für die Geschäftskommunikation die großen Messenger-Dienste wie WhatsApp nicht ohne Einschränkung als sicher. Wir haben schon beobachtet, dass Unternehmen hier einseitig diesen Kommunikationsweg vorgeben. Wichtig ist, dieses Thema mit Richtlinien oder Arbeitsanweisungen für alle Mitarbeiter greifbar und lebbar zu machen. Die sicheren alternativen IT-Werkzeuge dazu gibt es jedenfalls.

(+) PLUS: Personenbezogene Daten einfach per Mail schicken – das geht nicht?

Marko: Die Frage ist, ob das Sicherheitsniveau des Kommunikationsmittels der Sensibilität der übermittelten Information angemessen ist. Je sensibler die Information, umso höher der anzulegende Sicherheitsmaßstab. Wenn man für sensible Information E-Mail-Kommunikation vermeiden kann, sollte man andere Kanäle nutzen. Es gibt Systeme, die mit Upload- und Download-Schnittstellen einen vollständig sicheren Datenverkehr ermöglichen – beispielsweise auch für einen Arzt, der Befunde mit einem Labor austauscht. Wenn aber Mails oder Dateianhänge zumindest verschlüsselt werden, wird schon ein wesentlich höherer Sicherheitsgrad geschaffen. Es gibt auch Messenger-Dienste, die durch Verschlüsselung aber auch hinsichtlich des Datenstandorts »sicherer« als andere sind. Das betrifft nicht nur die Herkunft des IT-Dienstleisters sondern auch die vor Ort vorherrschenden gesetzlichen Rahmenbedingungen für behördliche Zugriffe auf Daten.

(+) PLUS: Sind hier europäische IT-Dienstleister gegenüber etwa Cloud-Provi-

dern aus den USA im Vorteil? Wird das Thema Datenschutz von Grund an anders gehandhabt?

Marko: Die Datenschutz-Grundverordnung hat zwei neue Aspekte eingebracht: »Privacy by Design« und »Privacy by Default«. Übersetzt bedeutet das datenschutzfreundliche Grundeinstellungen und Datenschutz durch Technikgestaltung, die in Diensten und Services von Anfang an mitbedacht sein müssen. Demnach müssen Hersteller und Provider ihre Produkte und Services letztlich so gestalten, dass die Anwender damit rechtskonform arbeiten können, andernfalls diese nicht marktfähig sein werden.

Hier sind die Anforderungen zweifellos in die Höhe geschraubt worden. Der Druck auf die Einkaufsabteilungen, die über den Kauf von Software entscheiden, die Datenschutzkonformität richtig einzuschätzen, ist hoch. Sie müssen sich gemeinsam mit der Rechts- oder Compliance-Abteilung dazu Gedanken machen.

(+) PLUS: Behaupten kann man so etwas leicht – aber wie kann ein Anbieter nachweisen, dass sein Produkt oder Service DSGVO-konform gestaltet ist?

> ES GIBT ZERTIFIZIERUNGEN, DIE DURCH **DIE DSGVO NUNMEHR AUCH RECHTLICH** VERANKERT WERDEN. AUCH DIE ISO-NORMEN HABEN EINE HOHE ANERKENNUNG IM MARKT.

Marko: Es gibt Zertifizierungen, die durch die DGSVO nunmehr auch rechtlich verankert werden. Sie entlasten bis zu einem gewissen Grad die Einkaufsabteilungen, da hier ein unabhängiger Dritter – das können eine Datenschutzbehörde, der TÜV oder andere privatwirtschaftliche Organisationen sein – eine entsprechende Prüfung durchgeführt hat.

Unterschieden wird zwischen reinen IT-Sicherheitszertifikaten, die klassischen ISO-Normen wie 27001, 27002 und auch ISO 27018 für die Verarbeitung personenbezogener Daten in Public Clouds. Die ISO-Normen sind zwar noch nicht rechtlich als DSGVO-Norm anerkannt, haben aber prinzipiell eine hohe Anerkennung im Markt. Wir gehen davon aus, dass diese und andere Standards jedenfalls wichtiger werden.

Im Bereich Datenschutz bietet auch unsere Kanzlei Audits nach dem europäischen Datenschutz-Gütesiegel »European Privacy Seal – EuroPriSe« an. Der Vorteil liegt hier in den Zertifizierungskriterien, die ein Softwareprodukt oder einen IT-Service technisch und rechtlich durchleuchten und damit sowohl Datenschutz als auch Datensicherheit gleichermaßen berücksichtigen. ■

WIE GEHT MEIN UNTERNEHMEN MIT SICHERHEITSPROBLEMEN UM?

Eine Auswahl wichtiger Fragen von UnternehmensentscheiderInnen an ihre IT-Verantwortlichen zur Einschätzung der IT-Sicherheitslage eines Unternehmens.

Diese Liste des österreichischen nationale CERT (Computer Emergency Response Team) spricht organisatorische Themen abseits der rein technisch fokussierten Maßnahmen wie etwa Backup, Passwortrichtlinien oder physikalische Sicherheit an.

>> Informationsfluss <<

- Wie und vor allem wer erfährt im Unternehmen von IT-Sicherheitsproblemen (wenn beispielsweise Dritte eine Sicherheitslücke melden)?
- Gibt es dazu eine klar definierte Prozesskette, wie Meldungen & Eskalationen zu erfolgen haben?
- Verfügt das Unternehmen über ein entsprechendes Social-Media- bzw. Medienmonitoring, um allfällige Sicherheitsvorfälle in Verbindung mit dem eigenen Firmen- oder Produktnamen selbst erkennen zu können, sobald berichtet wird?

>> Verantwortlichkeiten <<

- Gibt es im Unternehmen für alle Systeme und Services klare Verantwortlichkeiten mit entsprechenden Stellvertretungsregelungen?

>> Abläufe <<

- Wenn ein IT-Sicherheitsvorfall eingetreten ist: Gibt es entsprechende Einsatz- oder Ablaufpläne? (Idealerweise nach unterschiedlichen Kategorien sortiert).

>> Erreichbarkeit <<

- Ist die Erreichbarkeit der wichtigsten Unternehmensbereiche (Geschäftsführung, Technik, PR) auch außerhalb der Bürozeiten sichergestellt?

>> Vertrauenswürdigkeit der Dienstleister <<

- Sind alle extern zugekauften Dienstleistungen (von Co-Location bis hin zur Cloud) mit entsprechenden Security Service-Level-Agreements versehen, als vertrauenswürdig einzustufen und verfügen die Dienstleister über eine entsprechende Zertifizierung (z.B. ISO 27001)?

>> Versicherung <<

- Welche IT-Risiken eines Unternehmens sind prinzipiell versicherbar?
- Bei welchen könnte das aus Sicht des Unternehmens auch wirtschaftlich vernünftig sein?

>> Eigene Zertifizierung <<

- Was wäre der Aufwand einer IT-Security-Zertifizierung (z.B. ISO 27001) und was der potenzielle Nutzen aus Sicht des Unternehmens (Sicht von IT, Marketing, neuen Auftragsmöglichkeiten)?
- Ist das Unternehmen hinsichtlich NIS-Richtlinie selbst der »kritischen Infrastruktur« zuzuordnen?
- Wenn ja: Wie ist das Unternehmen auf die Anforderungen der europäischen NIS-Richtlinie vorbereitet?

>> Investitionen <<

- Wieviel Aufwand (personell, finanziell) wird derzeit in IT-Security-Themen investiert?
- Wie ist das Verhältnis von reiner Angriffs-Abwehr (Prävention) zu Erkennung erfolgreicher Angriffe (Detection) im Unternehmen?

>> Verhaltensregeln <<

- Gibt es im Unternehmen klare Richtlinien zu Privatnutzung, Verhaltensregeln und Themen wie Smartphones/Tablets?
- Kann jedes Gerät im Unternehmensnetzwerk einem Benutzer bzw. einem Verantwortlichen zugeordnet werden und ist sichergestellt, dass alle Geräte auf aktuellem Stand und sicher konfiguriert sind?

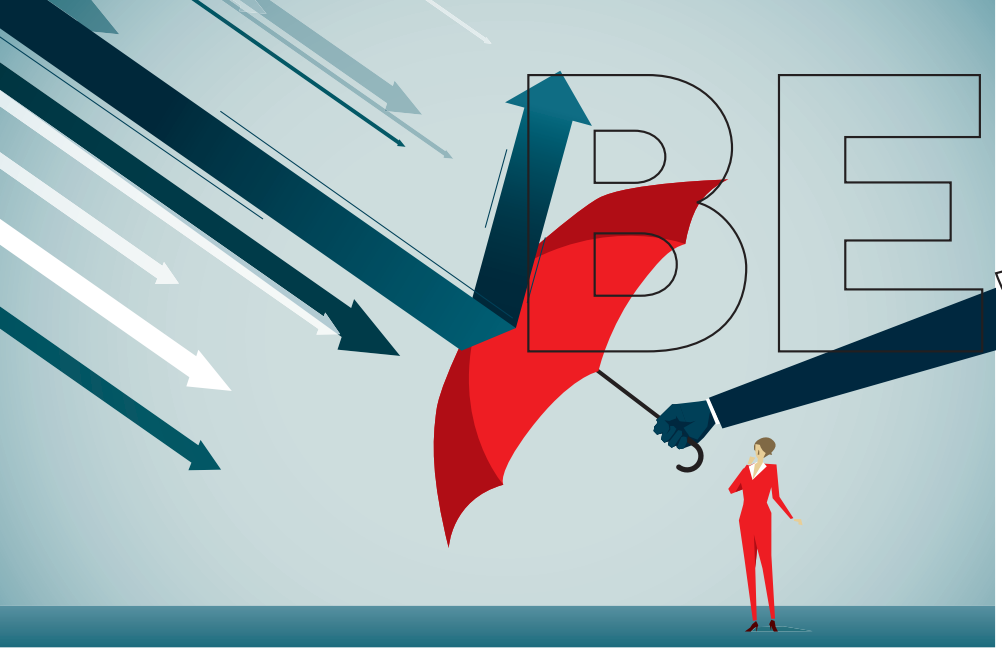
Sollten Unklarheiten oder weitere offene Fragen auftauchen, empfehlen CERT.at und GovCERT.gv.at Firmen, sich intern wie auch extern – etwa durch SicherheitsexpertInnen – näher mit IT-Sicherheit zu befassen.

BUCHTIPP

FÜR UNTERNEHMER

Der neue DatKomm. Der »DatKomm – Praxiskommentar zum Datenschutzrecht (DSGVO und DSG)« stellt sich den wirklich schwierigen Fragen, die im Zusammenhang mit dem neuen Datenschutzregime auftauchen. Dem Aufbau der DSGVO folgend werden die jeweils passenden Bestimmungen des österreichischen DSG gleich »mitgenommen«. Die Kommentierung bezieht sich auf beide Normen und behandelt inhaltlich sinnvoll verschränkt und tiefgehend die wesentlichen Auslegungsschritte, wichtige Literatur und Judikatur – auch zu bisher geltendem Recht – inklusive. Anhänge mit Guidelines und Beschlüssen des Datenschutzausschusses, wichtigen Bestimmungen aus Nebennormen, wie zum Beispiel der Richtlinien über Polizei und Strafjustiz, runden den Praxiskommentar ab. Erarbeitet wurde die fundierte Rechtsinformation von einem 33-köpfigen Autorenteam.

Titel: »DatKomm – Praxiskommentar zum Datenschutzrecht (DSGVO und DSG)«,
Herausgeber: Rainer Knyrim
1024 Seiten, 198 Euro
Reihe: Manz Großkommentare, 2018
Verlag: MANZ Verlag Wien
ISBN: 978-3-214-17236-7



BEST PRACTICE

DATENSCHUTZ AUS EINEM GUSS

DER BAUSTOFFSPEZIALIST WIENERBERGER HAT NAHEZU ALLE PROZESSE, DIE FÜR DIE EINHALTUNG DER DSGVO NÖTIG SIND, AUF EINER HOCHSICHEREN CLOUD-PLATTFORM LAUFEN. DIE USERFREUNDLICHE LÖSUNG VERURSACHT NUR MINIMALEN ADMINISTRATIONSAUFWAND.

Die Vielfalt der Niederlassungen von Wienerberger hängt mit dem Geschäftsmodell zusammen. Weil Ziegel, Rohrsysteme und Betonsteine nicht weit transportiert werden können, produziert der Baustoffspezialist in Zentral- und Osteuropa sowie in Nordamerika lokal an knapp 200 Produktionsstandorten.

Das Inkrafttreten der europäischen Datenschutzgrundverordnung hat Wienerberger vor die Herausforderung gestellt, ein funktionierendes Tool zu implementieren, das dem Unternehmen auch in seiner länderspezifisch unterschiedlichen Struktur hilft und die gesetzlichen Anforderungen erfüllt.

Dass die Wahl am Ende auf eine Datenschutzmanagementlösung von T-Systems gefallen ist, lag zunächst einmal an der hohen Sicherheits- und Datenschutzexpertise, die die Österreich-Tochter der Deutschen Telekom mitbringt. Schließlich ist für eine gesetzeskonforme Verarbeitung von personenbezogenen Daten die sichere Speicherung eine Grundvoraussetzung. Die Daten für die Wienerberger-Lösung werden daher in einer mehrfach abgesicherten GRC-Cloud gelagert, die dazugehörige Infrastruktur befindet sich im Twin Core-Rechenzentrum des IT-Dienstleisters in Wien. Die Benutzerkonten und Benutzerrechte werden ebenfalls gemanagt, was ein zusätzliches Sicherheitsplus ergibt.

> „WEIL DIE GESAMTE LÖSUNG IN DER CLOUD BETRIEBEN WIRD, MUSS SICH WIENERBERGER NICHT MIT UPDATES UND PATCHES HERUMSCHLAGEN."

>> Voller Service <<

Doch die GRC-Cloud – GRC steht für Governance, Risk and Compliance – hat noch einen weiteren Vorteil: »Weil die gesamte Lösung von T-Systems in der Cloud betrieben wird, müssen wir uns nicht mit Updates, Patches und sonstigen Revisionen herumschlagen. Wir bekommen das gar nicht mit«, erklärt Christoph Schacher, Corporate Information Security Manager bei Wienerberger. Nachsatz: »Okay, manchmal kommt eine E-Mail, dass das System am Wochenende kurz down sein wird. Das war's dann aber wirklich.«

Die Datenschutzmanagementlösung ist vorkonfiguriert und somit schnell einsetzbar, zugleich aber mit wenig Aufwand auch an sehr unterschiedliche konkrete Anwendungssituationen anpassbar. Risk2value, wie die dafür verwendete GRC Software von Avedos heißt, ermöglicht in Verbindung mit den von T-Systems entwickelten Kontrollkatalogen, Workflows und Prozessen den DSVGO-Verantwortlichen in den einzelnen Bereichen des Unternehmens nicht nur mögliche Verstöße gegen die EU-DSGVO aufzudecken, sondern sie bietet auch Lösungen an, die – wieder direkt über die Plattform – gesetzt werden können, um zu einem rechtskonformen Status zu kommen. Und sie schlägt auch Routinen vor, die gewährleisten, dass der rechtskonforme Status auch langfristig erhalten bleibt. Zudem erlaubt die Plattform die Erweiterung des reinen Datenschutzmanagements zu einem umfassenden Informationssicherheitssystem und Risikomanagement.

>> Erfahrung als Asset <<

In seinem Kern umfasst die Datenschutzmanagementlösung alle zur Einhaltung der EU-DSVGO notwendigen Tools, also ein revisionssicheres Datenanwendungsverzeichnis, die Durchführung und Dokumentation von benötigten Datenschutzfolgeabschätzungen sowie Workflows für die Bearbeitung von Datenpannen und Anfragen gemäß EU-DSGVO.

Zu einer Anwendung mit Mehrwert wird das System aber durch das DSVGO-spezifische Know-how. »Es war schon sehr stark zu merken, dass die Kollegen von T-Systems nicht nur Daten- und IT-Spezialisten sind, sondern auch bei der Umsetzung der gesetzlichen Vorgaben in der Praxis bereits sehr viel Erfahrung haben«, blickt der Wienerberger-CISO Christoph Schacher auf das Projekt zurück. »Sie wissen wirklich auch in praktischer Hinsicht, wovon sie reden.«

>> Blick für die Praxis <<

Praxisorientiert ist auch das Frontend des Systems, das mit übersichtlichen Zuordnungen von potenziellen Gefahren zu Farben arbeitet und so zunächst einmal jedes Szenario in die Grundkategorien Rot (sehr sensibel), Orange, Gelb und Grün einteilt. Die Implementierung der Lösung bei Wienerberger ist ebenfalls sehr userfreundlich abgelaufen – mit Onlineschulungen, die nicht nur den Umgang mit der Software zeigten, sondern zugleich auch eine, jeweils dem Anwenderlevel angepasste, Einführung in die EU-DSGVO enthielten. ■

Foto: iStock

»DATENSCHUTZ IST EIN GRUNDRECHT«

Andrea Jelinek, Leiterin der österreichischen Datenschutzbehörde, wacht über die Einhaltung der Datenschutzgrundverordnung (DSGVO). Im Report(+)PLUS-Interview zieht sie eine erste Bilanz.

VON ANGELA HEISSENBERGER

(+) PLUS: Seit 25. Mai ist die DSGVO in Kraft. Haben sich die Wogen inzwischen gelegt?

Andrea Jelinek: Die DSGVO hat bewirkt, dass Datenschutz einen anderen Stellenwert eingenommen hat. Unternehmen und Behörden haben begonnen, sich intensiver damit auseinanderzusetzen und interne Prozesse zu adaptieren. Auch außereuropäische Länder machen sich mehr Gedanken und planen, Datenschutzgesetze zu verabschieden oder zu verbessern.

Die Datenschutzbehörde ist seit 25. Mai – im Vergleich zum Vorjahr – verstärkt befasst worden. Während im gesamten Jahr 2017 circa 490 Beschwerden bzw. Eingaben zu verzeichnen waren, sind es seit Mai 2018 über 1.000, Tendenz steigend. Dies zeigt, dass datenschutzrechtliche Fragen stärker in den Mittelpunkt gerückt wurden.

(+) PLUS: Anfangs zeigten sich viele Unternehmer noch recht gleichgültig, je näher der Mai rückte, desto größer wurde die Aufregung. Waren Sie von den heftigen Reaktionen überrascht?

Jelinek: Im Vorfeld des 25. Mai wurde über die DSGVO viel berichtet und es gab unzählige Veranstaltungen, um die Thematik zu erklären. So war auch die Datenschutzbehörde mit einer Vielzahl an Anfragen beschäftigt. Fakt ist, dass seit dem 25. Mai ein starker Anstieg an Beschwerden zu verzeichnen ist, die große Aufregung hat sich jedoch gelegt und der Umgang mit der DSGVO beginnt sich zu »normalisieren«.

