in|pact mediaverlag

OKTOBER **2020**

Auch als APP für Smartphones & Tablets

IT-SECURITY & CLOUD MANAGEMENT

Sicher, flexibel, skalierbar

»IT-SECURITY & CLOUD MANAGEMENT« ist eine unabhängige Publikation des in|pact media Verlags und erscheint als Beilage im Handelsblatt.

Liebe Leserin, lieber Leser,

ist Ihnen schon einmal aufgefallen, dass wir über die Digitalisierung oft so sprechen, als ob eine Naturgewalt über uns hereinbricht? Also etwas, auf das wir nur noch reagieren können, ohne wirklich noch die Option zu haben, es zu gestalten? Das mag eine nur allzu menschliche Reaktion sein, angesichts des enormen Veränderungspotenzials digitaler Technologien, die in den nächsten Jahrzehnten auf uns zukommen werden und die wir heute schon spüren.

Andererseits ist diese Haltung aber auch brandgefährlich. Denn sie macht uns träge und ignorant für die Gestaltungsmöglichkeiten, die wir dennoch haben. Wie jede industrielle Revolution vor ihr ist auch die sogenannte vierte, digitale ein Werk von Menschen. Und als solches sehr wohl zu regulieren und in unserem Sinne zu beeinflussen und zu lenken.

Sehr gute Beispiele hierfür finden wir in den Bereichen IT-Sicherheit und Cloud-Technologien, denen wir uns in diesem Heft widmen. GAIA-X, die sogenannte Europa-Cloud, hat nämlich genau dieses Ziel: uns Gestaltungsmöglichkeiten zurückzugeben, derer wir uns bislang viel zu wenig bewusst waren. Als eine nach europäischen Werten und Maßstäben designte Datenplattform soll sie uns das zurückgeben und für die Zukunft bewahren, was wir in unserer zunehmenden Abhängigkeit von US-amerikanischen Firmen verloren hatten: die Kontrolle über unsere Daten. Wie genau das funktionieren soll und was es mit dem gerade so häufig zitierten Begriff der Digitalen Souveränität auf sich hat, darüber haben wir mit den beiden Open-Source-Experten Peter Ganten und Kurt Garloff gesprochen, die mit einem eigenen Projekt an GAIA-X mitwirken (S. 3).

Dass uns im Zuge einer immer größeren Vernetzung auch das Thema Cybersicherheit immer stärker beschäftigen wird, ist ebenso klar. Unsere Autoren Lars Klassen und Axel Novak haben die neuesten Trends und Entwicklungen für Sie zusammengefasst (S. 4-8).

Viel Spaß beim Lesen!

Ihre Redaktion

INHALT

HINWEIS: Alle nicht mit dem Zusatz »Redaktion« gekennzeichneten Beiträge sind Auftragspublikationen und somit Anzeigen.

IMPRESSUM

in|pact mediaverlag

European Newspaper AWARD Preisträger

in|pact media GmbH
Dircksenstraße 40
D-10178 Berlin

T +49 (0) 30 802086 -530
F +49 (0) 30 802086 -539
E redaktion@inpactmedia.com
www.inpactmedia.com

HERAUSGEBER
Edi Karayusuf (V.i.S.d.P)

REDAKTEUR
Klaus Lüber

PROJEKTLEITUNG
Konstantinos Tsavalos

PROJEKTASSISTENZ
Carola Rothe
Michael Stoephasius

ART DIREKTION/LAYOUT
Denis Held

ILLUSTRATIONEN
Mario Parra
www.oq.design

LEKTORAT
Gina Wittlich

AUTOREN
Lars Klaaßen, Klaus Lüber, Axel Novak, Julia Thiem

DRUCK
BVZ Berliner Zeitungsdruck GmbH

CHEFREDAKTION
Mirko Heinemann
Klaus Lüber (stellv.)

GESCHÄFTSFÜHRUNG
Sara Karayusuf-Isfahani
Edi Karayusuf

Die Europa-Cloud

Um die Zukunftsfähigkeit der deutschen Wirtschaft zu erhalten, ist es zwingend notwendig, die Kontrolle über die Datenströme der digitalen Transformation zu behalten. Ein Gespräch mit den Open-Source-Experten Peter Ganten und Kurt Garloff.

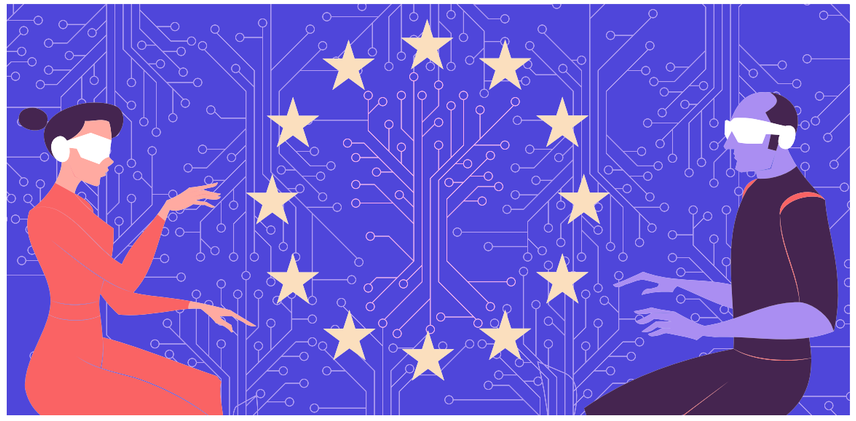
Interview: Klaus Lüber / Redaktion

Herr Garloff, Herr Ganten, denkt man in Deutschland über die Chancen und Risiken der Digitalisierung nach, ist ein gewisser Alarmismus spürbar. Andere Länder, vor allem die USA und China, so heißt es, würden uns mit ihren Technologien überrollen. Deshalb brauchen wir dringend eigene Lösungen. Sehen Sie das auch so?

Ganten: Man muss einfach feststellen, dass in Zukunft so gut wie jede Industrie, jedes Geschäft eine digitale Komponente hat und über digitale Plattformen abgewickelt wird. Ohne diese Plattformen und den Zugriff auf die Daten, die sie verwalten und analysieren, sind im Grunde strategische Entscheidungen und Innovationen gar nicht mehr möglich. Und genau an dieser Stelle sind wir in Deutschland und Europa tatsächlich in eine gefährliche Abhängigkeit vor allem von US-amerikanischen Anbietern gekommen.

Sie meinen von den großen Cloud-Service-Providern wie Amazon, Microsoft oder Google?

Ganten: Ganz genau. Und die Lage ist meiner Meinung nach wirklich ernst. Denn was bedeutet das denn eigentlich für Unternehmen, sagen wir aus der Automobilindustrie? Die würden in



Zukunft völlig der Fähigkeit beraubt, überhaupt noch ganze Produktpakete anbieten zu können. Die würden, etwas drastisch formuliert, am Ende nur noch Bleche formen und irgendwann sähe unsere gesamte mittelständische Wirtschaft aus wie McDonalds- oder Subway-Filialen. Die Unternehmen sind auf dem Papier zwar noch eigenständig, aber alles, was sie verkaufen, kommt irgendwie aus einer US-amerikanischen oder chinesischen Cloud.

Warum entwickeln wir keine eigene, europäische Cloud?

Garloff: Genau das ist ja das Ziel des europäischen Projekts GAIA-X. Nämlich ein IT-Ökosystem zu schaffen, das es ermöglicht, Daten kontrolliert weiterzugeben und zu nutzen, ohne den US-amerikanischen oder chinesischen Weg zu gehen. Also ohne Privatunternehmen oder dem Staat das Recht einzuräumen, Daten nach Belieben auszubeuten. Sondern eine Plattform zu bauen, auf der eine Vielzahl hochprofessioneller Cloud-Dienste angeboten werden können und dabei allen unseren hohen europäischen und deutschen Standards im Bereich Datensicherheit und Datenschutz genügen. Letztlich geht es um digitale Souveränität.

Das würde doch bedeuten, dass man als Nutzer auch vollen Zugriff auf den Programmcode solcher Systeme benötigte, oder?

Garloff: Und genau deswegen wird GAIA-X auch mit Open-Source-Technologie entwickelt. Nur wenn Sie genau nachvollziehen können, wie bestimmte Dienste funktionieren, haben Sie die volle Kontrolle darüber, was mit Ihren Daten passiert. Ganz abgesehen davon können Sie die Dienste viel genauer an Ihren bestimmten Bedarfsfall anpassen und bei Problemen auch viel schneller reagieren.

Und das kann funktionieren? Hat nicht Open-Source-Software nach wie vor das Problem, mit proprietären Produkten nur mäßig mithalten zu können?

Garloff: Das mag für den Consumer-Bereich vielleicht noch vereinzelt gelten. Und natürlich gibt es auch Open-Source-Projekte, die qualitativ schlecht sind und trotzdem noch viel zu lange weiterentwickelt werden. Aber das ist nicht die Masse.

Ganten: Was wir beobachten können, ist gewissermaßen ein Wachstum von unten nach oben. Das Internet läuft komplett mit Open-Source-Technologie, nämlich Linux, ebenso Datenbanken und Web-Frameworks. Und eigentlich ist auch bei Betriebssystemen, wenn man die mobilen Android-Geräte mitzählt, Open Source im Kampf gegen Windows – dem einzig verbliebenen Player mit einem proprietären Produkt – als Sieger hervorgegangen.

Aber eben noch nicht bei den großen Cloud-Anbietern.

Ganten: Wobei diese ja alle überhaupt erst durch den Einsatz von Open-Source-Technologie so erfolgreich werden konnten. Das beruht alles auf Open-Source-Software.

Warum sind wir nicht längst denselben Weg gegangen?

Garloff: Eine berechtigte Frage. Ich glaube, die Open Source Community hat lange nicht verstanden, dass der Wettstreit um Cloud-Angebote ein Wettstreit um Plattformen ist. Für den hochfragmentierten Markt für Open-Source-Cloud-Lösungen bedeutet das: Man kann mittel- und langfristig nur dann gegen große Player bestehen, wenn man Kräfte bündelt. Und genau daran arbeiten wir mit unserem Projekt Sovereign Cloud Stack.

Ist das ein Teil von GAIA-X?

Garloff: Inzwischen ja. Sovereign Cloud Stack soll eine einheitliche, standardisierte Infrastruktur für das Datenökosystem von GAIA-X aufbauen. Dann hätten wir genau den Netzwerkeffekt, den wir brauchen – mit zahllosen kleinen und mittelgroßen Cloud-Anbietern, die offen und einsehbar zusammenarbeiten und zueinander kompatible Lösungen entwickeln und anbieten.

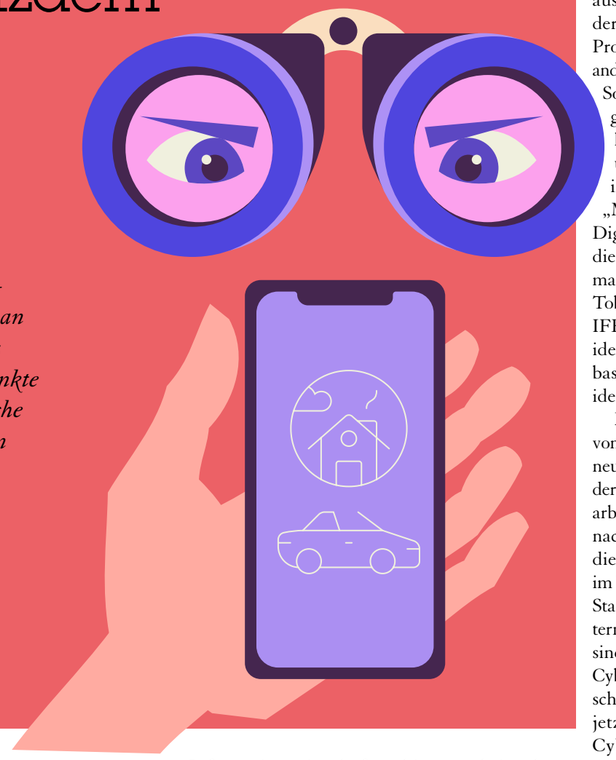
Das Projekt wird inzwischen auch gefördert von der kürzlich gegründeten Agentur für Sprunginnovationen. Dabei gehe es auch, so Leiter Rafael Laguna de la Vera, um nichts Geringeres als die Verteidigung europäisch-humanistischer Werte.

Ganten: Eine Haltung, die ich voll und ganz unterschreibe. Wenn sowohl große US-Tech-Firmen als auch der chinesische Staat der Meinung sind, Technologie würde die Bedürfnisse von Menschen besser kennen als sie selbst, müssen wir erstens damit nicht einverstanden sein. Und zweitens dafür kämpfen, auch in Zukunft die Freiheit zu haben, zwischen verschiedenen Optionen zu wählen.

PETER GANTEN
ist Gründer und CEO der Univention GmbH sowie seit 2011 Vorsitzender der Open Source Business Alliance.

KURT GARLOFF
ist IT-Berater und Open-Source-Experte und hat erfolgreich bei der SUSE und T-Systems offene Betriebssystem- und Cloudentwicklung geleitet. Er ist Leiter des Projektes Sovereign Cloud Stack (SCS).

Hochkomplex – und trotzdem sicher?



5G-Netzwerke ermöglichen ein neues Level an Interkonnektivität, das öffnet neue Angriffspunkte für Kriminelle. Kritische Infrastrukturen müssen deshalb besonders gut geschützt werden.

Lars Klaaßen / Redaktion

5G-Netze können große Datenmengen zuverlässig übertragen. Der neue Standard wird damit zu einer digitalen Schlüsseltechnologie im Zeitalter der Vernetzung. Das eröffnet einerseits völlig neue Möglichkeiten: Industrie 4.0, Telemedizin, automatisiertes und vernetztes Fahren, Smart Buildings. „5G ist ein zentraler Hebel für die digitale Transformation in Wirtschaft und Gesellschaft, der ökonomische, ökologische und soziale Entwicklungssprünge ermöglicht", wie die Bundesregierung betont. Doch die Vernetzung birgt auch Risiken, kann Kriminellen Einfallstore für Angriffe öffnen. Deshalb steht beim nächsten großen Schritt der Digitalisierung die Cybersicherheit ganz oben auf der Agenda.

„Die Mehrheit der innovativen deutschen Unternehmen in der Informationswirtschaft und im verarbeitenden Gewerbe sieht einen hohen Schutzbedarf ihrer IT für Innovationstätigkeiten", so Uwe Cantner, Vorsitzender der Expertenkommission Forschung und Innovation (EFI), die Bundeskanzlerin Angela Merkel Anfang des Jahres ein Jahresgutachten zu diesem Thema übergeben hat. „Über die Hälfte dieser innovativen Unternehmen geht davon aus, dass die Gefahr durch Cyberangriffe auf ihr Unternehmen in den kommenden Jahren weiter zunehmen wird." Die Expertenkommission ließ untersuchen, ob sich die Bedrohung durch Cyberangriffe auf die Innovationsaktivitäten der Unternehmen auswirkt: Eine im Auftrag der EFI durchgeführte repräsentative Umfrage bei Unternehmen in der Informationswirtschaft und im verarbeitenden Gewerbe im dritten Quartal 2019 zeigt zwar, dass 64 Prozent der Unternehmen keine Beeinflussung ihrer Innovationsprojekte durch die Gefahr eines Cyberangriffs sehen. Bei immerhin rund 30 Prozent der Unternehmen verzögern sich deshalb jedoch existierende Innovationsprojekte, werden geplante (bei rund 17 Prozent) gar nicht begonnen oder auf neue (rund 12,5 Prozent) sogar ganz verzichtet.

Wie man Sicherheit auch für große, komplexe Strukturen gewährleistet, machen Forscherinnen und Forscher des Fraunhofer-Instituts für Fabrikbetrieb und -automatisierung IFF gemeinsam mit Industriepartnern in den Häfen von Magdeburg und Wilhelmshaven vor. Häfen zählen zu den kritischen Infrastrukturen, da Störungen und Ausfälle immense, nicht nur volkswirtschaftliche Auswirkungen haben können. Dabei sind die möglichen Sicherheitsrisiken vielfältig, insbesondere in digitalisierten Containerterminal-Prozessen, die durch Industrie 4.0 immer mehr an Bedeutung gewinnen. Die Akteure aus Wissenschaft und Wirtschaft haben ein neues Methoden- und Werkzeugset entwickelt, das die präventive Abwehr von Angriffen auf automatisierte cyberphysische Systeme ermöglicht und hilft, die Sicherheit entlang der gesamten Logistikkette inklusive der IT-Systemlandschaft zu erhöhen.