(+) PLUS: Vor allem der hohe Strafrahmen sorgt für Empörung. Wurden bereits Strafen verhängt?

Jelinek: Die Datenschutzbehörde hat bereits Geldstrafen verhängt, die jedoch sehr weit vom möglichen Höchstrahmen von 20 Millionen Euro entfernt sind. Bei der Verhängung von Geldstrafen sind nämlich immer die Verhältnismäßigkeit und auch die finanzielle Leistungskraft des Beschuldigten zu beachten, was selbstverständlich geschieht. Die Datenschutzbehörde hat auch schon Verwarnungen ausgesprochen.

(+) PLUS: Braucht es hohe Strafen, damit das Thema ernst genommen wird?

Jelinek: Wie es scheint, ist der mögliche Strafrahmen auch ein Grund, weshalb das Thema Datenschutz nunmehr Beachtung findet. Dies ist insofern schade, als Datenschutz ein Grundrecht ist. Wenn Datenschutz ernst genommen wird, bringt er auch einen wirtschaftlichen Vorteil für Unternehmen, indem nachgewiesen wird, dass mit Kundendaten sorgfältig umgegangen wird. Das Vertrauen der Kunden ist ein unverzichtbarer Bestandteil des Wirtschaftslebens.

(+) PLUS: Einer der Gründe für die Einführung der DSGVO war Entbürokratisierung. Die Unternehmen klagen aber gerade über den großen Aufwand für die Umsetzung. Zu Recht?

Jelinek: Zirka 80 % des Inhalts der

Fotos: iStock, EDPB

ZUR PERSON

Andrea Jelinek, geb. 1961, studierte Rechtswissenschaften an der Universität Wien und kam 1991 als juristische Referentin ins Generalsekretariat der Österreichischen Rektorenkonferenz. Zwei Jahre später wechselte Jelinek ins Innenministerium, wo sie zunächst als Referentin, später als Leiterin der Legistikabteilung tätig war.
2003 wurde die Juristin und Führungskräftetrainerin als erste Frau zur Leiterin eines Polizeikommissariats ernannt. Von Oktober 2010 bis Juni 2011 übernahm sie die Leitung der Wiener Fremdenpolizei.
Seit 2014 steht Andrea Jelinek der österreichischen Datenschutzbehörde vor, die die frühere Datenschutzkommission im Bundeskanzleramt ersetzte. Sie ist außerdem Vorsitzende des Europäischen Datenschutzausschusses (EDSA) in Brüssel.

DSGVO gilt bereits seit den 90er-Jahren bzw. in Österreich sogar seit 1980. Wer Datenschutz schon vor dem 25. Mai 2018 ernst genommen hat, musste nicht viel ändern und anpassen.

(+) PLUS: Wie stark wurde die Datenschutzbehörde personell aufgestockt?

Jelinek: Die Datenschutzbehörde wurde um insgesamt sechs Planstellen im juristischen Bereich aufgestockt. Außerdem wurden Mittel für zusätzliches Kanzleipersonal zur Verfügung gestellt.

(+) PLUS: Welche Unternehmen werden zuerst geprüft?

Jelinek: Die Datenschutzbehörde prüft einerseits, wenn Beschwerden einlangen; davon kann jedes Unternehmen betroffen sein. Schwerpunktaktionen werden in Bereichen gesetzt, wo es vermehrt Beschwerden gibt oder wo Daten in großem Umfang verarbeitet werden.

(+) PLUS: Kommen auch verstärkt Anfragen von Konsumentinnen und Konsumenten?

Jelinek: Anfragen kommen aus allen Bereichen und von allen Personengruppen.

(+) PLUS: Trägt die DSGVO zu einem bewussteren Umgang der Bevölkerung mit Daten bei?

Jelinek: Die DSGVO hat zumindest dafür gesorgt, dass diesem Thema eine erhöhte Aufmerksamkeit zukommt.

(+) PLUS: Welche Ausrede können Sie nicht mehr hören?

Jelinek: Ausreden werden an die Datenschutzbehörde nicht herangetragen. ■

DATENSCHUTZ IN ÖSTERREICH

Österreich richtete 1978 als einer der ersten europäischen Staaten eine eigene Behörde für Datenschutz, die »Datenschutzkommission«, ein. Mit der Datenschutzrichtlinie der EU wurde das Datenschutzrecht in ganz Europa neu geregelt; in Österreich floss diese Richtlinie in das Datenschutzgesetz 2000 ein.

Am 25. Mai 2018 traten die Bestimmungen der europäischen DSGVO und des überarbeiteten österreichischen Datenschutzgesetzes in Kraft. Die Datenschutzbehörde (DSB) sorgt für die Einhaltung des Datenschutzes in Österreich. Betroffene können sich wegen Verletzung ihrer Rechte bzw. Verletzung der Pflichten eines Auftraggebers oder Dienstleisters mit einer Eingabe an die DSB wenden. Im Fall eines begründeten Verdachtes kann die DSB vom Auftraggeber oder Dienstleister alle notwendigen Aufklärungen verlangen und Einschau in Datenanwendungen und diesbezügliche Unterlagen nehmen. Darüber hinaus kann die DSB jederzeit bei Routinekontrollen die Einhaltung der DSGVO prüfen und Strafen verhängen.

RUND UM DIE UHR RUNDUM SICHER

mit Incident Response von T-Systems

Cyber-Kriminalität ist zu einer realen Herausforderung geworden. Trotz fundierter Vorkehrungen gibt es jedoch keine absolute Sicherheit. Die digitalisierte Welt stellt Unternehmen vor vielfältige Herausforderungen, besonders die Sicherheit rückt hier immer wieder in den kritischen Fokus. System- und Netzwerkadministratoren sind kaum noch in der Lage, eine ganze Organisation alleine vor derartigen Angriffen zu schützen. Der einzige effiziente Weg ist eine vielschichtige und umfassende Security-Strategie, die einen Notfallplan für einen Cyber-Angriff parat hält.

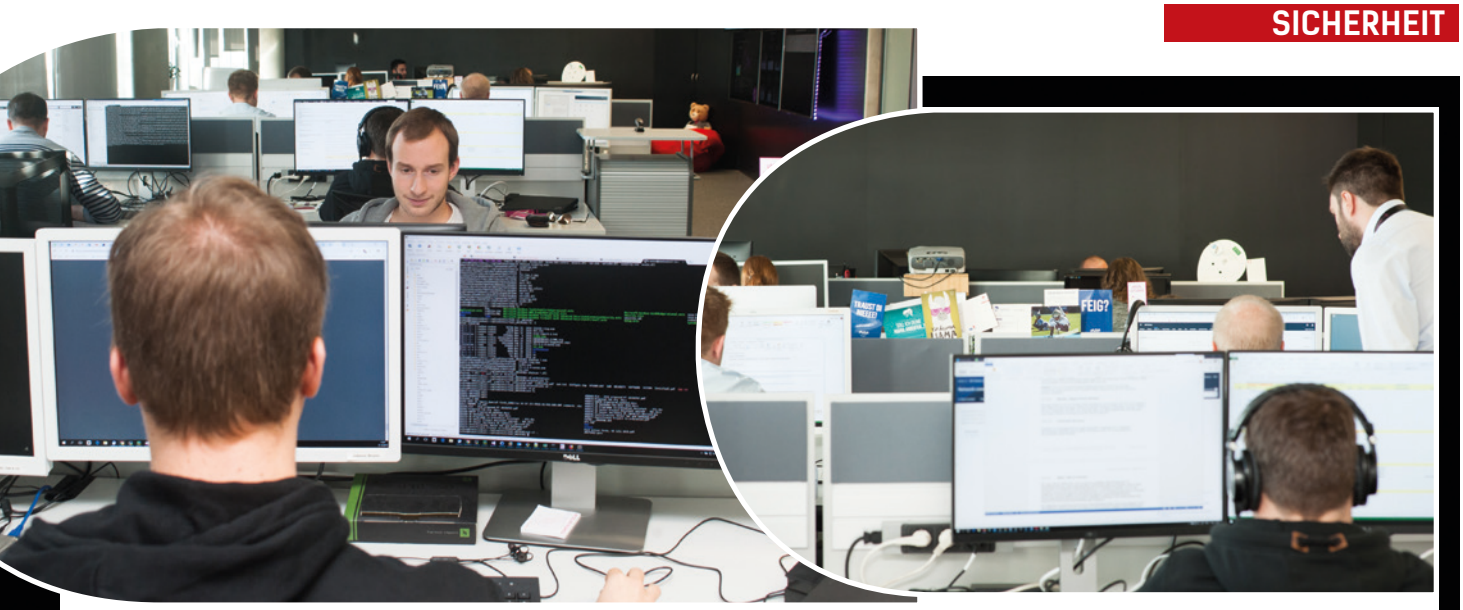
T-Systems bietet mit dem »Security Operations Center« eine rund um die Uhr besetzte Service-Stelle an, die Kunden laufend über aktuelle Entwicklungen und Bedrohungen im Cyberspace informiert, im Fall von Sicherheitsvorfällen unterstützt und Angriffe bewertet. Die jahrelange Erfahrung in hochkomplexen IT-Landschaften macht T-Systems damit zu einem starken Partner in Sachen Sicherheit.

>> Security Intelligence as a Service zum Schutz der IT-Infrastruktur <<

Mittlerweile bleiben Cyberattacken von betroffenen Unternehmen durchschnittlich mehr als 200 Tage unentdeckt. Und das, obwohl die Firmen präventive Maßnahmen wie Virenscanner oder Firewalls im Einsatz hatten. Dies zeigt, dass die Erkennung und Reaktion auf komplexe Angriffe gestärkt werden muss. Security Intelligence as a Service – kurz SIaaS – von T-Systems schließt diese Lücke und verbessert im Falle von Cyberangriffen sowohl die Erkennung als auch die Reaktion darauf. SIaaS stellt die Balance zwischen präventiven, detektiven und reaktiven Maßnahmen mit Fokus auf die beiden Letztgenannten her. Ziel ist es, die Zeit bis zur Erkennung von Bedrohungen wesentlich zu verkürzen und rasch mit geeigneten Gegenmaßnahmen zu antworten. Hinter SIaaS steht eine gemanagte Plattform zur übersichtlichen Bewertung der Bedrohungslage für die gesamte IT-Infrastruktur, die eine große Anzahl an Basisleistungen umfasst.

Mit Security Intelligence as a Service steht eine Lösung zur Verfügung, die in Österreich entwickelt wurde, aber dennoch weltweit einsetzbar und skalierbar ist. Somit passt sich die Lösung nahtlos dem Wachstum eines Unternehmens an. Mit dem Know-how von über 1.500 Security-Experten weltweit, 40 davon in Österreich, sorgt T-Systems für den höchstmöglichen Schutz

Advertorial, Fotos: iStock, Milena Krobath



Weltweit 1.500 Security-Experten sorgen bei T-Systems für höchstmöglichen Schutz.

von Wissen und finanziellen Ressourcen. Über 1,2 Mio. gemanagte Server und Clients weltweit profitieren bereits von den Security Services von T-Systems. Außerdem betrachtet T-Systems das Thema Cyber Security aus einer 360°-Sicht. So werden auch umfassende Maßnahmen zur Überprüfung bestehender IT-Infrastrukturen angeboten, sei es durch Security Assessments, Penetration Tests oder Identity & Data Screenings.

>> vCloud von T-Systems – die Basis der Digitalisierung <<

T-Systems bietet mit vCloud eine von VMware zertifizierte Private-Cloud-Lösung mit den höchsten Sicherheitsstandards. Damit die Daten auch tatsächlich einen maximalen Schutz genießen, setzt T-Systems auf eine Vielzahl von relevanten Parametern, die sowohl technische als auch organisatorische Elemente beinhalten. Nicht nur die Anwendung selbst, auch das Netzwerk der vCloud ist virtualisiert und standardisiert. Das bedeutet eine Trennung der Netze (Service-, Internet-, Intranet-, Management-Zone), die Einrichtung von Demilitarized Zones, eine Entkopplung durch Sicherheitsgateways sowie die logische Trennung von Mandanten auf Netzwerkebene.

Die Anbindung an das Cloud Management Portal erfolgt beim Hybrid-Cloud-Modell mittels einer Anbindung über das Internet und beim Private-Cloud-Modell mittels Anbindung über private Netzwerkverbindungen. Über vordefinierte Rollen und Berechtigungen werden die Zugriffe auf die vCloud kontrolliert. Der Zugriff der Kunden zum eigenen Netzwerk erfolgt dabei immer über einen Firewall-Cluster mit dezidierter, virtueller Firewall.

>> Governance, Risk und Compliance – im Griff mit der GRC Cloud von T-Systems <<

Korrektes Management von Governance, Risk und Compliance (GRC) ist essentiell für den Geschäftserfolg. Mangelnde Übersicht gefährdet die Reputation und finanzielle Stabilität eines Unternehmens. risk2value von avedos ist die umfassende Lösung für das Management von GRC-Prozessen – betrieben wird diese in der hochsicheren GRC-Cloud von T-Systems. Die GRC-Cloud trägt durch integriertes GRC-Management zur Einhaltung von Standards in den Bereichen GRC bei. Vorteil ist die Konsolidierung der bisherigen Datensilos an einer zentralen Stelle. Damit gehören System- und Medienbrüche der Vergangenheit an. Die eingesetzte Lösung risk2value geht über eine bloße Datenspeicherung hinaus. Sie unterstützt beim aktiven Management und berücksichtigt vor allem auch Informationssicherheit und Datenschutz.

>> Serverausfällen und Überlastungsangriffen gezielt entgegenwirken – mit IP DDoS Security <<

Die Zahl und die Möglichkeiten von Cyber-Kriminalität steigen. Unter einer Vielzahl von möglichen Szenarien haben sich DoS (Denial of Service) bzw. DDoS (Distributed Denial of Service) als hochgradig schwerwiegende Angriffsarten herauskristallisiert. Bei diesen Angriffen wird in der Regel durch Überlastung versucht, bestimmte Online-Dienste arbeitsunfähig zu machen. T-Systems bietet mit »IP DDoS Security« eine Sicherheitslösung für genau diese gezielten Überlastungsangriffe von außen. Damit sind Serverausfälle kein Security-Thema mehr. Diese Lösung ist exklusiv nur mit T-Systems Austria Internet Uplink nutzbar. Sollte der Verdacht eines DDoS Angriffs bestehen, so folgt T-Systems einer klaren Vorgehensweise, die versucht, innerhalb kürzester Zeit nach Beginn des Angriffs eine zumindest eingeschränkte Wiederherstellung der betroffenen Dienste zu erreichen. Aufgrund der Komplexität der möglichen Angriffe kann für die Abwehr des Angriffs allerdings keine Zeitspanne zugesichert werden. Auch bietet die IP DDoS Security Lösung keinen Schutz vor Einbruchsversuchen in Computersysteme (Hacker-Angriffe), Angriffe auf Sicherheitslücken in Hard- und Software, SPAM-Mails oder Schadsoftware.

>> Security Assessment Cyber-Angriff im Kundenauftrag <<

Die Sicherheit der eigenen IT-Infrastruktur einzuschätzen, ist nicht immer einfach, wird aber immer wichtiger. Wie leicht oder schwer sich Hacker beim Durchbrechen von Sicherheitsmaßnahmen tun, kann man mit »Friendly Hacking« von T-Systems testen. Bei diesen Sicherheitstests im Auftrag des Kunden führen Experten eine Bestandsaufnahme durch und analysieren systematisch den aktuellen Sicherheitsstand des getesteten IT-Systems. Es werden aber darüber hinaus auch öffentliche Standards und Normen, die regelmäßige Prüfungen und Dokumentation vorschreiben, überprüft. Um zu wissen, wie stabil und sicher seine Systeme sind, muss man letztlich die Methoden der Angreifer anwenden. So werden Schwachstellen objektiv identifiziert und adäquate Gegenmaßnahmen abgeleitet. ■

> *Weitere Informationen unter:*
www.t-systems.at oder
http://blog.t-systems.at

DIE GROSSE UMFRAGE

IT-SICHERHEIT

Cyberattacken nehmen massiv zu und erfolgen immer zielgerichteter auf bestimmte Unternehmen oder Personen. Trotz modernster Schutzmechanismen bieten sich insbesondere durch das Internet der Dinge unzählige Angriffspunkte für Kriminelle. Ob und wie Sicherheit überhaupt möglich ist, hat **Report(+) PLUS** bei ExpertInnen nachgefragt.

1 Wie kann Sicherheit in einem Netz intelligenter Systeme gewährleistet werden?

Franz Hoheiser-Pförtner
Stv. Obmann des Vereins Cyber Security Austria

Maschinelles Lernen ist eng mit dem Konzept der künstlichen Intelligenz verbunden und hat ein fundamentales Problem: die Qualität der Informationen, die beim Training von neuronalen Netzwerken verwendet wird. Künstliche Intelligenz ist jedoch (noch) nicht in der Lage, Vernunft, Emotionalität, Empathie sowie Kreativität umzusetzen. Künstliche Intelligenz hat kein Verständnis für Zusammenhänge und Hintergrundwissen ist ihm fremd. Maschinelles Lernen, künstliche Intelligenz und der Einsatz von neuronalen Netzwerken sind wie eine »Black Box«, bei der die Nachvollziehbarkeit der Berechnungen, die zu einer Entscheidung führen, nur sehr wenigen Personen möglich ist. Bei allen Erfolgen von künstlicher Intelligenz, die durch zukünftige Entwicklungen immer mehr unseren Alltag bestimmen wird, scheint mir aber ganz wichtig zu sein: Blindes Vertrauen kann gefährlich sein, auch intelligente Algorithmen sollten kritisch im Auge behalten werden.

Ingrid Schaumüller-Bichl
Leiterin des Information Security Compliance Center (ISCC) der FH OÖ

In Anbetracht der zunehmenden Vernetzung und Komplexität wird es von entscheidender Bedeutung sein, Sicherheit zu einem inhärenten Bestandteil aller Systeme zu machen. Egal ob Großrechner, Cloud-Lösungen, Mobile Devices oder kleine Komponenten und Sensoren im IoT, für sie alle müssen Sicherheitsfunktionen – möglichst transparent und benutzerfreundlich – bereits im Systemdesign vorgesehen werden und integraler Bestandteil der Systeme sein. In Anlehnung an den Begriff »Privacy by Design«, den wir aus dem Datenschutz kennen, können wir hier von »Security by Design« sprechen.

Christian Pfundner
CIO der Schrack Technik GmbH

Im Zeitalter der Digitalisierung und damit einhergehend der Bildung immer offenerer technischer Ökosysteme sind Sicherheitsaspekte ein kritischer Erfolgsfaktor für alle Beteiligten. Klar ist, dass konventionelle Sicherheitsansätze der IT, z.B. auf Netzwerkebene, nicht ausreichen werden. Es müssen vielmehr Geschäfts- oder Produktionsprozesse selbst abgesichert werden, wobei hier Ansätze der Anomaliedetektion und Mustererkennung auf Prozessebene einen möglichen Weg darstellen könnten.

Fotos: beigestellt

2 Gegen welche Bedrohungen müssen sich Unternehmen in nächster Zeit wappnen?

Franz Hoheiser-Pförtner

Die Berichte zu Sicherheitsvorfällen wie WannaCry, NotPetya und Spectre im Jahr 2018 zeigen, dass Ransomware sowie Hardware-Sicherheitslücken als massive Gefährdung auch weiterhin vorhanden sein werden. Ein weiterer neuer Angriffsvektor liegt beim illegalen Krypto-Mining. Die Betreiber von kritischen Infrastrukturen sind verstärkt im Fokus von Cyber-Bedrohungen. Diese Gefährdungspotenziale machen deutlich, dass die Cyber-Sicherheit in einer immer mehr digitalisierten Welt noch stärker betrachtet und beachtet werden müssen. Österreich und Europa müssen in den Fragen »security and privacy by design« und »security and privacy by default« eine Vorreiterrolle einnehmen.

Ingrid Schaumüller-Bichl

Es ist damit zu rechnen, dass die »Klassiker« wie Malware, Angriffe auf Web-Applikationen, Phishing, CEO-Frauds, Spams oder Ransomware auch in den kommenden Jahren noch die größten Herausforderungen für Unternehmen darstellen werden und professionelle Gegenmaßnahmen erfordern.

Dazu kommen aber zunehmend neue Bedrohungen und Herausforderungen, die sich aus den neuen Technologien ergeben. Wesentlich höhere Bandbreiten, das IoT, autonome Systeme oder Artificial Intelligence sind mächtige Instrumente, die unserer Gesellschaft viele neue Möglichkeiten und Chancen bieten. Gerade deshalb sind sie aber auch verwundbar und müssen rechtzeitig und effizient geschützt werden.

Christian Pfundner

Wir sehen, dass neben stetiger »technischer« Angriffe soziale Attacken in den letzten Monaten massiv zugenommen haben. Immer neue Varianten von E-Mail-basierten Versuchen, entweder an Zugangsdaten der Mitarbeiter zu kommen oder aber Überweisungen auszulösen, werden an uns weitergeleitet. Wichtig ist hier ein klar definierter und kommunizierter Incident-Response-Prozess, um im Fall der Fälle schnell reagieren zu können, sowie eine Unternehmenskultur, die Mitarbeiter dazu motiviert, potenzielle Sicherheitsvorfälle sofort zu melden.

3 Ist der Mensch die größte Schwachstelle?

Franz Hoheiser-Pförtner

Der Mensch ist gleichzeitig Konsument und auch Erzeuger von Informationen. Die Grenzen zwischen den handelnden Personen und Organisationen verschwimmen. Digitalisierung birgt einerseits das Potenzial, den Zugang zu Informationen und damit den Bildungszugang zu erleichtern und Chancengleichheit zu steigern. Andererseits müssen wir tatsächlich alle Menschen mit den notwendigen Kompetenzen ausstatten, um sie zu »Digital Natives« zu machen.

Die Erfassung und Verknüpfung riesiger Datenmengen ist inzwischen nicht nur technisch möglich, sondern bildet auch einen gewaltigen Markt. Erfasst wird längst nicht mehr nur das Surfverhalten am heimischen PC oder auf dem Smartphone, sondern jede Handlung, die digital abgebildet ist. Und mit der fortschreitenden Digitalisierung aller Lebensbereiche werden immer mehr personenbezogene Daten aus ehemaligen Offline-Bereichen gesammelt. Vollständige Datenverfügbarkeit ist keine Illusion mehr, sondern nur noch eine Frage der Vernetzung.

Ingrid Schaumüller-Bichl

Natürlich gibt es viele Angriffe, die Unwissenheit, Bequemlichkeit, sehr oft aber auch die Hilfsbereitschaft von Menschen ausnutzen. Sicherheitsbewusstsein und entsprechende Schulungen sind daher von immenser Bedeutung. Die größte Schwachstelle sind für mich aber nach wie vor veraltete, schlecht oder gar nicht gewartete und gepatchte Systeme, dazu kommen oft fehlendes Risikomanagement und unklare Verantwortlichkeiten.

Ein gut funktionierendes Sicherheitsmanagement ist die wesentliche Voraussetzung für den sicheren Einsatz von IT, das umfasst sowohl technisch-organisatorische als auch menschliche Aspekte. Nur durch ein Gesamtkonzept und permanente Verbesserung kann Sicherheit dauerhaft gewährleistet werden.

Christian Pfundner

Was als größte bzw. bedrohlichste Schwachstelle wahrgenommen wird, ist sicherlich von Unternehmen zu Unternehmen verschieden. Fakt ist, dass der Mensch im Gegensatz zur Maschine für soziale Attacken empfänglich ist und technische Möglichkeiten der Schadensverhinderung für solche Fälle weniger gut anwendbar sind. Gut geschulte Mitarbeiter sind jedoch potenziell in der Lage, als weit gespanntes Netz von Sensoren zu wirken, welches »neue« Bedrohungen intelligent erkennt und an die Sicherheitsverantwortlichen im Unternehmen rückmeldet.

SAVE

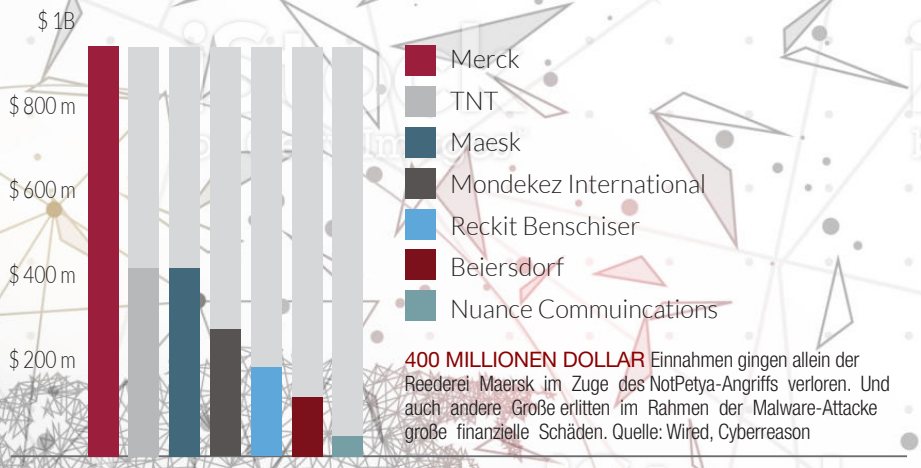
Die Welt der Passwörter, Ransomware und künstliche Intelligenz: Welche Tatsachen Firmen erschüttern, Sicherheitsbeauftragte quälen und Millionenbeträge auf die dunkle Seite der IT-Welt spülen. Zahlen und Fakten aus 2017 und 2018.

DAS WAREN DIE 20 HÄUFIGSTEN PASSWÖRTER 2017:

1) 123456
2) password
3) 12345678
4) qwerty
5) 12345
6) 123456789
7) letmein
8) 1234567
9) football
10) iloveyou
11) admin
12) welcome
13) monkey
14) login
15) abc123
16) starwars
17) 123123
18) dragon
19) passw0rd
20) master

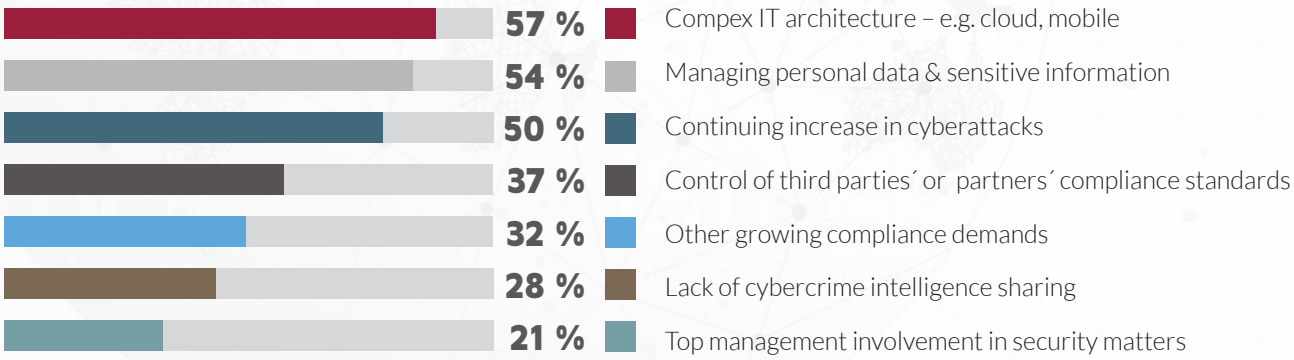
Quelle: SplashData

UMSATZEINBUßEN DURCH DIE NOTPETYA-ATTACKE 2017



400 MILLIONEN DOLLAR Einnahmen gingen allein der Reederei Maersk im Zuge des NotPetya-Angriffs verloren. Und auch andere Große erlitten im Rahmen der Malware-Attacke große finanzielle Schäden. Quelle: Wired, Cyberreason

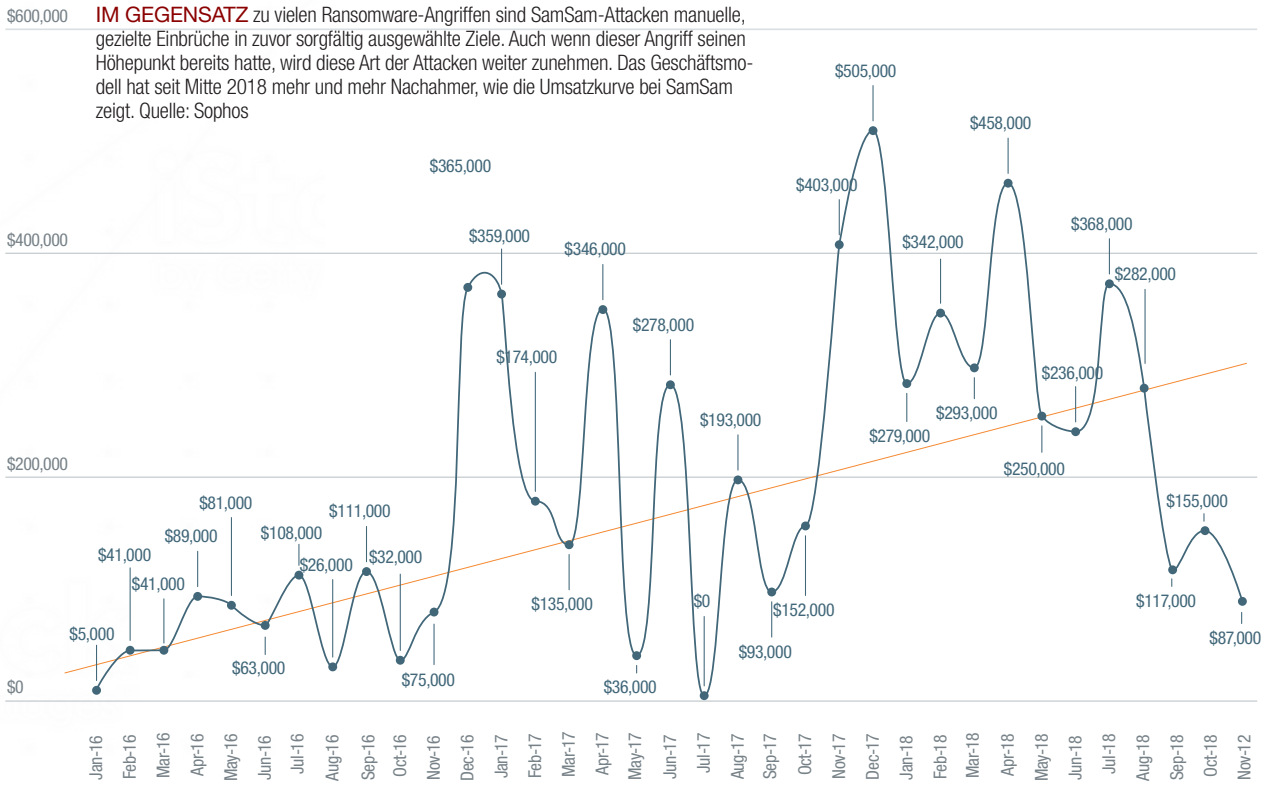
URSACHEN FÜR SORGENFALTEN BEI CISOS



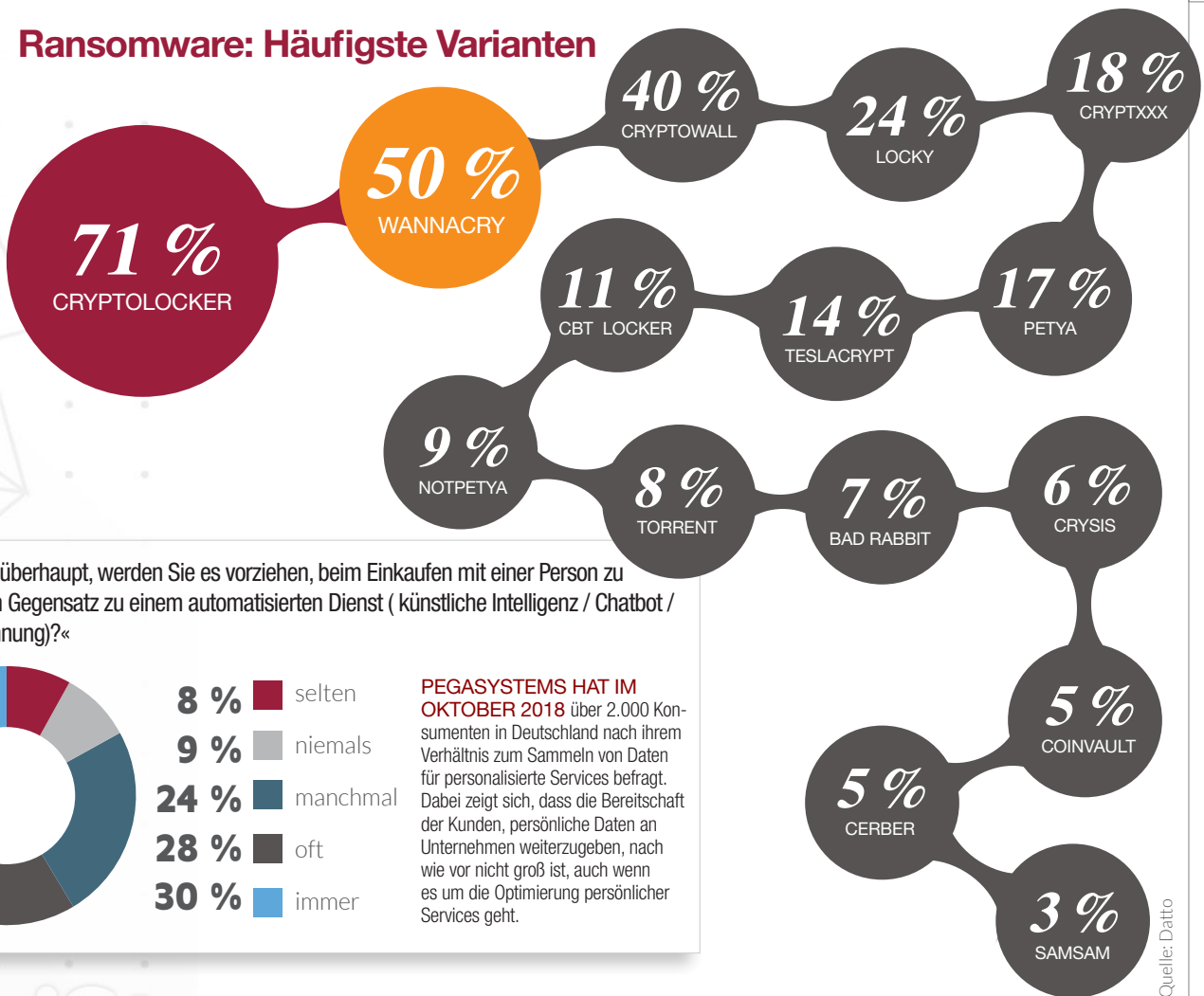
LAUT EINER STUDIE VON KASPERSKY LAB stehen »Chief Information Security Officers (CISOs)« verstärkt unter Druck: 57 % sehen die durch Cloud und mobile Geräte komplexer werdende IT-Infrastruktur als größte Herausforderung. Jeder Zweite betrachtet auch die zunehmende Zahl von Cyberangriffen mit Sorge.

»SAMSAM« RANSOM PAYMENTS – GESAMT 6,5 MIO. DOLLAR

IM GEGENSATZ zu vielen Ransomware-Angriffen sind SamSam-Attacken manuelle, gezielte Einbrüche in zuvor sorgfältig ausgewählte Ziele. Auch wenn dieser Angriff seinen Höhepunkt bereits hatte, wird diese Art der Attacken weiter zunehmen. Das Geschäftsmodell hat seit Mitte 2018 mehr und mehr Nachahmer, wie die Umsatzkurve bei SamSam zeigt. Quelle: Sophos



Ransomware: Häufigste Varianten



Quelle: Datto

»Wie oft, wenn überhaupt, werden Sie es vorziehen, beim Einkaufen mit einer Person zu interagieren, im Gegensatz zu einem automatisierten Dienst (künstliche Intelligenz / Chatbot / Sprachaufzeichnung)?«

8 % selten
9 % niemals
24 % manchmal
28 % oft
30 % immer

PEGASYSTEMS HAT IM OKTOBER 2018 über 2.000 Konsumenten in Deutschland nach ihrem Verhältnis zum Sammeln von Daten für personalisierte Services befragt. Dabei zeigt sich, dass die Bereitschaft der Kunden, persönliche Daten an Unternehmen weiterzugeben, nach wie vor nicht groß ist, auch wenn es um die Optimierung persönlicher Services geht.