Cyberphysische Systeme – das können auch Gabelstapler oder Kräne sein – sind hochkomplex: Software interagiert mit mechanischen wie elektronischen Teilen und ist damit Risiken wie Hackerangriffen oder physischer Manipulation ausgesetzt. Die Forscher suchen einen Ansatz, der es einerseits erlaubt, auftretende Fehler oder Probleme automatisiert schnell zu erkennen, und andererseits das System weniger anfällig zu machen: So soll nicht ein gesamtes System, sondern nur gestörte Teilkomponenten abgeschaltet werden können. Sind Fehlerursachen schnell ermittelt und behoben, ist ebenso schnell die Wiederinbetriebnahme des Gesamtsystems möglich. „Mithilfe von Simulationen bauen wir einen Digitalen Zwilling des Hafens auf und gleichen die Prozesse der realen Hafeninfrastruktur permanent mit dem Digitalen Zwilling ab", erläutert Tobias Kutzler, Wissenschaftler am Fraunhofer IFF in Magdeburg. „Verhalten sich beide nicht identisch, liegt ein Problem vor." Der Abgleich basiert dann auf einem Drei-Stufen-Konzept: identifizieren, lokalisieren, beheben.

Mit der Corona-Pandemie hat die Sicherheit von IT-Strukturen auch in den meisten Büros eine neue Dringlichkeit – genauer: in den Homeoffices der Mitarbeiter, die auch langfristig häufiger extern arbeiten als bis vor kurzem. „Die neue Normalität nach Covid-19 ist für die Unternehmensleitung, die Mitarbeiter und die IT-Security-Abteilung im Besonderen eine Herausforderung", sagt Palo Stacho, Mitgründer von Lucy Security, einem Unternehmen im Bereich IT-Sicherheit. „Die Firmen sind mit der Tatsache konfrontiert, dass sich der Cyberraum aufgrund von Homeoffice massiv und schlagartig erweitert hat." Unternehmen bieten jetzt also eine noch größere Angriffsfläche für Cyberkriminelle. 75 Prozent der IT-Security-Anbieter vermelden laut DA Davidson Security Software Report aus dem ersten Quartal dieses Jahres massiv mehr Phishing-Angriffe seit Ausbruch der Corona-Pandemie.

Ob Zuhause oder im Büro: Durch Smart Buildings wird das Thema IT-Sicherheit künftig an fast jedem Ort relevant sein. Am Deutschen Forschungszentrum für Künstliche Intelligenz arbeitet der Forschungsbereich „Agenten und simulierte Realität" an Lösungsansätzen, wie sich mithilfe von künstlicher Intelligenz und maschinellem Lernen Rohdaten noch innerhalb eines smarten Gebäudes intelligent kombinieren und abstrahieren lassen, sodass die erforderlichen Informationen verfügbar, weitergehende Rückschlüsse jedoch nicht mehr möglich sind. Fragt also ein Energieanbieter Informationen über den Wärmeverbrauch eines smarten Gebäudes ab, sollte nicht minutiös mitgeteilt werden, wie hoch die Temperatur jedes einzelnen Zimmers in den vergangenen Monaten war. Es reicht, wenn die Information gegeben wird, dass sich aufgrund des erwarteten Nutzungsverhaltens der Wärmebedarf etwa in den kommenden vier Stunden mit einer Wahrscheinlichkeit von 80 Prozent um 20 Prozent verringern wird. Voraussetzung für solche Aussagen und den Einsatz von künstlicher Intelligenz ist die leichte Vernetzbarkeit und Interoperabilität der beteiligten Dienste, Systeme und Geräte. Eben jene Technologie, die Risiken mit sich bringt, sichert uns vor diesen auch wieder ab.

»Das Thema IT-Sicherheit wird künftig an fast jedem Ort relevant sein.«

— Beitrag Q_PERIOR —

»Die kleinste digitale Komponente wird zum Einfallstor«

IT- und Informationssicherheit sind in aller Munde, möchte man meinen. Doch die führende Business- und IT-Beratung Q_PERIOR sieht beim Thema Cyber Security noch immensen Nachholbedarf.

Herr Wöhler, „smart" und „connected" sind zwei Begriffe, die uns überall begegnen – sei es bei Produkten, die wir hierzulande produzieren, oder auch bei Maschinen, mit denen produziert wird. Wie angreifbar macht sich die deutsche Wirtschaft mit einer zunehmenden Vernetzung?

Die Gefahren, die mit der zunehmenden Digitalisierung und Vernetzung unserer Wirtschaft einhergehen, sind tatsächlich nicht zu unterschätzen. Diese Diskussion führen wir ja jetzt beispielsweise auch immer wieder im Zusammenhang mit den coronabedingt aus dem Homeoffice arbeitenden Belegschaften – beispielsweise die Frage, wie sicher die genutzte Videokonferenzsoftware eigentlich ist, ob sie unseren Ansprüchen an den Datenschutz genügt oder wie anfällig Mitarbeiter für Social-Engineering-Attacken sind. Gefährlich ist Vernetzung aber auch dann, wenn kleinste, digitale Komponenten, die vielleicht von einem Zulieferer kommen, zum Einfallstor für Cyberkriminalität werden. Hier kann mein Kollege Dr. Brandt sicher das ein oder andere Beispiel aus dem Automotive-Sektor nennen, wo Vernetzung und smarte Fahrzeuge eine immer größere Rolle spielen.

Herr Dr. Brandt, sind vernetzte, smarte Autos also gar nicht erstrebenswert?

Wer einmal den Komfort eines vernetzten Fahrzeugs erleben durfte – von der Adresseingabe per Sprachbefehl bis zur Navigation mit Echtzeitverkehr – hat diese Frage längst für sich beantwortet. Allerdings öffnet ein immer größerer Softwareanteil tatsächlich Einfallstore, wie der Kollege richtig sagt. Interessant ist in diesem Zusammenhang, dass sie gar keinen großen technologischen Fortschritt brauchen, um ein Auto angreifbar zu machen. Es reicht ein vermeintlich simples Element wie der Regensensor, der durch Manipulation der Software theoretisch Informationen bis aus der zentralen Steuerung des Fahrzeugs ziehen könnte. Denkbar wäre somit ein Missbrauch in Richtung Datendiebstahl und damit verbunden die Auswertung des Fahrverhaltens der Nutzer oder ihrer Wegstrecken. Am Beispiel des Automobils wird deutlich, dass Cyber Security einen höheren Stellenwert in der Industrie einnehmen muss. Cyber Security muss fester Bestandteil bestehender Geschäftsprozesse werden.

Nun sind Cyberangriffe keine Seltenheit. Immer wieder geraten Unternehmen ins Visier, es kommt zu Reputationsschäden. Warum ist die Industrie in diesem so wichtigen Bereich noch nicht weiter, Herr Davignon?

Das kann man so pauschal nicht sagen. Es gibt zahlreiche Unternehmen, die IT- und Informationssicherheit sehr ernst nehmen und hier auch schon sehr weit sind. Insgesamt haben sie jedoch Recht, dass es Nachholbedarf gibt, vor allem, weil Cyber Security kein Ziel ist, das einmal erreicht werden kann. Es ist ein kontinuierlicher Prozess, der damit in erster Linie auch kontinuierlich Kosten verursacht. Und genau hier liegt aus unserer Sicht auch das größte Problem: Cyber Security ist eben kein Business Case. Und einen reinen Kostentreiber tut man dann schon mal leichtfertig mit der Hoffnung ab, dass es ja nur den anderen passiert.

Wobei doch spätestens bei einem Vorfall die Kosten-Nutzen-Abwägung zugunsten der Cyber Security ausfallen sollte, oder, Herr Wöhler?