Gebuchtes Hacking

VON KARIN LEGAT

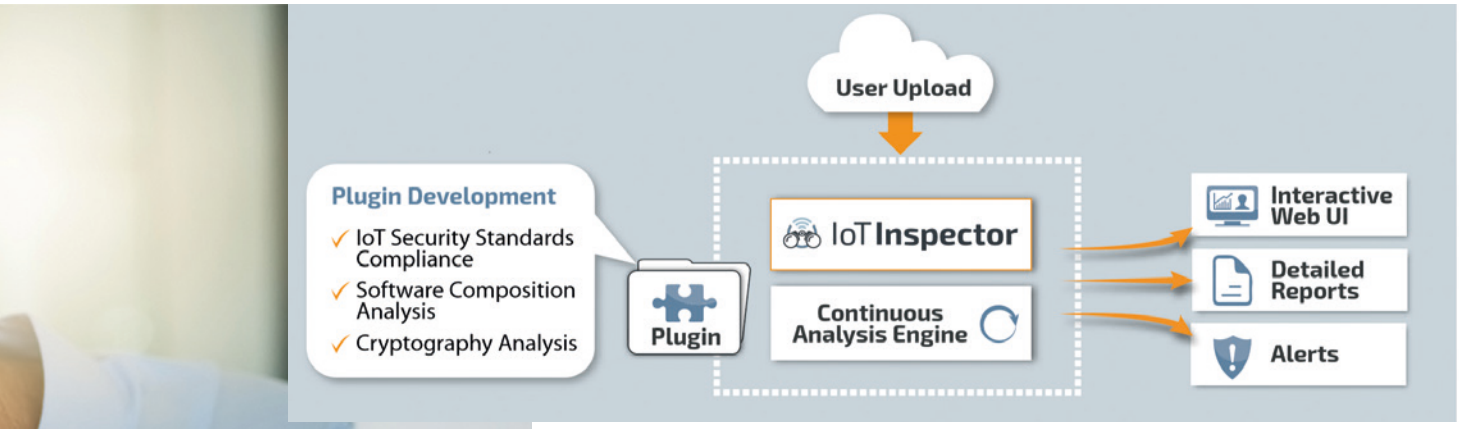
Schadsoftware auf Wunsch einschleusen, das ist Penetration Testing. In Systemen werden damit Sicherheitsschwachstellen aufgezeigt.

Ein Blick zurück in die Welt des Schwarzweißfernsehens. In Western hatten die Guten stets helle Hüte auf, die Bösen die schwarzen. Daraus leiten sich die Begriffe White und Black Hat Hacking ab. »Meine Mitarbeiter stehen alle auf der guten Seite, sind daher White Hat Hacker«, lacht Markus Robin, General Manager von SEC Consult. Sein Unternehmen ist führender Berater in den Bereichen Cyber- und Applikationssicherheit, vertreten in Europa, Asien sowie Nordamerika, und bietet Penetration Tests seit 2002 an. »Unternehmen sind deutlich offener geworden. Die Nachfrage nach Sicherheitstests steigt. Vor 15 Jahren mussten wir noch überzeugen, heute verlangen Kunden von sich aus danach.« Damals musste der Vorgang auch von Grund auf erklärt werden. Meist sind Interessenten heute bereits vorinformiert, wissen, dass Penetration Testing eine wirkungsvolle Vorgehensweise ist, um ein sicheres IT-Umfeld zu schaffen.

>> Hacken auf Auftrag <<

Ein Penetration Test ist der Versuch, mit denselben Tools wie ein Hacker in ein IT-System einzudringen und Sicherheitsschwachstellen in Webanwendungen oder beispielsweise Backoffice-Systemen zu identifizieren. Software wird eingeschleust, wodurch geschützte Daten ausgelesen und genutzt werden können. Diese Daten sind entweder selbst wertvoll oder dienen dazu, weitere Systeme zu infiltrieren und zu übernehmen. Bei SEC Consult heißt das Tool für die automatisierte Sicherheitsanalyse IoT Inspector. Damit wird eine große Bandbreite an vernetzten Geräten wie auch IP-Kameras, Router sowie Drucker abgedeckt. Unternehmen können die Firmware von IoT-Devices selbst auf Schwachstellen überprüfen. Dazu braucht es drei Schritte: Firmware hochladen, IoT In-

Fotos: SEC Consult



Der IoT Inspector ist die automatisierte Sicherheitsanalyse für IoT-Firmware von SEC Consult. Plugins erkennen Schwachstellen und nutzen dabei zusätzlich auch Datenquellen wie die IoT-Suchmaschinen Shodan und die National Vulnerability Database von NIST.

spector analysieren lassen, Report checken. Grundlage für wirkungsvolles Testing ist Vertrauen, für Robin eines der wertvollsten Güter. Wenn Sicherheit getestet wird, verlangt die Vorgangsweise Seriosität. Hier trennt sich für den Geschäftsführer die Spreu vom Weizen. Man müsse als Schuster mit guten Schuhen wahrgenommen werden. »Wir investieren selbst viel in Sicherheit. Bei Mitarbeitern sind etwa Backgroundchecks Standard.« SEC Consult ist ISO-27001- und CREST-zertifiziert, ebenso Mitglied bei Open Web Application Security Project (OWASP).

Markus Robin, SEC Consult: »Viele Unternehmen meinen, sie können selbst für ausreichend Sicherheit sorgen und übersehen, dass sie längst gehackt worden sind.«

>> Bedarf für White Hacking <<

»Sicherheit ist wie ein Radrennen. Es ist stark gesplittet«, vergleicht Robin. Es gebe eine Spitzengruppe, aber auch viele Nachzügler. Viele meinen, sie können für ihre Sicherheit noch selbst sorgen, übersehen dabei, dass sie schon gehackt wurden. Hacker haben in der Regel kein Interesse wahrgenommen zu werden, Ausnahme: Ransomware. IT-Sicherheit wird von Kunden oft nicht ausreichend geschätzt, nur als Kostenfaktor gesehen. Als Treiber für ein sensibleres Bewusstsein sieht Robin die Datenschutz-Grundverordnung, die auf IT-Sicherheit Bezug nimmt. Hilfreich wäre, würden Hersteller und Serviceanbieter bei jedem ihrer Produkte bereits Sicherheitstests vornehmen. Das wird als Teil der Qualitätssicherheit bereits geboten. In den letzten zehn Jahren hat es sich stark verbreitert, aber es ist laut den Experten noch immer nicht ausreichend. Im IT-Umfeld besteht noch sehr viel Nachholbedarf. Stichwort NIS-Richtlinie: Da ist Österreich noch säumig, das Gesetz befindet sich erst in Begutachtung.

>> Sicherheitsweg <<

Kosten und Zeitrahmen der Penetration Tests entscheiden sich danach, wie groß die IP Range des Kunden ist. »Bei einem Gebäude muss ich wissen, wie viele Fenster als potenzielle Einstiegspunkte für Angreifer es gibt und wie komplex diese sind«, zieht Robin den Vergleich mit dem Bauwesen. Als Mindestsumme nennt er 8.000 Euro, darunter würden Sicherheitstest wenig Sinn machen. Zwei bis drei Wochen müssen für die Tests in der kleinsten Konfektionsgröße veranschlagt werden. »Der aktive Test selbst läuft mindestens eine Woche. Dazu kommen Vor- und Nachabstimmung mit dem Kunden, das heißt Auflistung der Schwachstellen, Erklärung, Vorschläge zur proaktiven Verbesserung des Sicherheitskonzepts.« SEC Consult empfiehlt einen zweiten Test ähnlich einer Nachsorgeuntersuchung. Sicherheitsschwachstellen gibt es genügend, diese würden sich aber nicht wesentlich ändern. Injections bleiben laut OWASP die größte Gruppe.

Thema der letzten Jahre waren vor allem Penetration Tests für IoT-Devices, die die gesamte IT-Umgebung immer stärker durchdrungen haben. »Viele Geschäftsprozesse sind heute nicht mehr ausschließlich im Internet, sondern werden auf Geräte ausgelagert. Das bedeutet eine Schwerpunktveränderung im Testing.« ■

METHODEN

> Bei einem »Blackbox Penetration Test« agiert der Sicherheitsexperte ohne Informationen zum System. Das Gegenteil: der »White Box Penetration Test«, bei dem ausführliche Informationen zum Testobjekt zur Verfügung stehen. »Damit es nicht zu einfach wird, gibt es auch die Grey Box«, erklärt Markus Robin. Die Tests selbst erfolgen in unterschiedlichen Detailierungsstufen bis runter zum Source Code.

Herwig Köck, T-Systems: »Das Wichtigste für Unternehmen sind die Basisaufgaben Patching, Netzwerk-Trennung und ein Berechtigungs-Management. Wenn das nicht erfüllt ist, können die besten Sicherheitstools nicht vor Angreifern schützen.«

Wenn es Angreifern zu leicht gemacht wird

Welche Einfallstore besonders beliebt sind und warum auch Social Engineering nicht zu unterschätzen ist. Ein Einblick, wie die dunkle Seite arbeitet.

VON MARTIN SZELGRAD

Herwig Köck, Head of Security Professional Services bei T-Systems, sieht Unternehmenswebsites als häufigen Angriffspunkt bei Sicherheitsvorfällen. Diese werden oft nicht von der eigenen IT-Abteilung administriert, sondern auch an Webagenturen ausgelagert und extern gehostet. Viele setzen bei ihrem Webauftritt auf gängige Content-Management-Systeme – Wordpress, Joomla oder Drupal, die bei Bedarf auch umprogrammiert werden. »Gerade jene, die den Code anpassen, tun sich dann auch beim regelmäßigen Einspielen von Updates eher schwer. Hier geht es auch um Geschwindigkeit, da Schadsoftware innerhalb weniger Tage nach Bekanntgabe einer Sicherheitslücke Seiten im Netz automatisiert infiziert«, erklärt Köck. Beliebte Zeitfenster für Attacken sind Wochenenden oder Feiertage – ein Zeitraum, in dem das Web-Team meist unterbesetzt ist oder überhaupt erst an einem darauffolgenden Arbeitstag reagieren kann. Angreifer arbeiten dabei ebenso arbeitsteilig wie herkömmliche Organisationen. »Ein Teil kümmert sich um die Basis-Infrastruktur, registriert etwa Domains. Ein anderer treibt die die Phishing-Attacken voran und schreibt die Mails«, sieht sich der Experte einer Wirtschaftssparte gegenüber,wie man sie auch aus klassischen Bereichen kennt – mitsamt Arbeitszeitmodellen, Urlaubsregelungen und Weiterbildungsmaßnahmen.

Fotos: Milena Krobath

Warum werden Webseiten überhaupt gehackt? »Sie sind der Bereich eines Unternehmens, der besonders exponiert ist – mit eher komplexen Softwareumgebungen mit unterschiedlichen Anwendungen und auch vielen potenziellen Sicherheitslücken. Bei diesen Mengen an Code kann man schon viel falsch machen«, warnt er. Ist eine Seite einmal kompromittiert, versuchen Eindringlinge sich vom Webserver aus per »lateral movement« zu weiteren Systemen zu bewegen. Auch verschlüsselte, schwache Passwörter können mit entsprechenden Rechenleistungen heutzutage schnell geknackt werden. Wenn die IT dann noch dieselben Passwörter für Server verwendet, stehen Angreifern die Türen zu sensibleren Netzwerkbereichen offen, etwa Datenbanken. »Windows hat die Eigenheit, dass Hashes von Passwörtern eingeloggter User missbraucht werden können. Da muss ich bei einem infizierten Windows-Webserver nur solange warten, bis sich ein Administrator über den Fernzugang darauf anmeldet. Mit dem Hash kann ich mich dann im Netzwerk an anderen Stellen frei bewegen«, berichtet Köck direkt aus der Praxis.

> IST EINE WEBSEITE EINMAL KOMPROMITTIERT, VERSUCHEN EINDRINGLINGE SICH VOM WEBSERVER AUS PER »LATERAL MOVEMENT« ZU WEITEREN SYSTEMEN ZU BEWEGEN.

>> Lösungen vorhanden, aber ungenutzt <<

Natürlich gibt es für den Betrieb von Windows-Domänen Empfehlungen des Herstellers, um ein Mitschnüffeln zu verhindern. »Die meisten haben davon aber nie etwas gehört, da dies auch etwas aufwendig ist.« Grundlegend empfiehlt der Experte, Administratoren-Accounts mit unterschiedlichen Berechtigungen zu nutzen. Im Falle des Falles hat dann ein Eindringling nicht vollends freie Hand. Die Administration verschiedener Ebenen ist aber für kleinere Firmen oft nur schwer durchsetzbar, ist ihm bewusst. Meist scheitert es schon am notwendigen Know-how. »Auch bei Größeren bleibt mitunter das Administratorenkennwort in den ausgerollten Images auf den Rechner der Mitarbeiter gespeichert – selbst wenn der Mitarbeiter das Unternehmen längst verlassen hat. Eine Gratislösung von Microsoft kann bei der übersichtlichen Verwaltung schon gut helfen. Die wird aber kaum verwendet.«

Wie sieht generell die Lage bei Social Engineering aus? Wenn sich Angreifer weniger auf technische Exploits verlassen, sondern auf internes Wissen über Firmenabläufe und Personen setzen? »Firmen machen es auch hier Kriminellen oft viel zu einfach«, berichtet der Experte von einem Fall in Deutschland. Dabei wurde der Mailverkehr mit einem asiatischen Zulieferer manipuliert und kurzerhand eine Kontonummer ohne Wissen der Betroffenen getauscht. Obwohl aufmerksame Mitarbeiter eine Bankbestätigung einforderten, verlor das Unternehmen einen sechsstelligen Betrag – und das gleich zweimal. »Dabei war der Nachweis denkbar schlecht gefälscht. Man hatte sich einfach nicht die Mühe gemacht, genauer hinzusehen.«

> USB-Sticks mit der Software Rubberduck an Bord kosten im Darknet 40 Dollar und werden für Angriffe auf Endgeräte absichtlich »liegen gelassen« oder »verloren«. Andere Sticks gibt es bereits ab 5 Dollar.

>> Tool und Empfehlung <<

Doch nicht nur Mail-Verkehr und Websites – auch scheinbar zufällig herumliegende USB-Sticks sind eine Gefahrenquelle. Sie können gezielt und unbemerkt Schadsoftware auf einen Rechner spielen, indem sie als »Human Interface Device« an der Virenschutz-Software vorbei Tastatureingaben simulieren. Das Tool Metasploit wird sowohl von White als auch von Black Hackern genutzt und bietet fertige Skripte für Angriffe – aktuell befinden sich mehr als 1.000 Exploits in der Programm-Datenbank. »Dabei wird gezielt nach Bereichen in einem Computersystem gesucht, in denen auf Sicherheitsfeatures vergessen oder Patches nicht rechtzeitig eingespielt worden sind«, erklärt Köck und betont: Admins sollten stets Updates einspielen und den Netzwerkverkehr monitoren. Die Empfehlung für die User: Hirn einschalten, mitdenken! ■

»Spielwiese für Script-Kiddies, Wutbürger und Kriminelle«

Im Interview mit Report(+)PLUS erklärt Oberst Walter Unger, seit 2017 mit dem Aufbau eines Cyber-Verteidigungszentrums im Abwehramt des Bundesheeres verantwortlich, wie sich die nachrichtendienstliche Arbeit durch Cyber-Bedrohungen verändert hat. Außerdem spricht er über konkrete Bedrohungen, die Schwachpunkte von Staaten und Unternehmen und die »radikale Verkleinerung der Angriffsfläche« als wichtigstes Mosaiksteinchen der Cyber-Verteidigung.

Foto: iStock

VON BERND AFFENZELLER

> *Auch Cyber-Terrorattacken sind nicht auszuschließen. Angriffe gegen Betreiber kritischer Infrastrukturen könnten echte Krisen auslösen.*

(+) PLUS: Das Abwehramt beschafft Informationen über »Bestrebungen und Tätigkeiten, die vorsätzliche Angriffe gegen Leben und Gesundheit von Personen, Infrastruktur und militärisch klassifizierte Informationen erwarten lassen«. Welche Rolle spielen dabei Cyber-Attacken?

Walter Unger: Die Masse der militärischen Geheimnisse liegt heute in digitaler Form vor. Es ist bekannt, dass weltweit viele Nachrichtendienste, Informationshändler, aber auch Amateure auf der Suche nach geheimen Informationen sind. Es kann daher davon ausgegangen werden, dass jegliche Informationen in ungeschützten, mit dem Internet verbundenen Systemen ausgespäht werden. Entsprechende Gegenmaßnahmen sind daher zwingend erforderlich.

(+) PLUS: Wie hat sich die nachrichtendienstliche Arbeit durch Cyber-Bedrohungen verändert?

Unger: Vor allem der Bereich der Auswertung und Analyse von offen verfügbaren Informationen, die sogenannte Open Source Intelligence OSINT, hat sich grundlegend verändert. Man schätzt, dass ungefähr 80 bis 85 Prozent der Berichte von Nachrichtendiensten auf OSINT basieren. Die Herausforderungen dabei sind die gigantisch verfügbaren und täglich neu hinzukommenden Datenmengen. Alle paar Monate verdoppelt sich die Menge der global verfügbaren Daten. Die Erfassung und zeitgerechte Auswertung dieser enormen Datenmengen ist für die Rechenleistung und den erforderlichen Speicherplatz sehr anspruchsvoll. Ebenso ist die Bewertung der Quellen und des Wahrheitsgehaltes eine noch wesentlich größere Herausforderung, die letztlich nicht von Software allein gelöst werden kann. Es braucht am Ende des Intelligence-Prozesses immer noch den erfahrenen und hochqualifizierten Analytiker.

Im klassisch operativen nachrichtendienstlichen Bereich kompensieren Cyber-Mittel teilweise den Einsatz von Personen. Es lassen sich so Informationen aus der Ferne beschaffen, ohne Einsatz der Personen vor Ort. Außerdem kann die Übermittlung von Ergebnissen technisch sehr gut unterstützt werden. Die nachrichtendienstliche Abwehr muss daher zur erfolgreichen Auftragserfüllung entsprechende technische Fähigkeiten entwickeln und anwenden.

(+) PLUS: Welche konkreten Gefahren und Bedrohungen gibt es?

Unger: Der Cyber-Raum ist eine Spielwiese für sogenannte »Script-Kiddies«, aber auch ein Aktionsraum für Aktivisten und Wutbürger, der Tatort für Kriminelle und Terroristen. Er kann zum Operations- als auch Kriegsgebiet für staatliche Cyber-Warrior werden. Die Akteure unterscheiden sich nach ihrer Motivation, Zielsetzungen, verfügbaren Ressourcen und Fähigkeiten.

(+) PLUS: Welche Bereiche sind aus Sicht des Abwehramtes am stärksten vom Cyber-Angriffen bedroht?

Unger: Staaten, Unternehmen, Organisationen und Einzelpersonen müssen mit Datenmissbrauch und subversivem Hacktivismus rechnen, also mit Cyber-Angriffen, um Geld zu ergaunern. Aber auch die Ausforschung und das Sammeln von Informationen sowie Sabotageangriffe gegen strategisch bedeutsame Unternehmen und Behörden sind für genannte Akteure eine Gefahr. Letztlich ist ein digitaler Stillstand eines Staates durch großangelegte Cyber-Attacken nicht auszuschließen.

Aber Cyber-Attacken kommen laufend und treffen jeden – Unternehmen, Behörden und Einzelpersonen. Die Angreifer werden immer professioneller und beschäftigen sich intensiv mit den Opfern, auch staatliche Akteure sind vermehrt zu beobachten.

(+) PLUS: Wie sehen Cyber-Angriffe in der Regel aus?

Unger: Mittels Ransomware und Distributed-Denial-of-Service werden Unternehmen, Behörden und Spitäler sowie Einzelpersonen erpresst. Angriffe werden indirekt geführt und als Attack-as-a-Service als Dienstleistungen im Netz angeboten. Derartige Übergriffe gegen strategische Infrastrukturen nehmen zu, Schadprogramme werden industriell gefertigt. Täglich tauchen 400.000 bis 500.000 neue Versionen auf. Mittelfristig muss vermehrt mit Angriffen beispielsweise auf Chipebene, gegen Cloud-Systeme, gegen Apps und gegen hochsichere Verschlüsselungen gerechnet werden. Weiters sind Cyber-Terrorattacken nicht auszuschließen. Angriffe gegen Betreiber kritischer Infrastrukturen könnten echte Krisen auslösen. Cyber-Angriffe als politisch-militärische Waffe im Vorfeld und in heißen Konflikten werden an Häufigkeit und Intensität noch zulegen.

(+) PLUS: Welche Ziele verfolgen sogenannte Cyber-Terroristen in der Regel?

Unger: Nach Peter Waldmann sind unter Terrorismus »planmäßig vorbereitete, schockierende Gewaltanschläge gegen eine politische Ordnung aus dem Untergrund« zu verstehen. Terrorakte sollen allgemeine Unsicherheit und Schrecken, daneben aber auch Sympathie und Unterstützungsbereitschaft erzeugen. Terrorismus ist also grundsätzlich als Kommunikationsstrategie zu verstehen, nach dem Motto: »Töte einen, erschrecke Tausende!«

Terroristen nutzen den Cyber-Raum für Kommunikation, Planung, Rekrutierung, Propaganda, Zielaufklärung und für das Einsammeln von Spenden.

(+) PLUS: Die IT-Infrastruktur eines Unternehmens zu schützen ist das eine, aber wie schützt man ein ganzes Land vor Cyber-Angriffen? Welche Bereiche haben oberste Priorität?

Unger: Moderne, hochentwickelte Staaten wie Österreich sind von ihren strategischen Infrastrukturen wie Stromversorgung, Telekommunikation, Internet, Flughäfen oder Krankenhäuser abhängig. Diese Infrastrukturen wiederum sind vom Funktionieren der IKT-Systeme und dem reibungslosen Fluss großer Datenströme abhängig. Eine Störung oder gar Zerstörung dieser Infrastrukturen kann schwerwiegende Auswirkungen auf die Gesundheit, die Sicherheit, das wirtschaftliche und soziale Wohl der Bevölkerung oder die effektive Funktionsweise von staatlichen Einrichtungen haben. Diese Infrastrukturen könnten daher zu vorrangigen Angriffszielen in einem mit Cyber-Mitteln ausgetragenen Konflikt werden. Großangelegte ▶

▶ gegen den Gesamtstaat gerichtete Cyber-Angriffe könnten die Souveränität bedrohen und stellen sowohl die politisch-strategische Ebene als auch die militärische Landesverteidigung vor neue Herausforderungen. Zur Cyber-Verteidigung tragen insbesondere präventive Absicherungsmaßnahmen, die permanente Verfügbarkeit eines aktuellen Cyber-Lagebildes, die Frühwarnung, die Alarmierung, die Abwehr von laufenden Angriffen einschließlich offensiver Maßnahmen, die Sicherstellung der vitalen Funktionen sowie die rasche Wiederherstellung des Normalzustandes bei.

(+) PLUS: Wie kann man sich einen Cyber-Angriff auf die sensiblen Ziele eines Landes vorstellen?

Unger: Wie so ein Szenario ausschauen könnte, konnte man an den Cyber-Angriffen gegen Estland 2007, Georgien 2008 oder gegen die Stromversorgung der Ukraine 2015 und 2016 beobachten. Dabei wurden mit Schadprogrammen und -methoden Systeme der kritischen Infrastruktur sabotiert.

(+) PLUS: In einem *Standard*-Artikel wird das Bundesheer zitiert, dass es rund zehn Millionen Euro kosten würde, Österreich mit Cyberattacken und Sabotageaktionen gegen Glasfaserleitungen weitgehend auszuknipsen. Wie viel kostet es, sich gegen solche Angriffe zu wappnen? Sind genügend finanzielle und personelle Ressourcen vorhanden?

Unger: Diese Zahl ist eine Schätzung und hängt sehr davon ab, welche Schutzmaßnahmen bei den strategischen Infrastrukturen bereits umgesetzt sind. Der Schutz der eigenen Systeme ist zweifelsohne nicht billig, aber alternativlos.

Die eigenen Kosten sind tragbar, wenn die wesentlichen Grundsätze der Verteidigung im Cyber-Raum von vornherein berücksichtigt werden. Dazu gehört zunächst die radikale Verkleinerung der Angriffsfläche. Wir alle bieten derzeit ein viel zu großes Ziel. Es stellt sich die Frage, warum wichtige Steuersysteme wie Industrieroboter, Kläranlagen, Atomkraftwerke mit dem Internet verbunden sein müssen. Eine beim Österreichischen Bundesheer seit Jahrzehnten erfolgreich angewandte und bewährte Absicherungsmaßnahme wäre, die wichtigsten IKT-Systeme von unsicheren Systemen physikalisch zu trennen und die internen Netze zu segmentieren.

Klar ist, dass Angriffe grundsätzlich nicht zur Gänze zu verhindern sind. Auch die beste Verteidigung kann nicht alle Schäden abhalten. Daher müssen Cyber-Bedrohungen in das Risikomanagement einbezogen werden. Mit Notfallplänen und Redundanzen muss einem Totalverlust bzw. einem langfristigen Stillstand vorgebeugt werden. Weiters müssen die technischen Absicherungsmaßnahmen mit der Bedrohungsentwicklung Schritt halten. Statische Maßnahmen greifen zu kurz; es braucht dynamische, selbst optimierende, automatisch reagierende Systeme mit sehr hoher Performance.

(+) PLUS: Der IT-Sektor kämpft wie viele andere Bereiche mit einem enormen Fachkräftemangel. Mit welchen Maßnahmen versuchen Sie, die besten Köpfe für das Abwehramt zu begeistern?

Unger: Motiviertes, gut ausgebildetes Personal ist die Schlüsselressource beim Schutz der eigenen Cyber-Sphäre. Derzeit herrscht bei Unternehmen und Behörden eine sehr große Nachfrage nach IT-Experten. In Österreich können derzeit etliche tausende Stellen nicht besetzt werden.

Für das Militär haben wir mit der Fachhochschule Hagenberg in den 2000er-Jahren einen eigenen Bachelorlehrgang entwickelt, um eigenes Personal zu qualifizieren. Eine weitere Initiative war die 2012 begonnene »Cyber Security Challenge«, mit der Talente unter Schülern und Studenten gefunden, gefördert und ua. auch vom Bundesheer beworben werden sollen. Mit der Einführung einer Cyber-Ausbildung für Grundwehrdiener wurde ein weiterer Baustein gesetzt. Aktuell wird an Ausbildungsgängen für Offiziere und Unteroffiziere gearbeitet.

»Cyber-Angriffe werden indirekt geführt und können als Dienstleistungen im Netz gekauft werden, quasi als Attack-as-a-Service«, sagt Oberst Walter Unger.

Foto: Bundesheer

(+) PLUS: Wie sensibel sind Entscheidungsträger in Politik und Wirtschaft gegenüber Cyber-Bedrohungen? Wie ist es um das Wissen über das Gefahrenausmaß bestellt?

Unger: Sensibilisierung ist ein Dauerthema. Wenn man das Regierungsprogramm studiert, hat die Cyber-Herausforderung einen ganz prominenten Platz und ist vielfach angesprochen. Unser Beitrag ist die jährliche IKT-Sicherheitskonferenz, die heuer zum 17. Mal stattfand. Mehr als 2.500 Teilnehmer, davon 80 Prozent aus dem zivilen Bereich, und 50 Aussteller zeigten, dass Cyber ein ganz wichtiges Thema geworden ist. Nicht nur für das Militär, sondern für unsere ganze Gesellschaft.

Es geht um gesamtstaatliche, strategische Aufgaben. Österreich als Hochtechnologiestandort, als Innovationsweltmeister sollte Cyber-Sicherheit zu einem Standortvorteil entwickeln. Österreich mit seinen starken IT-Unternehmen könnte hier ein großer Spieler werden.

(+) PLUS: Wie gut ist Österreich gegen Cyber-Attacken geschützt?

Unger: Die Meldelage ist noch nicht so dicht, dass dazu valide und vergleichbare Aussagen gemacht werden können. Faktum ist, dass die Anzeigen wegen Cyber-Kriminalität immer noch deutlich ansteigen. Entscheidend aber ist, zu verhindern, dass Unternehmen letale Schäden erleiden oder gar ein digitaler Stillstand die Souveränität Österreichs bedroht. ■

Business- und Security-Manager brauchen einander.

Erst priorisieren, dann innovieren

Wie Sie geschäftskritische Assets mit einem prioritätsbasierten Security-Ansatz vor Cyber-Attacken schützen.

VON MARKUS HIRSCH, *MANAGER SYSTEM ENGINEERING AUSTRIA BEI FORTINET*

Welche Assets sind unbedingt vor Angreifern zu schützen? Obwohl die Frage als Erstes auf der Hand liegt, wird sie in österreichischen Unternehmen zu selten gestellt. Eine Studie der Economist Intelligence Unit zeigt: Business-Entscheider assoziieren mit Datenschutz vor allem die eigene Reputation beim Kunden, während sich Sicherheitsexperten meist rein auf den Schutz von sensiblen Assets und Daten fokussieren.

Business-Entscheider und Cyber-Sicherheitsexperten im Unternehmen müssen auf einer Linie sein, was Security anbelangt – vor allem hinsichtlich klarer Rollen, Verantwortlichkeiten und Prioritäten. Ein gegenseitiges Verständnis zu entwickeln, ist dabei elementar. Führungskräfte auf Management-Ebene sollten deutlich machen, was sie befürchten und wie sie ein erfolgreiches Security-Programm definieren. Dazu müssen sie Assets, Personen und Prozesse identifizieren, die für das Unternehmen geschäftskritisch sind, sowie Ziele und Budgets für Cyber-Sicherheitsinvestitionen und Prozesse festsetzen. Im Gegenzug müssen die Security-Experten Bedrohungen und Sicherheitslücken erkennen und melden, Programme und Gegenmaßnahmen empfehlen sowie die Wirksamkeit von Cyber-Sicherheitsinvestitionen messen, überwachen und reporten. Sie treffen Personal- und Beschaffungsentscheidungen im Security-Bereich. Außerdem sind sie für die operative Ausführung des Cyber-Sicherheitsprogramms verantwortlich.

Das Wichtigste aber ist: Business- und Security-Führungskräfte brauchen einander, um ihre Aufgaben effektiv zu erfüllen. Business-Entscheider können ohne die Informationen der Security-Experten und ohne deren Beratung schlichtweg keine Prioritäten, Ziele und Budgets festsetzen. Auf der anderen Seite brauchen Security-Leiter den kaufmännischen Blickwinkel der Geschäftsführung, um erfolgreich zu sein. Obwohl Führungskräfte auf beiden Seiten die jeweiligen spezifischen Rollen des anderen respektieren, arbeitet keiner von ihnen isoliert in einem Silo.

>> Wirtschaftlicher Schaden vs. Risiko <<

Nicht alle Bedrohungen sind gleich. Um Abwehrmaßnahmen zu priorisieren, muss man den potenziellen wirtschaftlichen Schaden, den ein Risikofaktor anrichten kann, gegen die Kosten für seine effektive Bekämpfung abwägen. So kann es etwa sinnvoller sein, eine Bedrohung auf ein akzeptables Maß zu reduzieren, als sie vollständig zu beseitigen. Wenn es zum Beispiel doppelt so viel kostet, Spam-Nachrichten komplett zu eliminieren, statt zu 99 %, dann kann ein Unternehmen vielleicht mit zwei bis drei Spam-Nachrichten pro Tag leben. In diesem Fall ist es günstiger, Mitarbeiter regelmäßig per E-Mail daran zu erinnern, jeden Spam in ihrem Posteingang zu ignorieren.

In der Regel gibt es mehr interne Risikofaktoren für Cyber-Sicherheit als externe. Diese inneren Schwachstellen gefährden Unternehmen unabhängig von der äußeren Bedrohungslage. Zu ihnen zählen etwa Mitarbeiter, Auftragnehmer oder andere Personen mit Infrastrukturzugriffsrechten, die dem Unternehmen vorsätzlich Schaden zufügen wollen. Gefährlich sind außerdem fragmentierte, unkoordinierte Abwehrmechanismen und eine überlagerte IT-Landschaft mit Systemen vieler verschiedener Hersteller. Viele Unternehmen fokussieren zudem auf abstrakte Compliance statt auf echten Schutz. Neue Schwachstellen entstehen, wenn sich Geschäftsaktivitäten und Prozesse schneller ändern als Sicherheitsstrategien und -Investitionen. Die Angriffsfläche erhöht sich also potenziell jedes Mal, wenn Unternehmen in neue Technologien investieren oder ihre IT-Infrastruktur erweitern.

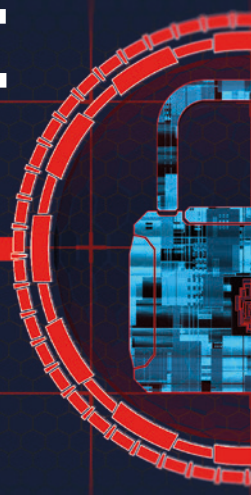
> Eine dynamische und dauerhafte Security Fabric ist gefragt.

Zudem sollte nicht vergessen werden: Cyber-Kriminelle werden immer gewiefter. Wichtig zu bedenken: Nicht nur ich als Unternehmen kann im Fokus stehen. So wählen Hacker Clients oder Netzwerke als Sprungbrett, um in andere Organisationen einzudringen. Das war zum Beispiel bei einem Heizungs- und Lüftungsunternehmen der Fall. Hacker nutzten dessen Computer als Vektor, um Transaktionsdaten von Debit-Karten von Kunden einer großen Baumarktkette zu stehlen.

Letztlich spricht ein prioritätsorientierter Ansatz für Cybersecurity stark für eine Sicherheitsarchitektur, die auf einer umfassenden und anpassungsfähigen Security Fabric basiert. Denn die einzige Konstante im Business und in der Cyber-Sicherheit ist Wandel. ■

Foto: Fortinet

MEHR ALS DIE SUMME ALLER TEILE



Sicherheit für Endgeräte? Dieses Thema wird vor allem der Informationstechnik zugeordnet, ist aber auch bei Überspannungsschutz, Flammendurchschlagsicherung und selbst Detonationssicherheit relevant.

VON KARIN LEGAT

Die größten Sicherheitsrisiken in Unternehmen aus Gerätesicht? Das sind falsche Benutzung, mangelnde Awareness der Anwender, Malware, Phishing und Social Engineering, vorsätzliches Anwenderfehlverhalten, generell die Vernetzung von Geräten und Anwendungen sowie überhaupt ungesicherte und mangelhaft gesicherte »Endpoints«. Gleichzeitig sind Smartphone, Tablet und Co bereits wertvollere Informationsträger und -mittler. Laut Umfragen sind bei Sicherheitsvorfällen am häufigsten PCs und Notebooks (34 %), Netzwerke (31 %) sowie Smartphones und Tablets (30 %) betroffen. Das ist insofern kritisch, als sie als Einfallstor in das Rechenzentrum genutzt werden. In Umfragen ortet mehr als die Hälfte aller IT-Verantwortlichen die größere Gefahr eher von den eigenen Mitarbeitern als von Cyber-Kriminellen ausgehend. Thomas Masicek, Chef des Bereichs Cyber Security bei T-Systems Austria: »Auf privaten Smartphones sind meist zahlreiche veraltete Apps installiert, die

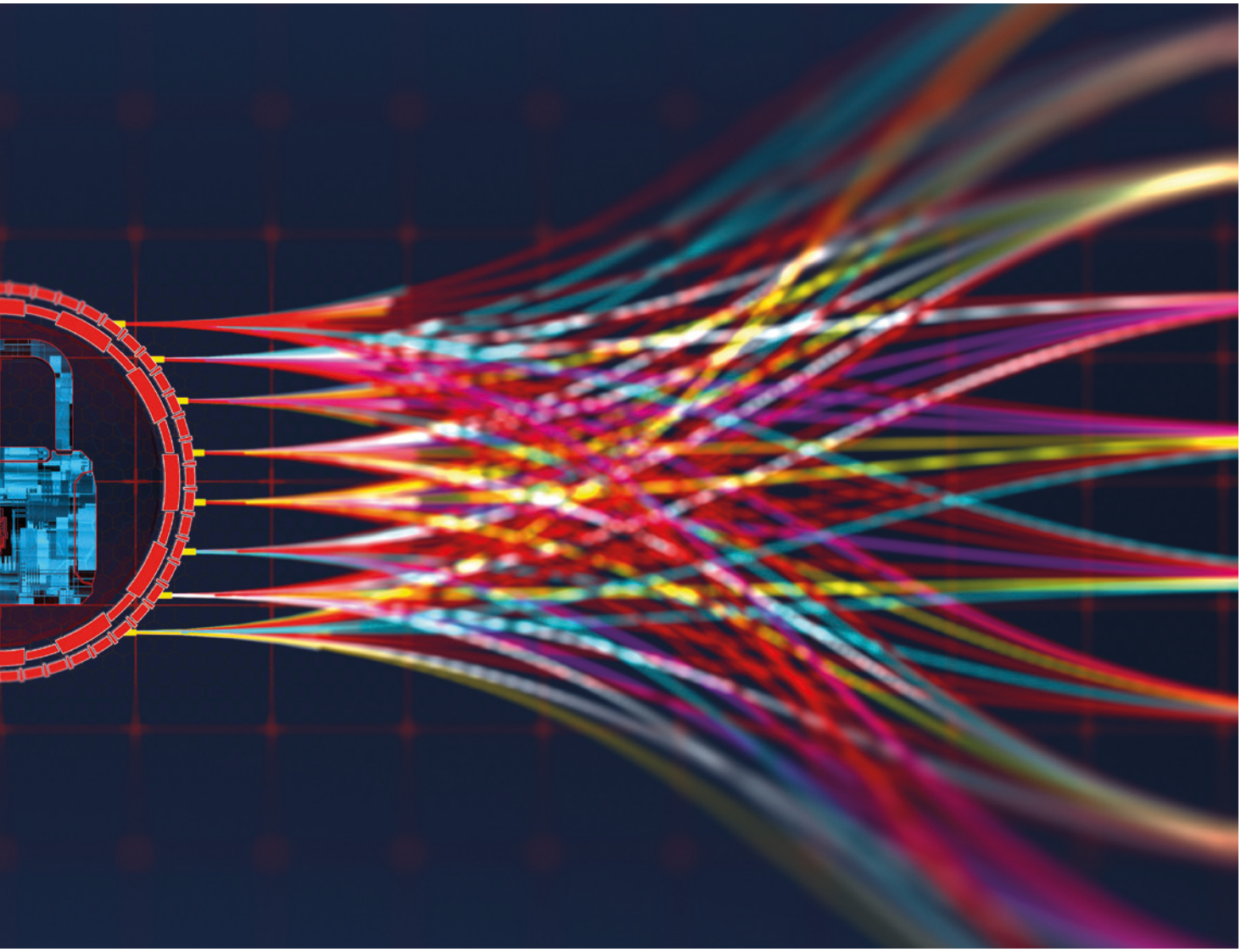
TIPPS FÜR SICHERHEIT BEI IOT-PROJEKTEN

1. Risiken identifizieren und Schritt für Schritt sichern. Um sich adäquat schützen zu können, sollte mit einer Risikoanalyse gestartet werden. Auf Basis dieser Risikoanalyse können Unternehmen ein umfassendes Sicherheitskonzept entwickeln. Idealerweise nutzen sie dabei den Defense-in-Depth-Ansatz. Dabei wird die IT-Architektur wie eine Zwiebel in verschiedene Schichten aufgeteilt und mit passenden Maßnahmen abgesichert. Gelingt es einem Angreifer, die Barrieren einer Schicht zu überwinden, steht er vor der nächsten verschlossenen Tür.