Auch das ist ein wichtiger Punkt: Solange die Cyber Security in einem Unternehmen noch nicht den Stellenwert hat, sehen Sie als Verantwortlicher nicht, wie viele Angriffe tatsächlich auf Ihre Systeme, Ihre Maschinen oder Ihr Netzwerk gefahren werden. Viele Angriffe bleiben nämlich unentdeckt. Ist ein umfangreiches Cyber-Security-Management-System jedoch erst einmal etabliert, verändert sich auch die Kosten-Nutzen-Abwägung, wie Sie richtig sagen. Bis dahin gilt es an vielen Stellen jedoch, Überzeugungsarbeit zu leisten.

DR. THIEMO BRANDT
Lead Automotive
Q_PERIOR

JÖRG WÖHLER
Lead IT Security
Q_PERIOR

BERNHARD DAVIGNON
Lead Technologie & Innovation
Q_PERIOR

Warum glauben Sie, ist noch so viel Überzeugungsarbeit nötig?

Weil Technik und Software für viele Unternehmen ein ganz neues Geschäftsfeld sind. Wenn ich ein Unternehmen zur Herstellung von Gartengeräten leite, weiß ich genau, wo meine Risiken sind oder welche Fehler in der Produktion passieren können. Werden in meine Rasenmäher nun beispielsweise aber Sensoren eines Zulieferers – und somit Fremdsoftware – eingebaut, kommen neue Risiken hinzu, die mir nicht bewusst sind oder die ich vielleicht gar nicht bewerten kann. Wir müssen also an vielen Stellen erst einmal ein neues Bewusstsein für diese branchenfremden Risiken schaffen, die mit der Digitalisierung einhergehen.

Muss vielleicht die Politik der Cyber-Sicherheit stärker unter die Arme greifen, Herr Davignon?

Wir vergleichen IT- und Informationssicherheit gerne mit dem Sicherheitsgurt im Auto. Keiner zweifelt seinen Mehrwert an, dennoch werden immer wieder Autofahrer angehalten und bekommen ein Bußgeld, weil der Gurt eben nicht angelegt ist. Das wäre natürlich auch ein gangbarer Weg, die deutsche Wirtschaft insgesamt vor der zunehmenden Cyberkriminalität zu schützen – vor allem in jenen Branchen, die keinen Software-geprägten Ursprung haben. Das zeigt sich ja beispielsweise im Automotive-Sektor, wo die UN mit dem ECE ein Gremium ins Leben gerufen hat, dessen Aufgabe es ist, einheitliche technische Kriterien für Kraftfahrzeuge zu entwickeln.

Herr Dr. Brandt, brauchen Autos tatsächlich zukünftig einen Digital-TÜV?

Jeder moderne Mittelklassewagen ist schon heute ein kleines Rechenzentrum auf vier Rädern. Ihre Vertragswerkstatt kann genau auslesen, wie oft Sie den Kofferraum öffnen, welche Durchschnittsgeschwindigkeit Sie fahren und viele andere Nutzerdaten. Das vernetzte Fahrzeug von morgen bietet unzählige Angriffsszenarien und Einfallstore für gezielte Manipulation und Datendiebstahl. Ich halte es daher für sinnvoll, dass hier mit neuen Richtlinien Maßstäbe und Standards für die Industrie gesetzt werden. Denn die Branche wandelt sich, von einem reinen Hardware- hin zu einem Software-Anbieter. Und wenn Software zum neuralgischen Punkt wird, muss die Sicherheit in der Entwicklung klar priorisiert werden.

Haben wir denn die nötigen IT-Ressourcen, um diesen Herausforderungen gerecht zu werden, Herr Davignon?

Die Kapazitäten sind erschöpft. Der Beratung sowie der Bereitstellung von Cyber Security Teams – die temporär Projekte für verschiedene Unternehmen umsetzen – kommen daher eine zentrale Bedeutung zu. Langfristig müssen Unternehmen, Wirtschaft und Staat in den Ausbau von IT-Ressourcen investieren.

www.q-perior.com

Geld und Daten

Cybercrime-Vorfälle nehmen zu, auch Dank des Digitalisierungsbooms während der Pandemie. Was sind die neusten Tricks der Hacker? Und wie können sich Unternehmen schützen?

Axel Novak / Redaktion

Es war der erste Todesfall nach einem Hacker-Angriff: Weil eine lebensbedrohlich erkrankte Patientin statt ins Universitätsklinikum Düsseldorf ins weiter entfernte Krankenhaus in Wuppertal eingeliefert werden musste, konnte sie erst verspätet behandelt werden und starb kurze Zeit später. Der Grund für die Verlegung: Hacker hatten im Juli das IT-System des Klinikums blockiert, um Lösegeld zu erpressen. Patienten konnten nicht behandelt werden.

Dabei kam der Angriff nicht unvermutet: „Bereits im Januar haben wir vor der Schwachstelle gewarnt und darauf hingewiesen, welche Folgen eine Ausnutzung haben kann", sagt Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik. „Ich kann nur mit Nachdruck appellieren, solche Warnungen nicht zu ignorieren oder aufzuschieben, sondern sofort entsprechende Maßnahmen zu ergreifen."

Der Tod der Patientin ist das tragische Ergebnis eines Phänomens, das immer stärker um sich greift. Unternehmen werden von Cyberkriminellen erpresst. Gerade die rasant erfolgte Digitalisierung im Verlauf der Corona-Pandemie hilft Hackern, schneller und erfolgreicher anzugreifen. Veränderte Prozesse und Geschäftsabläufe im Homeoffice oder beim Remote Working, das Abweichen von etablierten Workflows und fehlende oder unregelmäßigere Kontrollen bieten einen idealen Nährboden für Betrug. „Bei PhishingMails, betrügerischen Webseiten, Fake-President-Angriffen, Kredit und Subventionsbetrug sowie dem Einsatz von Finanzagenten ist seit März 2020 eine starke Zunahme zu verzeichnen", heißt es in einem Bericht der Unternehmensberater von KPMG zur Wirtschaftskriminalität. Mit „Fake-President-Angriffen" geben sich externe Angreifer als Vorgesetzte aus und versuchen, Überweisungen von größeren Beträgen ins Ausland zu veranlassen.

ENORME KOSTEN FÜR DIE UNTERNEHMEN

Insgesamt wurden im vergangenen Jahr fast 770.000 Nutzer durch Verschlüsselungs-Software angegriffen, so der Security-Spezialist Kaspersky – ein Fünftel davon mit dem Trojaner WannaCry: Der führte schon vor drei Jahren zu enormen Schäden bei Nissan, Telefónica und der Deutschen Bahn. Auch heute noch ist WannaCry das meistgenutzte Erpressertool.

Im Schnitt verzeichnet jedes Unternehmen heute 145 Sicherheitsvorfälle und Datenverluste pro Jahr – das ist ein Plus von elf Prozent gegenüber dem Vorjahr. Auch die Kosten, die mit Cyberangriffen verbunden sind, steigen auf 13 Millionen US-Dollar, beziffert eine Accenture-Studie die Kosten von Cybercrime. Demnach könnten die direkten und indirekten Gesamtkosten solcher Cyberattacken weltweit bis zum Jahr 2030 auf zehn Billionen US-Dollar steigen.

Den Kriminellen geht es um zwei Dinge: Geld und Daten. Dafür tricksen sie ihre Opfer raffiniert aus. In E-Mails schleichen sie sich emotional und privat an ihre Opfer an – Love Scams heißt das – oder imitieren die Hausbank, PayPal oder Amazon, um an Zugangsdaten zu gelangen. Wer Pech hat, zahlt dann nicht nur viel Geld, sondern kompromittiert seine Bank- oder Kreditkartendaten und lädt sich gleich noch eine Malware herunter, die weitere Informationen abgreift.

DIE SCHATTEN-IT DER FIRMEN WÄCHST

Das bedeutet für Unternehmen ein immenses Risiko: Viele mussten in den vergangenen Monaten heftig improvisieren. Hastig zusammengefügte Softwaretools und improvisierte Zugänge ins Firmen-Intranet sorgten für eine Schatten-IT, die die IT-Abteilungen im Unternehmen nicht mehr administrieren und kontrollieren konnten. Hinzu kommt die zunehmend private Nutzung von betrieblichen und die geschäftliche Nutzung von privaten Geräten. Mitarbeiter stellen Handy, Rechner und Tablet offensichtlich auch anderen Familienmitgliedern zur Verfügung. Die Nutzung unsicherer Apps und Websites stieg im vergangenen Halbjahr um 161 Prozent, die von Websites mit nicht jugendfreien Inhalten um 600 Prozent, haben Cloud-Security-Spezialisten von Netskope festgestellt.