2. Von Grund auf sicher. Noch besser ist jedoch Security by Design. Das Sicherheitsmanagement beginnt noch einen Schritt früher. Schon bei der Auswahl von Anlagen, Geräten, Systemen und Netzwerkkomponenten sollten Unternehmen darauf achten, ob der Hersteller Sicherheitsaspekte bereits mit dem ersten Entwicklungsschritt in das Produkt integriert hat (Security by Design). Das gilt auch für den Bezug von Konnektivitäts- und Cloud-Diensten. Anbieter wie die Deutsche Telekom lassen ihr hohes Sicherheitsniveau regelmäßig prüfen und zertifizieren. Denn nur wenn Sicherheit stetig weiterentwickelt wird, lässt sich ein möglichst hohes Schutzniveau erreichen.

3. Regelmäßig aktualisieren. Täglich werden neue Schwachstellen und Angriffsvektoren für Softwarekomponenten bekannt. Dies trifft auch für IoT-Systeme zu. Daher sollten alle Geräte regelmäßig auf existierende Schwachstellen überprüft und auf einem aktuellen Patchlevel gehalten werden.

Foto: iStock



hohes Sicherheitsrisiko darstellen.« Gerade das Modell »Bring Your Own Device« (BYOD), das in vielen Firmen praktiziert wird, erfordert ein umfangreiches Sicherheitskonzept: die Einbindung in ein Mobile Device Management (MDM), die Möglichkeit der Fernlöschung von Unternehmensdaten, eine strikte Security-Policy, die verpflichtende Verschlüsselung aller Unternehmensdaten sowie einen PIN-Schutz. Es braucht ein Überdenken von Security, denn auf mobile Technologien kann nicht mehr verzichtet werden. Die Endgerätesicherung muss dazu mit den konstanten technischen Erneuerungen in sämtlichen Bereichen Schritt halten. Sicherheit darf aber nicht auf die Anwender abgeladen werden. Es gilt, sichere Architekturen im Hintergrund bereitzustellen, Stichwort Security by Design.

>> Wege zur Sicherheit <<

Beim Schutz gegen Cyber-Kriminalität konzentrieren sich viele Unternehmen hauptsächlich auf die Perimeter-Firewall und den sogenannten North-South-Traffic. Es braucht aber auch Data Security wie E-Mail-Verschlüsselung und Authentifizierung, Network Security wie IP-Adress-Management-Konzepte, Internet Security – Firewall und Secure Access – sowie Endpoint Security. Dazu zählen Anti-Virus, Anti-Malware, Personal Firewall und Host IPS oder etwa Festplattenverschlüsselung. Beim Management mobiler Geräte spielt Enterprise Mobility Management eine wichtige Rolle. Jede App verfügt hier über einen isolierten Speicherplatz und isolierten Arbeitsspeicher. Thomas Masicek: »Mobile Endgeräte sind ständig unterwegs, direkt mit dem Internet verbunden und durch kein ▶

> *Industrielle Steuerungsanlagen stellen eine besondere Herausforderung für die moderne Cybersicherheit dar.*

INFO

Die internationale Normenfamilie IEC 62443 befasst sich mit der IT-Security sogenannter »Industrial Automation and Control Systems«. Sie wurde ursprünglich als Norm für die Automatisierungstechnik in der Prozessindustrie entwickelt, deckt heute alle Industriebereiche von diskreter Fertigung bis zu verteilten Versorgungssystemen ab. Die Norm wird laufend weiterentwickelt.

TIPPS FÜR DIE SICHERHEIT AUF MOBILEN ENDGERÄTEN

Was ist für Firmen bei »Bring Your Own Device (BYOD)« zu beachten?

Auf privaten Smartphones sind meist unzählige veraltete Apps installiert, die ein hohes Sicherheitsrisiko darstellen. BYOD erfordert daher ein umfangreiches Sicherheitskonzept. Generell sollten bei BYOD-Modellen niemals Unternehmens- und Privatdaten vermischt werden. Wenn dies nicht der Fall ist, können beispielsweise Unternehmensdaten, die in derselben App gespeichert sind, im Rahmen der Privatnutzung unbeabsichtigt auch Dritten zugänglich gemacht werden. Gängige Mobile-Device-Management-Systeme ermöglichen stets eine getrennte Speicherung der Daten auf dem Smartphone. Das Unternehmen benötigt stets Zugriff auf das Gerät, um beispielsweise Wartungsaktivitäten durchführen oder im Verlust- oder Kündigungsfall Unternehmensdaten vom Gerät löschen zu können. Gibt es keine saubere Trennung, kann es zu einer unbeabsichtigten Löschung von Privatdaten kommen.

Welche Programme und Dienste sollten Firmen zulassen und welche nicht?

Grundsätzlich ist wichtig, dass lediglich vertrauenswürdige Software auf Smartphones installiert wird. Dies kann mittels Black- oder Whitelisting zentral durch ein MDM erfolgen. Viele Apps sind dafür bekannt, dass sie ihre Benutzer ausspionieren. Solche Apps haben genauso wenig auf einem Smartphone verloren wie Jailbreaks oder gehackte Programme. Die Nutzung von Social Media und Kommunikationsplattformen wie WhatsApp erfordern klare Vorgaben vom Unternehmen. Wichtig ist, dass unternehmensinterne und datenschutzrechtliche Vorgaben strikt eingehalten werden: Fotos von erkennbaren Personen dürfen ohne Einverständnis zum Beispiel nicht veröffentlicht werden. Ebenso muss beachtet werden, dass unangebrachte Nachrichten im Unternehmenskontext stets auf das Unternehmen zurückfallen.

Quelle: T-Systems

abgesichertes Unternehmensnetzwerk vor unerlaubten Zugriffen geschützt.« Die zentrale Verwaltung über Mobile-Device-Management-Systeme sei daher unerlässlich. Ein MDM ermöglicht die zentrale Konfiguration sowie die Sperre des Zugriffs im Fall von Sicherheitsproblemen oder die Sperre veralteter Apps.

Wie sich Unternehmen zusätzlich vor Cyberattacken schützen können, dazu hat *Report(+)PLUS* auch mit Gilles Gabriel, Vice President Sales EMEA bei Quantum, gesprochen: »Eine effektive Methode zum Schutz der Daten vor Cyberangriffen besteht in der Aktualisierung der IT- und Backup-Infrastruktur, indem Offline-Speichermedien wie zum Beispiel Tapes Cloud- und Disk-basierte Backup-Systeme hinzugefügt werden.«

>> Ideen der Industrie <<

Sicherheit von Endgeräten schaffen auch Industrietechnik-Konzerne wie ABB mit Prozessleitsystemen, in die bereits Sicherheitsfunktionen integriert sind. ABB stimmt sich dafür eng mit einschlägigen Sicherheitsrichtlinien von Organisationen wie ISO/IEC, VDI/VDE, Namur und BSI ab. Darüber hinaus praktiziert ABB bei der Produktentwicklung Secure by Design. Zielführend ist auch die Umsetzung des sogenannten Defense-in-Depth-Ansatzes, also eines mehrschichtigen Sicherheitskonzeptes,

Erich Kronfuss, Phoenix Contact: »Jede Maschine muss in sich verfügbar sein. Die Kommunikation läuft von innen nach außen.«

in dem sich die ausgewählten Sicherheitsmechanismen gegenseitig ergänzen.

Bei Siemens wird ganzheitliche Security beginnend bei den Endgeräten etwa mittels Port Authentication IEEE 802.1x realisiert, die auf Zertifikaten basierend sicherstellt, dass Endgeräte im Netzwerk teilnehmen dürfen. Nur mit erfolgreicher Anmeldung und gültigem, verschlüsselten Zertifikat

Foto: iStock, Phoenix Contact, Quantum

> *Die bisherigen Mittel der Abschottung sensibler kritischer Infrastrukturen und der Kontrolle der Datenströme stoßen an ihre Grenzen.*

Das Speichern von Unternehmensdaten auf privat genutzten Smartphones stellt ein großes Sicherheitsrisiko dar.

kann eine Kommunikation aufgebaut werden. Entscheidend ist die klare, unterbrechungsfreie Kommunikation.

Laut Erich Kronfuss, Industrial IoT Security Specialist bei Phoenix Contact, besteht im Maschinenbau und Anlagenbe-

Gilles Gabriel, Quantum: »Eine effektive Abwehrmethode besteht in der Aktualisierung der IT- und Backup-Infrastruktur.«

trieb bei IT-Anwendungen grundsätzlich kein Bedarf für den Zugang ins Internet. Daher werden diese Systeme isoliert von anderen, unsicheren Netzen betrieben. Um diese in ein übergeordnetes Netzwerksystem sicher einbinden zu können, gibt es die internationale Normenreihe IEC 62443 über industrielle Kommunikationsnetze – eine IT-Sicherheit für Netze und Systeme, an der seit einigen Jahren gearbeitet wird. Eine der beschriebenen Methoden in diesem Standard ist die Zonierung und die gesicherte Verbindung der Netze. Das ist das Sicherheitskonzept der Industrie.

In der praktischen Umsetzung bedeutet dies zumeist, dass innerhalb eines Anlagennetzwerks eine eigene private IPv4-Adresse genutzt wird und kein Routing-Eintrag auf den Maschinen oder auch Windows PCs erfolgt. Wenn ein IP-System außerhalb des lokalen Anlagennetzwerks kommunizieren muss, so wird eine 1:1-NAT-Verknüpfung am Switch, Router und Firewall eingetragen.

Eine solche Segmentierung bewährt sich für Kronfuss auch in der konventionellen IT, erzielt durch mGuard. Die mGuard-Familie von Phoenix Contact umfasst eine Reihe an Security-Apps für Anwendungen wie sichere Fernwartung oder sichere Zugriffe durch Service-Mitarbeiter. Die Apps beinhalten Firewall-, Routing- und VPN-Funktionalitäten zum Schutz vor bösartigen Cyber-Attacken und ungewollten Störungen sowie die sichere Fernwartung über öffentliche Netze.

Die TU Wien setzt gemeinsam mit Phoenix Contact in der Pilotfabrik 4.0 in Aspern in Wien das Security und Netzwerk Modell der IEC 62443 um. »Die digitalisierten Produktionsschritte sind direkt am Shop-Floor in autonome Zonen aufgeteilt und über ein Produktionsnetzwerk sicher zusammengeführt«, informiert Kronfuss und lädt Interessierte zu einer Führung durch die Pilotfabrik 4.0 ein: »Wir wollen die Umsetzung des internationalen Standards IEC 62443 zeigen.«

>> Industrial Security <<

Die Automatisierung in der Industrie hat heute einen so hohen Grad der Vernetzung erreicht, dass eine Produktion ohne sie nicht mehr vorstellbar ist. Die bisherigen Mittel der Abschottung sensibler kritischer Infrastrukturen und der Kontrolle der Datenströme stoßen an ihre Grenzen. In der Industrial Security oder Automation Security geht es um die Absicherung aller Komponenten und Prozesse, die für den zuverlässigen und sicheren Betrieb einer automatisierten Produktionsanlage notwendig sind. Dazu gehören Steuerungen – genauer: speicherprogrammierte Steuerungen (SPS) – , Leitsysteme, Netzwerkkomponenten wie Firewalls oder Switches, Clients, Applikationen ebenso wie Prozesse der Planung, Umsetzung, Schulung, Bedienung und Wartung. Experten sind sich einig, dass Security gleichwertig neben anderen Produkt- und Produktionseigenschaften wie Qualität oder Safety zu behandeln ist. »Zuallererst gilt: Jede Maschine muss in sich verfügbar sein – die Kommunikation läuft von innen nach außen«, stellt Kronfuss fest.

INFO

Durch die ständigen Erneuerungen technischer Geräte, die immer smarter und vernetzter werden, entstehen völlig neuartige Sicherheitsrisiken. Dieser Fortschritt bedeutete für Siemens bereits in den letzten Jahren großen Bedarf an Maßnahmen zur Prävention von Cyber-Security Attacken. In den nächsten Jahren wird sich die Endgerätesicherung auf alle Geräte, die smart werden oder schon sind, ausweiten. Bis vor einigen Jahren waren Lichtschalter alles andere als »smart«, mittlerweile gibt es smarte Lichtschalter, die sich mittels Sprachsteuerung oder per App bedienen lassen. Bei einer solchen Vernetzung steigen natürlich auch die Sicherheitsrisiken.

Der größt

(+) PLUS: Wie ausgeprägt ist aus Sicht eines Versicherungsunternehmens das Bewusstsein, sich gegen Cyberattacken schützen zu müssen?

Olivera Böhm: Groß- und Industriebetriebe sind massiv der Cyberkriminalität ausgesetzt. Laut KPMG Österreich waren bereits zwei Drittel der österreichischen Großunternehmen von Cyberattacken betroffen, weitere 21 Prozent wissen nicht einmal, ob sie bereits Opfer eines Angriffes wurden. Der Schaden durch solche Attacken kann in die Millionen gehen.

(+) PLUS: Wo lauern aus Ihrer Sicht die größten Gefahren?

Böhm: Potenzieller Schaden droht besonders durch Datenverlust und Betriebsunterbrechung. Ein Datenleck, eine stehende Produktionsstraße oder gar eine vollständige Betriebsunterbrechung können enorme finanzielle Verluste verursachen. Neben schnell eintretenden materiellen Schäden drohen nachhaltige Reputationsverluste, die letztlich die Existenz des gesamten Betriebs bedrohen.

Viele Betriebe und auch Private in Österreich haben bereits heute umfangreiche Vorsorgen gegen Cyberattacken getroffen. Das beginnt bei einem Virenschutz und geht weiter über Firewalls, technische Absicherungen und reicht bis hin zu Datenschutz und Vorkehrungen im Rahmen der Datenschutzgrundverordnung. Nur: Die größte Gefahr ist immer der Mensch. Alle Schutzeinrichtungen sind wirkungslos, wenn sie nicht beachtet werden. Unachtsam geöffnete Mailanhänge oder USB-Sticks von Unbekannten zählen zu den häufigsten Ursachen für Cyberattacken. Auch bei einem Hackerangriff

»Bei einem Cyberangriff ist rasches Handeln zur Betriebsfortführung gefragt: Dann heißt es Netzwerke sichern, Systemintegrität wiederherstellen und alle nötigen technischen, rechtlichen und kommunikativen Schritte unternehmen«, erklärt Olivera Böhm, Head of UNIQA Corporate Business.

Foto: Sabine Klimpt

e Schaden droht durch Datenverlust und Betriebsunterbrechungen

VON BERND AFFENZELLER

Gegen Cyberattacken kann man sich schützen. Wenn doch etwas passiert, sollte man zumindest gut versichert sein. Im Interview mit Report(+)PLUS erklärt Olivera Böhm, Head of UNIQA Corporate Business, welche Leistungen eine Cyber-Versicherung umfasst und was im Ernstfall geschieht, um die Auswirkungen eines erfolgreichen Angriffs so gering wie möglich zu halten.

ist in den allermeisten Fällen der Mensch die Schwachstelle.

(+) PLUS: Welche Bereiche und Leistungen umfasst eine Cyber-Versicherung bei UNIQA?

Böhm: Beim Industrie- und KMU-Produkt sind einerseits Haftpflichtansprüche versichert, die etwa durch Datenschutzverletzungen oder Cyberattacken entstehen. Andererseits besteht Deckung sowohl für Eigenschäden wie Betriebsunterbrechungen durch Cyberangriffe als auch für die Kostenübernahme im Rahmen der Wiederherstellung aller Systeme und Daten. Ebenfalls gedeckt sind Kosten von behördlichen Verfahren bei Datenschutzverletzungen. Der Deckungsrahmen kann bis zu 20 Millionen Euro betragen.

Für Private kann ein Cyber-Schutz in die bestehende Haushaltsversicherung inkludiert werden und umfasst einen Online-Shoppingschutz und eine 24-Stunden-Hotline. Zudem bieten wir unseren Privatkunden ein Online-Monitoring, das das Internet und Darknet permanent nach Missbrauch der Email- und Bankdaten unserer Kunden scannt. Daneben bieten wir Schutz bei Online-Käufen, die nicht geliefert werden.

(+) PLUS: Mit welchen Kosten ist zu rechnen?

Böhm: Der Cyber-Schutz für Private ist bereits ab fünf Euro im Monat zu haben. Klein und Mittelbetriebe müssen mit rund 435 Euro im Jahr rechnen. Bei Industriekunden ist die Prämie abhängig von Branche, Umsatz, Versicherungssumme und natürlich von der Art des versicherten Risikos und liegt im niedrigen fünf- oder sechsstelligen Eurobereich.

(+) PLUS: In welchen Bereichen verzeichnen Sie die meisten Schadensfälle?

Böhm: UNIQA ist erst seit einigen Monaten mit diesen Produkten am Markt. Repräsentative Daten liegen leider noch nicht vor. Wir erwarten aber vermehrt Schäden aus den Bereichen Datenschutz und Betriebsunterbrechung nach einem Cyberunfall. Aber ein herausstechender Fall, der jedoch nicht bei uns versichert war, aber aus den Medien bekannt ist, war die Attacke auf das Lukaskrankenhaus Neuss in Deutschland: Nach einem Virusbefall musste es zwei Wochen lang ohne IT-Systeme arbeiten und auf Handbetrieb umstellen. Der Betriebsausfall sowie die IT-Maßnahmen zur Wiederherstellung kosteten rund eine Million Euro.