Für die Arbeitgeber heißt das: Sicherheitslecks in Software, die niemand richtig kontrolliert, kann niemand effektiv abdichten. Hacker können sich geradezu eingeladen fühlen, auf Server, Anlagen und Maschinen zuzugreifen.

Hauptangriffspunkt der Hacker sind Mailserver. Das ist nachvollziehbar, denn Geschäftsverkehr und unternehmensinterne Prozesse laufen stark über E-Mails ab, auf den Servern befinden sich viele hochattraktive Informationen. Doch über die Zugangsdaten der Mitarbeiter können Hacker auch Zugriff auf die OT (Operational Technology) von Anlagen und Maschinen erlangen. Mit entsprechend hohem Risiko für Kraftwerke, Wasserversorger oder Krankenhäuser.

UNSICHERE CLOUD-DIENSTE

Hacker setzen eine ganze Palette an Werkzeugen ein. Im Darknet boomt derzeit Malware aller Art: Programme, die geeignet sind, Facebook- oder Google-Chrome-Dienste zu knacken, sind derzeit besonders günstig, berichtet der US-amerikanische Cybersicherheitsanbieter *Fortsetzung auf Seite 8* ►►

— Beitrag ALSO —

ALSO Security Circle

Ihr Weg zur sicheren IT

In den vergangenen Jahren haben Cybersecurity-Attacken auf Unternehmen, Institutionen oder Entscheidungsträger in der Wirtschaft immer wieder verdeutlicht, wie wichtig die Absicherung von Infrastruktur und Daten ist.

Dabei sind Mobilität und die Nutzung von Cloud-Diensten heute entscheidende Faktoren für die Effizienz und Skalierbarkeit von Unternehmen. Ohne zuverlässige und leistungsfähige Kommunikation kann, unabhängig von Branche oder Größe, kein Geschäftsbetrieb aufrechterhalten werden. Gerade die Ereignisse rund um die Pandemie zeigen, wie sehr wir durch IT vernetzt sind und sein müssen – im Unternehmen, wie im Homeoffice.

Durch die Komplexität der IT-Infrastrukturen und neue Arbeitsweisen wird es jedoch immer schwieriger, die Sicherheit der eigenen Daten zu bewerten.

Mit unserem ALSO Security Circle möchten wir Ihnen einen Überblick darüber geben, welche Themen innerhalb von IT-Infrastrukturen betrachtet werden müssen, um den Geschäftsbetrieb dauerhaft sicher aufrechtzuerhalten.

Gerne beraten wir Sie gemeinsam mit unseren IT-Systemhaus-Partnern, wenn es um Security-Themen wie Data, Endpoint oder Network geht. Mit Hilfe des Security Circles haben Sie die gesamte Sicherheit der IT Ihres Unternehmens im Blick. Und mit unserem Netzwerk an Händlern auch die Profis vor Ort, um genau die richtigen Lösungen zu implementieren. Darüber hinaus helfen sie mit Schulungen das Bewusstsein für IT-Sicherheit bei den Anwendern zu schärfen.

Besuchen Sie uns online unter **www.also.de/itsecurity** um mehr Informationen zum ALSO Security Circle, dem ausführlichen Interview zum Thema Security Awareness und der Kaspersky-Lösung sowie Sophos' Managed Threat Response zu erhalten.

ALSO SPOTLIGHT, die virtuelle Veranstaltung zum Thema Cybersecurity und Cloud am 29. Oktober 2020, bietet Ihnen die Möglichkeit, sich unverbindlich in Experten-Talks und Webinaren einen direkten Eindruck über die Leistungen und Angebote der ALSO und ihren Partnern zu informieren. Die Teilnahme ist kostenlos. Einen Überblick über die Veranstaltung und Themen erhalten Sie hier:

www.also.de/spotlight

— Beitrag KASPERSKY —

IT-Security Awareness

Ein Interview mit dem Experten Mike Ritter vom Cybersicherheitsunternehmen Kaspersky

Wie viel ist das IT-Security Investment wert, wenn Mitarbeiter das schwächste Glied der Sicherheitskette sind?

So gut Security-Konzepte und die dazugehörigen Maßnahmen um Firewall und Co. auch sein mögen, moderne Cyberangriffe umgehen diese geschickt, indem sie direkt auf einzelne Personen im Unternehmen abzielen. Die Tarnung ist so perfekt, dass Angriffe gar nicht erkannt werden. Die Konsequenzen können gravierend sein.

Mike Ritter, Channel Sales Manager bei Kaspersky, ist Security Awareness-Verfechter und weiß, warum die Sensibilisierung einer Belegschaft in puncto IT-Security so wichtig ist – und vor allem, wie man sie nachhaltig und ganz ohne Präsenzveranstaltungen umsetzt.

MIKE RITTER
Channel Sales Manager, Kaspersky

Herr Ritter, wo liegt der Knackpunkt bei Security Awareness?

Kaspersky ist immer am Puls der Bedrohung und kennt die Probleme von Unternehmen genau. Was uns dabei immer wieder auffällt: Der Wissensstand hinsichtlich moderner Bedrohungsszenarien und Risiken muss dringend ausgebaut werden.

Wieso ist die „Schwachstelle Mensch" noch immer ein Thema?

Wahrnehmen und ernst nehmen sind leider zwei verschiedene Paar Schuhe. Die Motivation, sich Security Awareness zu widmen, weicht ziemlich schnell, sobald es um die Umsetzung geht.

Bedeutet die Integration entsprechender Maßnahmen denn so viel Aufwand?

Tatsächlich könnte der Aufwand mit Lösungen wie der virtuellen Kaspersky Automated Security Awareness Platform kaum geringer sein. Die Cloud-gehostete Plattform bietet MitarbeiterInnen einen individuellen Lehrplan zu aktuellen Bedrohungen in Form von Mikrokursen. In wenigen Minuten pro Woche minimieren Unternehmen die Risiken effektiv und nachhaltig – auch von zuhause aus.

www.also.de/kaspersky

Sicherheitsrisiko Homeoffice

Sie arbeiten im Homeoffice? Wenn Sie ein paar einfache Verhaltensweisen beachten, sind Sie am Arbeitsplatz zuhause genauso geschützt wie im Büro.