(+) PLUS: Welche Rolle spielt die Prävention im Angebot von UNIQA?

Böhm: Basis der Industrielösung ist eine individuelle Risikoanalyse in Form eines webbasierten Risikofragebogens. Daraus erstellt UNIQA einen Risiko-Report, der den Kunden zu möglichen Risiken in ihren Systemen und Abläufen Auskunft gibt und Basis für den Versicherungsabschluss ist. Gleichzeitig erhält der Kunde auch eine umfangreiche Dokumentation zu Stärken und Schwächen im eigenen Unternehmen.

(+) PLUS: Wie ist der Ablauf im Ernstfall, wenn ein Unternehmen oder eine Privatperson Opfer einer Cyberattacke wurde?

Böhm: Sowohl für private als auch für Unternehmen gibt es eine Hotline, die 24 Stunden erreichbar ist. Bei Privaten steht die Beratung und Hilfe im Ernstfall im Mittelpunkt. Industriekunden wird Hilfe geleistet, um nötige Gegenmaßnahmen zu setzen, das kann die Abschottung der Systeme und forensischen Untersuchungen ebenso betreffen wie im Notfall einfach den Stecker zu ziehen. Hier ist das wichtigste Ziel, so rasch wie möglich die Produktion wieder aufnehmen zu können, um Folgeschäden durch eine Betriebsunterbrechung so gering wie möglich zu halten.

(+) PLUS: Welche Schritte setzt UNIQA, um Unternehmen eine Betriebsfortführung im Schadensfall zu ermöglichen?

Böhm: Bei einem Cyberangriff ist rasches Handeln zur Betriebsfortführung gefragt: Dann heißt es Netzwerke sichern, Systemintegrität wiederherstellen und alle nötigen technischen, rechtlichen und kommunikativen Schritte unternehmen. Gemeinsam mit einem Partnernetzwerk bestehend aus T-Systems Austria als IT-Sicherheitsexperten, Schönherr Rechtsanwälte als »Legal Advisor« und Pantarhei als PR-Krisenberater bietet UNIQA den Kunden in diesen schwierigen Zeiten kompetente und rasche Hilfe an. Aufwendungen im Zuge des Krisenmanagements wie beispielsweise anwaltliche Beratung oder Public-Relations-Krisenberatung fallen unter den Deckungsumfang der UNIQA Industriekunden-Cyberversicherung. ■

WEG IN DIE ZUKUNFT

VON KARIN LEGAT

DER DIGITALE PFAD FÜR PRIVATE UND UNTERNEHMEN IST MITUNTER STEINIG. NICHT NUR IT-SECURITY IST GEFORDERT – AUCH BILDUNG UND GESELLSCHAFT.

Laut Bundeskriminalamt gibt es kaum eine Kriminalitätsform, bei der Elektronik, IT und ihre Vernetzung keine Rolle spielen. In Österreich hielt sich die Zahl der Cybercrime-Delikte zwischen 2012 und 2015 bei etwa 10.000, 2016 sprang sie auf 13.100 und 2017 auf 16.800. 2017 wurden laut dem US-Versicherungskonzern American International Group weltweit so viele Stör- und Cyberattacken verzeichnet wie in den vier Jahren davor zusammengenommen. Bei den Angriffen handelt es sich meist um Ransomware, Verschlüsselungstrojaner, die den Datenzugriff oder den gesamten Computer bis zur Lösegeldzahlung lahmlegen. Zuletzt hat auch das Abschöpfen von Kryptowährungen von einzelnen Servern oder Computern zugenommen. In nahezu allen Geräten und Lebensbereichen spielen Computer mittlerweile eine zentrale Rolle. Die Welt ist geprägt von umfassender Digitalisierung und Vernetzung.

»Man muss keine physikalischen Hindernisse überwinden. Mit dem gleichen Effekt kann elegant, mit weniger Kosten und einfacher in jedes System weltweit eingedrungen werden. Alles läuft elektronisch«, benennt Helmut Leopold, Head of Center for Digital Safety & Security am AIT, das große Bedrohungs-

> DIE SICHERSTE IT-INFRASTRUKTUR HILFT NICHTS, WENN DER USER FAHRLÄSSIG HANDELT.

DER AUSBLICK IST DIGITALER DENN JE

Die Cyber Range ist eine virtuelle Umgebung des AIT mit online Zugriffsmöglichkeiten für die flexible Simulation kritischer digitaler IT Systeme mit unterschiedlichen Systemkomponenten und Benutzerstrukturen. Ein internationales Team forscht an modernsten Cyber-Security-Technologien, wie Security by Design, neuen Verschlüsselungstechnologien und künstlicher Intelligenz.

szenario. Digitalisierung und Vernetzung finden sich nicht nur im IT-Netz eines Unternehmens, vielmehr auch bei Brandmeldeanlagen und Videoüberwachung, Zutrittskontrolle und Sprachalarmierung. Schutz vor Bedrohung durch Internetkriminalität gestaltet sich für Privatpersonen als auch für Unternehmen und Einrichtungen der öffentlichen Verwaltung immer anspruchsvoller. »Das bremst leider das Vertrauen in neue Technologien, die eigentlich viel Potenzial für das Gemeinwohl haben«, betont Harald Leitenmüller, Chief Technology Officer von Microsoft Österreich.

>> Cybercrime im Vormarsch <<

Die Angriffe werden technisch immer raffinierter. Im Fokus der Angreifer stehen meist große Konzerne und mittelständische Betriebe. Aber nicht nur Banken, Versicherungen oder Fondsgesellschaften müssen sich gut vor Cyber-Attacken schützen. Spätestens seit Inkrafttreten der EU-Datenschutzgrundverordnung sollten auch Berater ihre IT-Systeme aufgerüstet haben. Nicht selten haben es Kriminelle auf hochsensible Daten abgesehen. Verschlüsselungstrojaner werden meist durch E-Mails, unsichere Downloads aus dem Internet sowie Sicherheitslücken in den verwendeten Web-Browsern und Betriebssystemen verbreitet. Ebenfalls auf die Verbreitung durch E-Mails setzen Cyberkriminelle bei Phishing-Attacken.

Die Bekämpfung von Cyberkriminalität und Schaffung sicherer Umgebungen muss deshalb oberste Priorität haben. Für einige Firmen wird das zum Problem. Denn durch die steigende Komplexität von IT-Systemen und immer neue Bedrohungslagen verfügen manche Unternehmen intern nicht mehr über die notwendigen Ressourcen. Sie müssen externe Partner wählen. Die Kosten für »Managed Services« liegen nicht in astronomischen Höhen – je nach Funktionsumfang zwischen zwei und zehn Euro pro Mitarbeiter und Monat. Wichtig ist die regelmäßige Überprüfung, ob die Geschäfts-Unit über die bestmögliche Software für die spezifischen ▶

TIPP

DIE ZAHL DER CYBER-ATTACKEN IST IN DEN LETZTEN JAHREN MASSIV GESTIEGEN. SIEBEN TIPPS, WIE SICH UNTERNEHMEN VOR UNLIEBSAMEN ANGRIFFEN SCHÜTZEN KÖNNEN.

1. Nicht nur das Virenprogramm updaten, sondern auch Software, Betriebssysteme und Firewall.
2. Umfassende Backup-Strategie bereit haben, z.B. gegenseitig überwachende Server-Systeme und tägliche Sicherungen, die offline aufbewahrt werden.
3. Passwortregelungen – Verzicht auf einfache Zahlenkombinationen sowie regelmäßige Änderung.
4. Erstellen einer Desaster-Recovery-Strategie für den Notfall.
5. Entsprechende Zusammenarbeit mit dem Internetdienstanbieter rund um die Überwachung des Datenverkehrs im Backbone.
6. Aufstellen einer Risiko-Analyse und einer Strategie zur Schadensbegrenzung.

Quelle: Iphos IT Solutions

In der Digitalen Fabrik der FH Technikum Wien wird ein integriertes Sicherheitskonzept als Pilotprojekt implementiert, validiert und von TÜV Austria zertifiziert. Die Digitale Fabrik ist Living Lab für den Wissenstransfer an Unternehmen, v.a. KMU, und Hochschulen.

Die Maschinensicherheit wird aufgrund des zunehmenden Softwareanteils in der intelligenten Produktion immer stärker von der IT-Sicherheit bestimmt. Maschinensicherheit (Safety) und IT-Sicherheit (Security) sind nicht mehr trennbar. Mit diesen komplexen Wechselwirkungen befasst sich das Forschungsprojekt SIP 4.0 an der FH Technikum Wien.

„MALWARE WIRD SMARTER UND IST IN DER LAGE, SICH INTELLIGENT ANZUPASSEN UND TRADITIONELLE ERKENNUNGS- WIE BESEITIGUNGSROUTINEN ZU UMGEHEN."

Anforderungen des Netzwerks verfügt. Zusätzlich sollten Protokolle aktiv sein, die dafür sorgen, dass diese Software niemals versehentlich deaktiviert wird. Daher ist es ratsam, eine Gruppenrichtlinienkontrolle einzurichten, die Endbenutzer und untergeordnete Administratoren daran hindert, die Anti-Malware-Software zu deaktivieren.

>> Awareness-Training <<

»Die digitale Transformation verändert jeden Bereich unseres Lebens grundlegend«, betont Harald Leitenmüller. Sieht er auch, dass wir Richtung vorgegebenes Leben steuern, Richtung gesicherter Ablauf? Ganz im Gegenteil: »Ein vorgegebener, strikter Ablauf gehört der Vergangenheit an.« Leitenmüller sieht Cloud Computing als hochflexibles Angebot, welches in der Lage ist, Menschen und Unternehmen in ihrer individuellen und unterschiedlichen Art zu unterstützen, Rechenleistungen an jedem Ort und zu jeder Zeit in Anspruch zu nehmen. Dadurch lässt sich Beschäftigung flexibler an die individuelle Lebenssituation anpassen und wird familiengerechter.

Microsoft investiert jährlich mehrere Milliarden Dollar in die Sicherheit und Weiterentwicklung seiner Cloud-Infrastruktur, die Server werden laufend gegen die neuesten Sicherheitslücken gepatcht.

Helmut Leopold vom AIT weist auf ein generelles Manko hin. »Meine Generation hat die Technik noch hinterfragt und Bedienungsanleitungen gelesen. Die junge Generation, die damit aufwächst, sieht alles als automatisch an. Man drückt einen Knopf und es funktioniert. Sicherheit ist für sie unsichtbar.« Dazu brauche es dringend Awareness-Trainings. In den letzten Jahren sei hier zu wenig getan worden, so der Experte, es gibt vieles nachzuholen. Die sicherste IT-Infrastruktur hilft nichts, wenn der User fahrlässig handelt. Als Aufgabe der Eltern sieht Leopold dieses Aufrütteln nicht. »Ältere Technologien wurden über mehrere Generationen langsam eingeführt, YouTube, Facebook & Co sind über wenige Jahre auf den Markt gekommen. Plötzlich war die gesamte Welt vernetzt.« Es wäre unfair, Eltern in die Verantwortung zu nehmen. Stattdessen müssten Mediengesellschaft, Servicebetreiber, Hersteller und Technologieanbieter agieren und zum Beispiel auch mit dem Schulsystem massiv zusammenarbeiten.

>> Arbeit an der Sicherheit <<

»In der Sicherheitswelt von morgen sehen wir verstärkt den Einsatz von Machine

„Für Helmut Leopold, Head of Center for Digital Safety & Security, ist das Prinzip Security by Design ein Ausweg aus der Sicherheitsproblematik. »Bereits im Software-Entwicklungsprozess müssen Sicherheitsaspekte erheblich stärker beachtet werden. Software ist so unempfindlich als möglich gegen Angriffe zu konzipieren.« Das bedeute zwar einen höheren Aufwand beim Designen, aber im Finish eine höhere Sicherheit."

Foto: FH Technikum Wien/Baumgartner, AIT, Microsoft

> Erhöhte Sicherheitsvorkehrungen werden oft mit Produktivitätshemmungen assoziiert. Harald Leitenmüller widerspricht: »Mit Windows Hello ist das Login am Computer per Fingerabdruck oder ausgeklügelter Gesichts- und Iriserkennung möglich. Die Anmeldung am Rechner dauert weniger als zwei Sekunden. Das ist nicht nur schneller als die herkömmliche Passworteingabe, sondern auch sicherer.«

Learning und Artificial Intelligence zur Unterstützung der Angriffserkennung«, betont Christian Kaufmann, Leiter des Master-Studiengangs IT-Security an der FH Technikum Wien. Die Sicherheit der Zukunft schafft damit neue Jobs, die sich vor allem mit dieser Thematik befassen. Denn der Mensch am Arbeitsplatz wird auch in dieser Branche künftig nötig sein. Kaufmann: »Bislang haben wir keine Silver Bullet im Bereich der Cybersecurity gefunden, auch AI ist definitiv keine.«

Dem herrschenden Expertenmangel steht gegenüber, dass Cybercrime ein Milliardengeschäft mit enormen Zuwachsraten ist. Jeder kann Opfer werden. In den letzten Jahren wurden verstärkt Klein- und Mittelunternehmen angegriffen. Diesen Unternehmen fehlt oft das Budget für die notwendigen Sicherheitsmaßnahmen, sie wiegen sich aber oft in Sicherheit: »Welcher Angreifer hat Interesse an uns Kleinen?« Auch Privatpersonen sind, wie spätestens seit den Ransomware-Angriffen deutlich, ein lukratives Ziel.

Auch die Gegenwehr organisiert sich: Microsoft verweist auf seine Digital Crimes Unit, die bereits vor über zehn Jahren geschaffen wurde. Am AIT wird seit Jahren ein modernes Cyber-Trainingszentrum betrieben, die Cyber Range, in der Schutz- und Abwehrmaßnahmen kritischer IT-Infrastrukturen realitätsnah getestet werden können.

AIT-Manager Leopold fordert, dass das Prinzip Security by Design vorangetrieben wird. »Alles, was wir bauen, ist funktionalitätsgetrieben, besser und schneller. Sicherheit wird als automatisch vorhandener Faktor angesehen und hat bislang keinen Marktwert.« Der Experte ortet das als menschliches Problem. Wenn die Gefahr nicht gesehen wird, warum soll ich mich dagegen schützen? Das betrifft auch die Industrie, die mitunter Sicherheitsmaßnahmen reduziert, wenn sie nicht eingefordert werden. Dort braucht es Standards und Vorgaben wie die NIS-Richtlinie, die EU-Richtlinie zur Sicherheit bei Netz- und Informationssystemen. Neue Zukunftstechnologien wie künstliche Intelligenz und das Internet der Dinge müssen den aktuellen Regeln und Gesetzen für das Sammeln, Nutzen und Speichern von Daten entsprechen. Die NIS-Richtlinie zielt auf Cybersicherheit, gilt für kritische Infrastruktur wie Trinkwasserversorgung, Energie, Finanz und Gesundheit und verlangt technische und organisatorische Maßnahmen zur Sicherung von Netzwerken sowie Informationssystemen und fordert die unverzügliche Benachrichtigung der Behörde bei Cyberattacken und Störfällen. »Der Kommunikationsaustausch muss verbessert werden. Vernetztes Kommunizieren ist nötig, denn kein Land kann die Probleme allein lösen. Kriminalität ist dagegen stets bestens vernetzt«, betont Leopold.

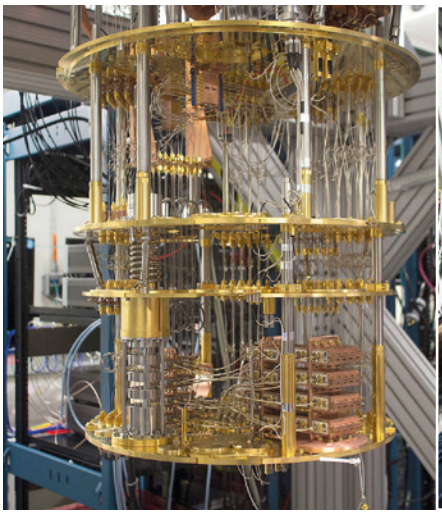
Vor zwei Jahren als Empfehlung veröffentlicht, hatten die EU-Mitgliedstaaten bis Anfang Mai Zeit, die Richtlinie in nationales Recht umzusetzen. Österreich ist säumig, NIS befindet sich nach wie vor in Begutachtung. Dem Vernehmen nach soll die Bundesregierung in den kommenden Wochen ein neues Cybersicherheitsgesetz vorstellen. Details daraus werden noch nicht genannt.

>> Security-Training <<

»In den klassischen informatiklastigen Bachelorstudiengängen wie Informatik, Wirtschaftsinformatik oder Informations- und Kommunikationssysteme wird das Thema IT Security im Regelstudium behandelt«, betont Christian Kaufmann. Darüber hinaus haben interessierte Studierende die Möglichkeit, ihr Wissen in Wahlpflichtfächern zu vertiefen. Mit dem Master IT-Security schafft die FH Technikum Wien eine fundierte und spezialisierte Ausbildung. Da Security eine komplexe Querschnittsmaterie ist, die viele Bereiche betrifft – von Security Policies für Unternehmen bis zu Ethical Hacking respektive Penetration Tests, von Risikoanalyse bis zur Firewall Konfiguration und System Hardening – bietet der Master IT-Security auch drei unterschiedliche Karrierepfade mit unterschiedlichen Wahlpflichtfächern an. »Jeder, der mit Computern zu tun hat, muss über ein grundlegendes Security-Knowhow verfügen. Die ›Dos and Don'ts‹ sollten bereits in der Sekundarstufe eins Teil des Unterrichts sein. Davon sind wir aber sehr weit entfernt«, bedauert Kaufmann. ■

DIGITALES IMMUNSYSTEM

Cyber-Angriffe und ihre Folgen stellen Unternehmen vor enorme Herausforderungen. Mit der Entwicklung von Quantencomputern wird künftig ein neues Kapitel in der digitalen Agenda aufgeschlagen.



Michael Osborne, Forschungsleiter im IBM-Zentrum Zürich, sieht in der Entwicklung des »IBM Q« größtes Potenzial.