1. **Nehmen Sie nur die Geräte und Informationen mit nach Hause, die sie wirklich benötigen. So verhindern Sie, dass Geräte oder Daten auf dem Weg oder im Homeoffice abhanden kommen.**
2. **Egal, wie sicher die Verbindungen im Büro sind, Ihr Heimnetzwerk macht Sie angreifbar. Deshalb sollten Sie das private Netzwerk entsprechend sichern. Dazu gehören natürlich eine starke WLAN-Verschlüsselung, ein individuelles und komplexes Passwort sowie regelmäßige Softwareupdates.**
3. **Sie arbeiten im Homeoffice vermutlich mit dienstlichen und privaten Geräten in einem Netzwerk. Ihr Datenverkehr läuft über einen Router, an den Sie und Ihre Familie viele weitere Devices angeschlossen haben. Achten Sie deshalb darauf, dass alle Geräte am Router die neueste Software haben. Durch automatische Updates schließen Sie potenzielle Einfallstore für Hacker.**
4. **Müssen Sie sensible Informationen austauschen oder auf Ihr Firmen-Intranet zugreifen, nutzen Sie immer die gesicherte Verbindung wie einen VPN-Tunnel, die Ihnen Ihre IT-Abteilung eingerichtet hat. Vermeiden Sie für sensible Daten öffentliche Cloud-Lösungen, auch wenn die vermeintlich einfacher zu bedienen sind.**
5. **Trennen Sie zwischen dienstlich und privat genutzten Geräten und Informationen. Übertragen Sie keine dienstlichen Daten auf private Geräte. Vermeiden Sie auch, dass Ihre Familienangehörige Ihre dienstlichen Geräte privat nutzen.**
6. **Sprachgesteuerte Assistenten bekommen mit, was im Raum gesprochen wird und übermitteln dies an den jeweiligen Betreiber. Deshalb sollten Sie solche Geräte aus Ihrem Arbeitszimmer auch im Homeoffice verbannen. Ist das nicht möglich, decken oder schalten Sie sie ab. Das gilt übrigens auch für die Webcam am Rechner, wenn Sie gerade nicht in der Videokonferenz sind.**
7. **Im Homeoffice sollten Sie stärker als im Büro auf auffällige E-Mails achten. Gerade zuhause gehen viele Nutzer leichtsinniger mit Phishing-Mails um. Achten Sie deshalb bei E-Mails auf Absender, Stil und Logik. Öffnen Sie nur Anhänge, die Sie als sicher einstufen. Lassen Sie sich nicht unter Druck setzen, sofort handeln zu müssen.**
8. **Wie im Büro sollten Sie auch in kurzen Pausen den Bildschirm Ihres PCs und anderer mobiler Geräte sperren, wenn Sie sich vom Schreibtisch verabschieden. Sichern Sie auch zuhause Ihre Geräte gegen unbefugte Nutzung oder gar Diebstahl.**
9. **Haben Sie einen unerlaubten Zugriff festgestellt, informieren Sie unverzüglich die Firmen-IT.**
10. **Statt persönlicher Meetings nutzen Sie Telefon- oder Videokonferenzen? Gerade bei großen Meetings mit vielen Teilnehmern ist es schwierig zu kontrollieren, ob alle, die in der Leitung sind, auch tatsächlich eingeladen wurden. Lassen Sie sich alle Teilnehmer, die in der Meetingsoftware angezeigt werden, kurz vorstellen. So verhindern Sie, dass Unbefugte sich Einwahldaten beschaffen und sensible Themen mitbekommen.**

Quelle: https://new.siemens.com/global/de/unternehmen/stories/forschung-technologien/cybersecurity/how-to-be-secure-in-the-home-office.html

Fortsetzung von Seite 6 ▸ Check Point. Weil die Kontaktbeschränkungen zum Boom von Videokonferenzen und anderen digitalen Kollaborationstools geführt haben, legten Hacker viele neue „Domains" von Videokonferenzen an, um unvorsichtige Mitarbeiter von Unternehmen einen mit Schadsoftware gespickten Download anzubieten. Oder Cloud-Services: Viele Nutzer laden auch sensible Unternehmensdaten in persönliche Instanzen von Cloud-Anwendungen hoch. Im ersten Halbjahr 2020 wurden 63 Prozent der Malware über Cloud-Anwendungen verbreitet, so die Netskope-Analysten.

Fast schon klassisch sind Phishing-Mails, um in die Systemlandschaft eines Unternehmens einzudringen. Neuester Trend ist das Smishing – eine Kombination aus SMS und Phishing. Dabei werden Textnachrichten versandt, die auf betrügerische Links verweisen oder bösartige Anhänge enthalten. Besonders ausgeklügelt ist Spear-Smishing: Dank Internetprofilen und sozialer Netzwerke des Opfers können Cyberkriminelle das Smishing präzise auf eine Person zuschneiden. So entsteht ein trügerisches Gefühl von Vertrauen und Glaubwürdigkeit. Klicken die Empfänger auf die Anhänge, starten sie bösartige Dateien, die weitere Schadprogramme laden und den Computer mit Malware infizieren. Häufig sind dies Ransomware-Trojaner, die eine Zahlung fordern, damit Änderungen rückgängig gemacht werden können, die der Trojaner auf dem Computer des Opfers vorgenommen hat. Im Zweifel ist das ganze System blockiert, wie im Falle des Düsseldorfer Klinikums.

VPN-TUNNEL IM PRIVATEN UMFELD

Viele Unternehmen haben reagiert und beispielsweise Virtual Private Networks (VPN) mit hohen Sicherheitsstandards für den Zugang aus dem Homeoffice eingerichtet. Doch das reicht nicht: Fachleute warnen davor, dass Kriminelle über smarte, vernetzte Geräte wie digitale Assistenten, Thermostate, Entertainmentsysteme oder andere private mobile Endgeräte ins Heimnetzwerk gelangen. Dabei kommt den Hackern entgegen, dass das Thema IT-Sicherheit in einigen Unternehmen lange Zeit nicht ernst genommen wurde.

Überhaupt sind die IT-Abteilungen in vielen Unternehmen schon seit langem überlastet. In den Anfängen der Corona-Pandemie wurden viele Sicherheitsvorschriften stillschweigend aufgeweicht, beispielsweise bei Zugangskontrollen von IT- und Cloud-Systemen. Zwar wissen IT-Fachleute, dass starke Authentifizierungs- und Zugriffsmanagementlösungen wichtig und schlechte Passwörter für die Mehrzahl der Datenschutzverletzungen verantwortlich sind. Doch mangels rasch realisierbarer Alternativen ist das gute alte Passwort nicht nur immer noch da, sondern wird wieder häufiger eingesetzt.

AHNUNGSLOSE MILLENNIALS

Sicher, einen hundertprozentigen Schutz gegen Cyberangriffe gibt es nicht. Allerdings können Unternehmen Risiken verringern, zum Beispiel durch IT-Sicherheitsschulungen für Mitarbeiter. Weil viele Menschen zum ersten Mal ohne den gewohnten Schutz interner Netzwerke arbeiten müssen, sind sie oft ein leichtes Opfer für Cyberkriminelle. Hinzu kommt: Die größten Sicherheitsrisiken für Unternehmen sind nicht Hacker, sondern sogenannte Insider Threats, die von ehemaligen oder aktuellen Mitarbeitern ausgehen. Die handeln meist ohne kriminelle Absicht, sondern einfach fahrlässig und mit mangelndem Problembewusstsein.

Dabei trägt auch die Hoffnung auf die technikaffine Generation Y, die sogenannten Millennials, nicht weit. Der schwedische Security-Anbieter Specops hat die IT-Sicherheitskompetenz der Generation einmal genauer unter die Lupe genommen – mit erschütterndem Ergebnis: Zwei Drittel der befragten Millennials wurden schon einmal gehackt, 73 Prozent der gehackten Nutzer haben ihr persönliches Surfverhalten dennoch unverändert beibehalten. Folgende Begriffe waren ihnen meist unbekannt: Firewall, Malware, Phishing und Spam. ■

— Beitrag CHERRY —

Einfallstor für Insider-Angriffe

Tastaturen können eine Sicherheitslücke sein. Doch sie lässt sich mit einfachen Mitteln effektiv schließen.

Daten und Informationen gehören zu den wertvollsten Ressourcen des 21. Jahrhunderts. Immer mehr geschäftsrelevante Daten werden in die Cloud verlagert. Entsprechend werden die Sicherungsmechanismen angepasst – wie etwa Firewalls, Virenscanner, dezentrale Speicherung, die Verschlüsselung von Daten und Kommunikationskanälen. Das intelligente Zusammenspiel von verschiedenen Sicherheits-Tools durch „Zero-Trust-Security-Konzepte" soll sicherstellen, dass sämtliche Aktionen und Zugriffe auf Daten verifiziert und sicher sind. Und doch hören wir immer wieder von Datendiebstahl oder Identitätsmissbrauch, durch die enorme Schäden entstehen. Dabei spielt die Schnittstelle Tastatur eine große Rolle.

Die eindeutige Authentisierung und Identifikation der Nutzer an Systemen und Anwendungen erfordert stets eine Aktion wie etwa die Eingabe von Passwörtern, biometrischen Informationen, das Einlesen von Chipkarten, Tags oder anderen Token. Das geschieht über Eingabegeräte, die meist über USB angeschlossen sind – und sich daher außerhalb des Wirkungsbereiches aller softwarebasierten Schutzmechanismen befinden.

Das CHERRY SECURE BOARD schützt Ihr Netzwerk vor Insider-Angriffen

Die Tastatur ist dabei noch immer das wichtigste manuelle Eingabegerät und kann nicht ausgesperrt werden. Ein Bad-USB-Device, das sich als Tastatur am USB-Port anmeldet, wird deshalb normalerweise nicht als solches erkannt. Ebenso unsichtbar für gängige Schutzmaßnahmen sind Hardware-Keylogger. Beide sind für jedermann leicht und kostengünstig beschaffbar.

Überall – in Behörden und Firmen, die auch Bestandteil kritischer Infrastrukturen sein können, in Banken, Kaufhäusern oder Krankenhäusern – finden wir ungeschützt zugängliche USB-Schnittstellen. Sie alle können Einfallstor für Insider-Angriffe über die Tastaturschnittstelle sein. Ob zielgerichtet oder aus Frust, ist es für Mitarbeiter wie auch Patienten, Kunden oder Service-Personal möglich, Bad-USB-Devices oder Hardware-Keylogger in wenigen Sekunden unbemerkt zu platzieren. Sie zeichnen alle Tastatureingaben auf und können remote ausgelesen werden. Vertrauliche Daten können so abgeschöpft werden, bevor sie in die mit riesigem Sicherheitsaufwand entwickelte Infrastruktur gelangen. Das gleiche gilt für Passwörter und E-Mails, die abgefangen werden, bevor sie verschlüsselt versendet werden. Keylogger können nicht durch USB-Überwachung oder Software, weder lokal noch aus der Cloud erkannt oder abgewehrt werden.

Die Lösung sind vertrauenswürdige Eingabegeräte, zum Beispiel authentisierbare Tastaturen mit verschlüsselter Tastenübertragung. Das CHERRY SECURE BOARD schließt diese Sicherheitslücke. Es kann als Standardtastatur mit integriertem Dual-Interface-Leser für Chipkarten oder mit RF/NFC-Karten und Token verwendet werden. Damit ist sie ideal geeignet für 2-Faktor-Authentisierung mit Chipkarten, kontaktlosen Karten, Tags und FIDO-2 NFC-Token.

Im „SECURE Modus" überträgt die Tastatur alle Eingaben verschlüsselt über eine TLS 1.3 Verbindung. Gleichzeitig wird der Standard-HID-Kanal gesperrt. Sowohl Keylogger als auch Bad-USB-Devices sind wirkungslos und können keinen Schaden mehr anrichten. Denn Endpoint-Security beginnt bereits am Eingabegerät!

www.cherry.de

— Beitrag STORMSHIELD —

KRITIS und Cyberresilienz

Laut dem Cybersecurity-Spezialisten Stormshield ist eine solide Strategie zur Stärkung der Cyberresilienz kritischer Organisationen eine Frage der Verantwortung.

Unter kritischen Infrastrukturen (KRITIS) versteht die Bundesregierung „(…) Organisationen oder Einrichtungen (…), bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden" (Zit. kritis.bund.de). Von Fertigungsanlagen über Gesundheitseinrichtungen, Museen und Einkaufszentren bis hin zu den öffentlichen Verkehrsmitteln, alle nutzen operative (OT-)Informationssysteme, die es uns ermöglichen, unseren Alltag „normal", ggf. sogar komfortabler und sicherer zu leben. Doch infolge der zunehmenden „Smartisierung" dieser Infrastrukturen und der Allgegenwart digitaler Technologien werden diese traditionell isolierten Systeme zwar effizienter und agiler, aber auch anfälliger für neue Cyberrisiken.

Als europäische Referenz für Cybersecurity im Bereich IT- und OT-Systeme, kritischer Infrastrukturen und sensibler Daten sind wir bei Stormshield der Meinung, dass die unaufhaltsame Vernetzung der KRITIS und die damit verbundenen Fragen der Cybersicherheit nicht länger als rein technische Anliegen betrachtet werden dürfen. Beide sind heute nämlich Grundpfeiler der geschäftlichen Belastbarkeit dieser Organisationen und deren Fähigkeit, trotz möglicher Krisensituationen lebenswichtige Dienste zu erbringen. Genau das ist die Cyberresilienz und sie zu steigern ist angesichts der sich rasant entwickelnden Cyberbedrohungen mehr denn je eine Frage der Verantwortung. Doch wie setzt man sie um?

DIE RICHTIGE KOMBINATION

Der Ansatz der Resilienz zielt darauf ab, die Auswirkungen einer Cyberattacke auf den Betrieb des Unternehmens zu minimieren. Wie bei allen Prozessen im Krisenmanagement muss die Cyberresilienz als erste unerlässliche Schutzschicht bereits gewährleistet sein, bevor es zu einem Vorfall kommt. Es gilt hierbei zu bedenken, dass es sich um kein einmaliges Verfahren handelt: Das eigene Cyberresilienz-Niveau muss regelmäßig getestet werden. Ein neues Geschäftsprojekt kann zum Beispiel das Risiko für einen Cyberangriff erhöhen, und wenn diese Gefahr nicht rechtzeitig erkannt wird, ist die gesamte Strategie wirkungslos. Die Cybersicherheit spielt hier eine wesentliche Rolle. Die Auswahl vertrauenswürdiger Technologien und die Implementierung einer geeigneten Segmentierung der Netze und adäquater Sicherheits-Policies genießen dabei Vorrang.

UWE GRIES
Country-Manager DACH, Stormshield

Die menschliche Komponente ist ebenfalls entscheidend. Man darf sich nicht nur darauf verlassen, dass die automatisierten Prozesse und technischen Security-by-Design-Maßnahmen greifen. Für die Erlangung der Cyberresilienz bedarf es ebenfalls fachkundiger Teams und der weitreichenden Sensibilisierung der Mitarbeiter für das Thema Cybersicherheit und digitale Hygiene.

Und schließlich sollte dasselbe auch innerhalb der gesamten Versorgungskette der KRITIS verlangt werden, denn eine Kette ist nur so stark wie ihr schwächstes Glied.

www.stormshield.com/de

FORUM DER AKTEURE

IT made in Germany

Die Redaktion befragt Akteure zu Trends in den Bereichen Cybersecurity und Cloud Management.

Susanne Dehmel
Mitglied der Geschäftsleitung
Bitkom

Unternehmen stehen zunehmend unter Beschuss durch Cyberattacken. Drei von vier Unternehmen in Deutschland sind in den Jahren 2018/2019 Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Dadurch ist ein Schaden von mehr als 100 Milliarden Euro pro Jahr entstanden. Umfang und Qualität der Angriffe nehmen immer mehr zu, Angriffsarten verändern sich ständig.

»IT-Sicherheit muss Chefsache sein.«

Fakt ist, dass durch einen vergleichbar geringen Aufwand hoher Schaden angerichtet werden kann, weshalb Cyberattacken für Kriminelle attraktiv sind. Entsprechend müssen Unternehmen vorbeugen und ein robustes IT-Sicherheitsmanagement aufbauen, aktuell halten und engagiert betreiben. Dazu gehört die organisatorische, technische und personelle Sicherheit im Betrieb. Viele Unternehmen investieren derzeit verstärkt in IT-Sicherheit und haben bereits Maßnahmen ergriffen, um sich besser gegen Angreifer zu schützen. Wer dies nicht tut, handelt fahrlässig. Ein erfolgreicher Angriff kann Unternehmen operativ beeinträchtigen oder ihr Image beschädigen, in Einzelfällen kann es die Existenz gefährden.

Sehr oft erfolgen Angriffe durch aktuelle oder frühere Mitarbeiter. In manchen Fällen kommt es zu bewusster Sabotage oder Datendiebstahl, wenn ein Beschäftigter beispielsweise zum Wettbewerber wechselt. Oft werden Mitarbeiter unwissentlich als Angriffsvektor benutzt. Hier helfen regelmäßige Schulungen, die für die Gefahren sensibilisieren und Verhaltensregeln erklären. So ließe sich die Sicherheit in den Unternehmen mit vergleichsweise geringem Aufwand und in kurzer Zeit deutlich erhöhen.

Absolute Sicherheit wird es aber nie geben können. Entscheidend ist, dass Unternehmen das Thema IT-Sicherheit zur Chefsache machen und es über eigene Wirtschaftsschutzbeauftragte oder IT-Sicherheitsbeauftragte fest verankern, operativ wie strategisch.

www.bitkom.org

Dr. Oliver Grün
Präsident
Bundesverband IT-Mittelstand

Durch die Corona-Pandemie hat der Anteil der im Homeoffice arbeitenden Menschen drastisch zugenommen. Die meisten Unternehmen hat das kurzfristig vor enorme Herausforderungen bezüglich ihrer IT-Infrastruktur gestellt.