Cyberattacken in Form von Trojanern, gehackten Passwörtern, Spam-Emails und vielen weiteren Formen von Datenklau sind zu einer Begleiterscheinung der digitalisierten Welt geworden. Beim Information Breakfast Meeting von IBM am 13. September skizzierten die IBM-Sicherheitsexperten Michael Osborne, Forschungsleiter Security im IBM Forschungszentrum in Zürich, und Matthias Ems, IBM Associate Partner Security Services DACH, die Potenziale und Risiken der IT-Sicherheit von morgen. Die 2018 präsentierte Studie »Cost of Data Breach«, die das Ponemon Institut in Zusammenarbeit mit IBM erstellte, beleuchtete neben der aktuellen Bedrohungslage auch die versteckten Kosten, die Datenpannen nach sich ziehen. So haben Unternehmen neben verlorenen Geschäftschancen und schlechtem Ruf auch mit den finanziellen wie personellen Ressourcen zu kämpfen, die zur Behebung der Datenpannen aufgewendet werden müssen. Die Studie, für die MitarbeiterInnen von mehr als 450 Unternehmen weltweit befragt wurden, beziffert die Kosten einer Datenpanne mit mehr als 3,8 Millionen Dollar.

>> Ganzheitliche Sicherheit <<

»In der Medizin beobachten wir seit Jahren den Trend, Patienten ganzheitlich zu behandeln. Auch im Management der Unternehmenssicherheit müssen wir weg von der Behandlung akuter Einzelfälle und beginnen, die IT-Sicherheit als ganzheitliches (Immun-)System zu betrachten. Nur so können Unternehmen den aktuellen Bedrohungen aktiv begegnen, die jährlich steigenden Schadenskosten regulieren und das Vertrauen ihrer Kunden behalten«, erklärt Sicherheitsexperte Matthias Ems. Neben der laufenden Weiterentwicklung intelligenter Systeme wie IBM Watson, die beim Aufdecken von Sicherheitsproblemen und Datenlecks unterstützen, forscht IBM an der Entwicklung von Quantencomputern, die aufgrund ihrer enormen Leistungsfähigkeit die IT-Sicherheit von morgen maßgeblich mitgestalten werden.

Forschungsleiter Michael Osborne sieht dringenden Handlungsbedarf, um IT-Systeme auch künftig absichern zu können: »Das Fenster, um neue kryptografische Schemata einzuführen, die nicht quantenresistent sind, schließt sich. Wir müssen jetzt schon daran arbeiten, dass die Daten, die wir heute schützen, auch in Zukunft sicher sind. Um die Nase vorn zu haben,brauchen wir neue Algorithmen, die auf herkömmlichen Computern laufen, aber gegen zukünftige Quantencomputer abgesichert sind.« Mit der Erforschung von Quantum-Safe-Kryptografiemethoden schaffen die IBM-Sicherheitsexperten die Voraussetzungen für eine sichere Entwicklung der Quantentechnologie, welche auf diese Weise zur Lösung künftiger Sicherheitsprobleme beitragen kann.

>> Partnerschaft mit der Forschung <<

Im IBM Q Network forschen Industrie und Wissenschaft gemeinsam an ersten kommerziellen Anwendungen der Quantentechnologie. Über die Cloud steht der derzeit modernste, skalierbare Quantenrechner weltweit Unternehmen und wissenschaftlichen Institutionen mit entsprechendem Hintergrundwissen zur Verfügung. Mit ihm können komplizierte Berechnungen schneller und effizienter als mit herkömmlichen Computern gelöst werden.

Als Gründungspartner sind JP Morgan Chase, die Daimler AG, Samsung sowie JSR, ein führendes japanisches Chemie- und Rohstoffunternehmen, in die Entwicklungsarbeit eingebunden. Erste und vielversprechendste Anwendungsfelder sind Simulationen von quantenmechanischen Vorgängen auf molekularer Ebene in der Chemie. Auch Medikamenten- und Materialforschung, die Optimierung von globalen Lieferketten und Logistikabläufen, neue Ansätze bei der Analyse von Finanzinformationen und Risikobewertungen sowie KI-Bereiche wie Machine Learning könnten von Quantencomputing-Technologie profitieren.

Seit dem Start der IBM Quantum Experience im Jahr 2016 führten rund 90.000 NutzerInnen mehr als 4,8 Millionen Experimente auf der Plattform durch. WissenschafterInnen und Studierende aus über 100 Ländern verwendeten die Lernangebote im Unterricht oder für ihre Forschung. Der jährlich vergebene »IBM Q Award« ging heuer nach Österreich: Alwin Zulehner von der Johannes Kepler-Universität Linz überzeugte in der »QISKit Developer Challenge« mit einem Compiler, den er für seine Doktorarbeit entwickelt hatte. ■

Foto: IBM

ARCHITEKTEN FÜR DIE SICHERHEIT

Usecase Industrie: Wie ein ICT-Dienstleister sein Kerngeschäft Informationssicherheit für einen Kunden in der verarbeitenden Industrie umgesetzt hat.

Ein in Österreich ansässiger, international tätiger Industriekonzern stand vor der Herausforderung, dass sein Security-Team aufgrund steigender Anforderungen und zu geringer Ressourcen die IT-Sicherheit nicht mehr gewährleisten konnte. Das Unternehmen lud zu einer Wettbewerbspräsentation, die T-Systems nach einer intensiven Proof-of-Concept-Phase für sich entscheiden konnte. T-Systems punktete mit seinem Cyber Security Competence Center in Wien, dem exzellenten Know-how der 40 in Österreich beschäftigten Security-Experten sowie seiner jahrelangen Erfahrung in diesem Bereich.

Die erfahrenen Security-Architekten von T-Systems designten gemeinsam mit dem Kunden die technische Lösung für eine auf zukünftiges Wachstum ausgelegte stabile Architektur, wobei die eingesetzte, kommerzielle Software auf die besonderen Anforderungen des Kunden angepasst wurde. Etabliert wurden traditionelle Sicherheitsmaßnahmen, mit starkem Fokus auf Prävention wie Anti-Viren-Lösung auf Clients und Servern, Firewalls, Proxy zum Filtern des Internet-Traffics. Ziele waren das Erkennung von Angriffen und laufende Unterstützung durch Security-Spezialisten von T-Systems und die generelle Erhöhung der Sichtbarkeit, um auf Knopfdruck analysieren zu können was in IT-Landschaften und im Netz gerade passiert.

Hinter der sogenannten Security Intelligence as a Service, kurz SIaaS, steht eine gemanagte Plattform zur übersichtlichen Bewertung der Bedrohungslage für die gesamte IT-Infrastruktur, die eine große Anzahl an Basisleistungen umfasst. Den technologischen Kern dieser Basiskomponenten stellt die Security Visibility dar. Diese umfasst eine zentrale Speicherung der Log-Daten für alle Security Events, ein Network Security Monitoring sowie eine laufende automatisierte Risikobewertung und Korrelationsanalyse, um selbst komplexe Angriffe erkennen zu können. Ziel ist es, die Zeit bis zur Erkennung von Bedrohungen wesentlich zu verkürzen und rasch mit geeigneten Gegenmaßnahmen zu antworten. Das individualisierte Kundenportal und ein laufendes Reporting für den Chief Information Security Officer und Geschäftsführung verschaffen dabei den nötigen Überblick. Die periodisch erstellten Security Reports beinhalten alle offenen und geschlossenen Security Incidents inklusive Status, Überblick über die aktuelle Bedrohungslage, aber auch Trends und Auffälligkeiten sind darin ablesbar.

> „ZIEL IST ES, DIE ZEIT BIS ZUR ERKENNUNG VON BEDROHUNGEN WESENTLICH ZU VERKÜRZEN UND RASCH MIT GEEIGNETEN GEGENMASSNAHMEN ZU ANTWORTEN."

Die Umsetzung erfolgte nach einem exakten Rollout-Plan. In mehreren Phasen wurde dieser für alle Konzerngesellschaften, beginnend in Österreich über Europa bis hin zu den weltweiten Niederlassungen, in rund zwölf Monaten umgesetzt. Um den Betrieb in den jeweiligen Niederlassungen auch vor Ort zu gewährleisten, wurden das zentralen Security Team trainiert und der Know-how-Aufbau von T-Systems laufend unterstützt. Unterstützung stellt T-Systems bei Betrieb und Analyse von Sicherheitsvorfällen bereit, wie auch bei der ständigen Weiterentwicklung der Use Cases als auch bei der Verbesserung der Angriffserkennung. ■

Foto: iStock

Die besten Zitate aus der IT-Welt

»Ich kenne mich auch nicht mit Technik aus, meine Kinder lachen mich deswegen sogar aus. Ich versichere Ihnen aber, dass selbst ich die Regeln der DSGVO umsetzen kann.«

VERA JOUROVÁ, EU-Kommissarin für Justiz, Verbraucherschutz und Gleichstellung, ist die Hüterin des europäischen Datenschutzes und hat seit 2014 an der DSGVO mitgearbeitet.

»Ohne emotionale Intelligenz bringt Künstliche Intelligenz nichts.«

Auch KI kommt ohne den Menschen nicht aus, findet DOROTHEE RITZ, General Managerin von Microsoft Österreich.

»Sensorik, Datensammeln, Schlussfolgerungen ziehen – mittlerweile geht das eben automatisch. Das ist nicht ›spooky‹ oder problematisch, sondern der Fortschritt der Technologie.«

FÜR WKO-PRÄSIDENT HARALD MAHRER ist das Thema Künstliche Intelligenz »nicht superneu«.

»Auch für heuer erwarten wir eine weitere Individualisierung von Angriffen. Angreifer haben längst erkannt, dass mit zielgerichteten Attacken wesentlich mehr zu holen ist.«

JOE PICHLMAYR, Geschäftsführer Ikarus Security Software GmbH, warnt vor neuen Strategien der Cyberkriminellen.

»Wir haben schon im Vorjahr festgestellt, dass es ein großes Orientierungsdilemma gibt.«

RICARDO-JOSÉ VYBIRAL, KSV1870-Chef, im April 2018, als sich unter Österreichs KMU sanfte Panik breit machte.

»Auch wenn wir ziemlich verwöhnt sind in Sachen Sicherheit – ein unverletzbares System gibt es nicht.«

GÜNTHER OFNER, Vorstandsdirektor der Flughafen Wien AG, ist sich der Gefahren eines möglichen Cyberangriffs bewusst.

»Durchschnittlich erleben wir drei Angriffe pro Minute auf unsere Server und müssen diese abwehren, um Datensicherheit und Datenschutz zu gewährleisten.«

In der öffentlichen Verwaltung hat Sicherheit oberste Priorität, wie BRZ-Geschäftsführer MARKUS KAISER beim Europäischen Forum Alpbach betonte.

»Wie bei anderen Deliktsarten kann bei Cybercrime nicht von der oder dem typischen Cyberkriminellen gesprochen werden.«

EDITH HUBER, Sozialwissenschafterin an der Donauuniversität Krems, identifizierte im Rahmen eines Forschungsprojekts drei Tätertypen: den Business-Man, die Hausfrau und den Perspektivlosen.

»Unser Bildungssystem muss da mithalten können. In Österreich tut es das nicht.«

Die digitale Transformation hapert an Grundsätzlichem, weiß GÜNTHER APFALTER, Präsident von Magna International Europe. Bei der Ausbildung der 230 Lehrlinge fängt man deshalb ganz von vorne an – mit Lesen und Schreiben.

»Wenn die Systeme sehr komplex sind, fühle ich mich ein bisschen wie Sherlock Holmes, der einen neuen Fall lösen muss.«

RAINER REHAK ist IT-Sicherheitsberater und Dozent an der HTW Berlin.

»Phishing-Mails waren früher vor allem aufgrund sprachlicher Unzulänglichkeiten relativ leicht zu erkennen. Das ist heute deutlich schwieriger.«

Auch Cyberkriminelle haben dazugelernt, beobachtet LEOPOLD LÖSCHL, Leiter des Cyber Crime Competence Center im Bundeskriminalamt.

»Der Status der IT-Sicherheit lässt sich gut mit dem Besuch beim Zahnarzt vergleichen, denn auch hier gilt: Vorbeugen ist besser als heilen.«

DAMIAN IZDEBSKI, CEO der techbold technology group, empfiehlt zum Schutz proaktives Monitoring und regelmäßige Wartung.

»Würden Sie einem Mann glauben, der vor dem Bankomat steht und sagt: ›Grüß' Sie, ich bin Ihr persönlicher Bankberater und erleichtere Ihnen die Arbeit – geben Sie mir Ihre Karte samt PIN Code‹? Ich glaube nicht. Gleiches gilt auch für das Internet.«

Prävention kann so einfach sein, findet MARTIN PUASCHITZ, Obmann der Fachgruppe UBIT Wien.

»Heute sind Unternehmen offensiver. Sie verstehen: Sicherheit ist kein Zustand, sondern ein Prozess, der schon das Anlagendesign betrifft.«

Die Security-Debatte werde nicht mehr angstgetrieben geführt, meint KURT HOFSTÄDTER, Leiter Digital Factory CEE bei Siemens.

»Der Markt ist leer geräumt. Universitäten und Fachhochschulen haben nicht genug Absolventen.«

Der Fachkräftemangel macht der Branche zu schaffen, bestätigt PETER GERDENITSCH, IT-Sicherheitschef der Raiffeisen Bank International.

»KI ist ein Werkzeug ohne eigenes Bewusstsein und ohne Ziel, das programmiert und mit Daten gefüttert wird. Und wir sind die Gestalter und Entscheider.«

VIKTORIA PAMMER-SCHINDLER, TU Graz, fordert mehr Selbstbewusstsein im Umgang mit Künstlicher Intelligenz.

»Der nächste Tsunami kommt bestimmt. Diesmal werden die Ursache nicht Kreditrisiken sein, sondern Risiken im Bereich Cyber-Sicherheit«,

warnte PETER HIEKANN vom FinTech-Unternehmen NDGIT, bei der Konferenz Banking & Technology vor Gefahren für die Bankenbranche.

»Die Blockchain erfindet die Datenstruktur im Hintergrund neu.«

Neue Technologien könnten die IT-Sicherheit erhöhen, meint SHERMIN VOSHMGIR, Direktorin des WU-Forschungsinstituts für Kryptoökonomie.

»Man muss auch bei seinem Auto regelmäßig das Service und Pickerl machen oder die Bremsen reparieren.«

ROBERT KOLMHOFER, Professor an der FH Hagenberg, wundert nicht, dass Cyberattacken so erfolgreich sind, denn viele Rechner laufen noch mit alten Betriebssystemen.

»Wir versagen dabei, sichere Systeme zu produzieren. Es ist unmöglich.«

MARTIN STIERLE, AIT Center for Digital Safety & Security, hält den »Krieg um die IT-Sicherheit« für verloren.

Foto: iStock

EINE SICHERSTELLUNG VON RAINER SIGL

Deppen-sicher

Sicher ist nicht sicher genug, vor allem in unsicheren Zeiten. Nur totale Sicherheit macht wirklich sicher.

> *Für die totale Datensicherheit muss man auch ein paar Opfer bringen.*

Zwei-Faktor-Authentifizierung, Biometrie, Verschlüsselung: Alles schön und gut, aber ich sag Ihnen, man kann heute nicht vorsichtig genug sein. Daten sind das neue Erdöl, was red ich, das neue Gold, und deshalb tu ich zumindest mein Möglichstes, um mich vor den Gefahren bestmöglich zu schützen. Ich mein: Chinesische Hacker! Russische Social-Engineering-Trolle! Nordkoreanische Malwareschleudern! Iranische Phishing-Experten! Scheidungsanwälte! Nigerinaische Email-Scammer! Simple Kriminelle! Und dann natürlich noch der Karli Hutterer vom Kinderturnverein, der 375 Eltern per Massenemail im CC anschreibt! Es ist ein Dschungel da draußen, und da gilt: Nur die Starken kommen durch – und da nur zwei Prozent, die Steine fressen.

Ich mein, wenn man überlegt, wie fahrlässig mit sensibelsten persönlichen Daten umgegangen wird – zum Beispiel im Altpapier! Was ich da neulich, beim, öhm, Recherchieren im Container wieder alles an Daten ausgegraben habe – Wahnsinn! Ich schmeiß da ja schon jahrelang nichts mehr hinein, nein, mein Lieber – mein sensibler Papiermüll wird zuerst von einem eigens dafür angestellten Sehbehinderten selektiv geschwärzt, dann geshreddert, dann in einem Spezialbad aus ungelöschtem Kalk und Chlorbleiche im Keller nachbehandelt – ja, okay, seit diesem kleinen Gasunfall letztes Jahr und nach der Kur trag ich jetzt eh immer diese Maske, ich hab meine Lektion gelernt – der Rest wird dann gefriergetrocknet und von Hand in einem Mörser zu feinstem Industriestaub gemahlen, mit Klärschlamm in Ziegelform gepresst und in einem eigens angemieteten Bunker endgelagert – weil mir das meine Datensicherheit wert ist!

> ES IST EIN DSCHUNGEL.

Oder am Telefon: Was da für Sicherheitslücken drohen! Nennen S' mich übervorsichtig, aber wenn mich eine unbekannte Nummer anruft, reiß ich sofort die SIM-Karte raus und desinfiziere sie für fünf Minuten bei 800 Watt in der Mikro! Mit mir nicht, ihr Verbrecher! Und nein, natürlich geb ich die Telefonnummern meiner Kontakte dann nicht jedes Mal neu ins Handy ein – da kann ich ja gleich meinen Körper testamentarisch diesen ganzen US-Datenkraken verschreiben! Natürlich merk ich's mir auswendig – und die wichtigsten Telefonnummern hab ich mir sowieso zur Sicherheit an einer geheimen Stelle eintätowieren lassen. Nein, ich zeig's Ihnen jetzt nicht. Und was soll das heißen, »wenn aber jemand an der Tür läutet«? Wenn die erst mal meine Adresse haben, muss ich sowieso schon im Flieger nach Belize sitzen!

Ich sag S' Ihnen ehrlich: Die Leute haben ja keine Ahnung, dass Ihnen da dauernd die ganze Welt an Leib und Daten will! Die tun so, als wär nix! Aufwachen! Denn wenn's eins gibt, was ich sicher weiß, dann das: Man kann nie sicher genug sein. Wie bitte? Ich, paranoid? Na wenn schon: Nur weil ich paranoid bin, heißt das noch lang nicht, dass keiner hinter mir her ist. ■

Foto: iStock

SCHUTZ VOR CYBER THREATS

In der digitalen Welt geht es nicht ohne IT Security. Verlassen Sie sich hierbei auf Spezialisten!
Mit T-Systems können Sie Ihr Unternehmen vor Cyber Threats optimal schützen. Wir betrachten das Thema „Sicherheit“ aus einer 360° Sicht - von vorbeugenden Lösungen bis zur Unterstützung im Angriffsfall.
So können wir eine individuelle Anpassung an die Bedürfnisse Ihres Unternehmen garantieren. Gemeinsam mit unseren 1500 internationalen Experten arbeiten wir an einem Ziel: WE SECURE BUSINESS!

Cyber Security by

T · · Systems ·

www.t-systems.at

CLOUD SECURITY NETWORK DIGITALIZATION