Zwangsläufig hat die Pandemie viele Unternehmen, die dem Einsatz von Cloud-Lösungen kritisch gegenüberstanden, dazu gebracht, den Wechsel in die Cloud zu wagen. Oftmals waren es Bedenken im Bereich der Datensicherheit, die eben diese Transition in die Cloud verhindert haben. Das ist zwar verständlich und auch wichtig, doch die Schlussfolgerung dieser Überlegungen war viel zu lange, es mit der Cloud dann lieber ganz sein zu lassen.

»Es gibt viele gute Cloud-Lösungen Hosted und Made in Germany.«

Dabei ist der Wechsel in die Cloud vor allem für mittelständische Unternehmen mit vielen Vorteilen verbunden – besonders im Sicherheitsbereich, der oft als Risiko wahrgenommen wird. Für den Mittelstand bedeutet es einen hohen Zeit- und Kostenaufwand, die eigene IT mit allen Sicherheitsanforderungen auf dem neusten Stand zu halten. Wechselt das Unternehmen in die Cloud, können dort Sicherheitsstandards auf viel höherem Niveau geboten werden. Die Anbieter von Cloud-Lösungen sind Profis auf ihrem Gebiet. Und es gibt viele gute Cloud-Lösungen Hosted und Made in Germany, die dem strengen deutschen Datenschutz unterliegen und diesen erfüllen.

Der Mittelstand sollte in den Wechsel in die Cloud einen Gewinn sehen: Die Unternehmen gewinnen Flexibilität für ihre Mitarbeiter, aber auch für ihre Infrastruktur. Nach der Auswahl einer sicheren Cloud-Lösung, die dem deutschen Datenschutz unterliegt, ist der Kopf danach frei für das eigene Geschäft und neue Innovationen.

www.bitmi.de

Dr. Holger Mühlbauer
Geschäftsführer
TeleTrusT Bundesverband IT-Sicherheit e. V.

Deutschland ist nach wie vor zu großen Teilen im Home-Office-Modus: Die derzeitige Situation führt erzwungenermaßen zu einer enormen Digitalisierungsbeschleunigung. In kürzester Zeit werden zu Hause Arbeitsplätze nachgebildet, um Betriebsstrukturen digital aufrecht zu erhalten. Während technisch gut aufgestellte Unternehmen ihre Mitarbeiter mit professionellem Equipment ausrüsten, ist anderswo Improvisation und Pragmatismus gefragt. Dabei kann die IT-Sicherheit auf der Strecke bleiben.

»Cloud Management beginnt die Strukturen der Wirtschaft nachhaltig zu verändern.«

Gerade jetzt aber schwärmen digitale Raubritter aus, um die Gunst der Stunde zu nutzen und mit Spam, Phishing, Malware, Identitätsdiebstahl und Datenklau schnelle Beute zu machen. In etlichen Fällen werden hilfsweise private Hard- und Software sowie Netzanbindungen genutzt, die es den Tätern noch vereinfachen. Der Bundesverband IT-Sicherheit e.V. hatte dies zum Anlass genommen und befristet kostenfreie IT-Sicherheitslösungen seiner Mitglieder gelistet, um betroffenen Anwendern Unterstützung zu bieten.

Als Teil von IT-Sicherheit ist Cloud Management ein aktuelles Thema für Unternehmen. Cloud Management beginnt die Strukturen und Arbeitsabläufe in der Wirtschaft nachhaltig zu verändern. Dabei erschließt es Synergieeffekte durch die gemeinsame Nutzung von Ressourcen. Diese Synergieeffekte führen teilweise auch zu einer Verbesserung der IT-Sicherheit gegenüber traditionellen IT-Systemen. Andererseits sind viele Datenschutz- und Sicherheitsfragen beim Cloud Management zumindest nicht vollständig geklärt. Organisationen mit vereinfachter Infrastruktur können oft keine besonderen Bedingungen und SLAs mit den Anbietern aushandeln, umso mehr müssen sie die Bedingungen der Standardangebote sorgfältig prüfen. Dies besonders dann, wenn es um die Verarbeitung personenbezogener Daten geht.

www.teletrust.de

— Beitrag BOXCRYPTOR —

Verschlüsselung für Unternehmensdaten – 3 wichtige Kriterien

Richtig eingesetzt ermöglicht Verschlüsselung datenschutzkonforme Cloudnutzung im Unternehmen. Folgende Kriterien sind für die Wahl einer Verschlüsselungslösung für Ihre schutzbedürftigen Unternehmensdaten besonders entscheidend.

ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Sensible Daten, die das Unternehmen verlassen, müssen bereits direkt auf den Endgeräten der Mitarbeiter und Mitarbeiterinnen verschlüsselt werden. Nur so sind sie weder beim Transport noch am Ablageort in Klartext einsehbar. Achten Sie auch darauf, welche Verschlüsselungsverfahren zum Einsatz kommen. Aktueller Standard ist der öffentliche Verschlüsselungsalgorithmus Advanced Encryption Standard (AES) mit einer Schlüssellänge von 256 Bit.

FLEXIBILITÄT UND SKALIERBARKEIT

Binden Sie sich mit der Verschlüsselung nicht an einen bestimmten Cloud-Anbieter. So sollten neben verschiedenen Clouds auch Fileserver oder lokale Daten mit der gleichen Software verschlüsselt werden können. Bedenken Sie auch Plattformen wie Microsoft Teams, über die ebenfalls Dateien in einem Cloud-Speicher abgelegt werden. Zudem sollte die Lösung skalierbar sein und sich ohne größeren Aufwand an eine geänderte Unternehmenssituation anpassen lassen.

ANWENDERFREUNDLICHKEIT

Nur wenn die Verschlüsselungslösung eine intuitive Zusammenarbeit gewährt, wird sie im Unternehmen in der Praxis angenommen. Im Idealfall weicht sie so wenig wie möglich vom bekannten Ablauf ab und bietet eine einfache und datenschutzkonforme Möglichkeit der Zusammenarbeit. Darüber hinaus sollte Ihnen der Anbieter nebst passenden Materialien, Webinaren oder Videos auch ein schnelles, zuverlässiges Support-Team zur Verfügung stellen.

— Beitrag FRAUNHOFER ACADEMY —

Pole Position für die International Data Spaces und GAIA-X

SASCHA WESSEL
Abteilungsleiter am Fraunhofer AISEC

Das Projekt GAIA-X, oftmals als „die europäische Cloud" umschrieben, ist derzeit in aller Munde. Dabei handelt es sich nicht um einen weiteren neuen Cloud-Anbieter, sondern vielmehr eine vernetzte Dateninfrastruktur für ein europäisches digitales Ökosystem. Durch offene Schnittstellen und Standards soll hierbei eine Interoperabilität zwischen verschiedenen Anbietern und Services geschaffen werden. Wesentliche Motivation dafür ist die Sicherstellung der Datensouveränität für Unternehmen sowie für Bürgerinnen und Bürger.

Im Rahmen der Initiative IDS (International Data Spaces) beteiligt sich Fraunhofer in Kooperation mit einer Vielzahl von Industrieunternehmen an der Entwicklung von GAIA-X. Zentrales Ziel des bereits 2015 gestarteten IDS-Projektes ist der souveräne Austausch von Daten, ohne dabei die Kontrolle über ihre Verwendung zu verlieren. Hierfür können IDS-Konnektoren Nutzungsrestriktionen erzwingen und einen sicheren sowie vertrauenswürdigen Datenaustausch ermöglichen – und zwar unabhängig davon, ob dieser Austausch zwischen Konnektoren in der Cloud, in Rechenzentren oder auf Edge Devices erfolgt.

Entscheidend für den Erfolg ist die nachweisbare Vertrauenswürdigkeit der Konnektoren bzw. der Infrastruktur. Unter der Leitung von Fraunhofer hat die Arbeitsgruppe Zertifizierung der International Data Spaces Association hierfür das IDS-Zertifizierungsschema erarbeitet, das die verschiedenen Sicherheitslevel und die dafür zu erfüllenden Anforderungen beschreibt.

Zu diesem Thema bieten die Fraunhofer-Institute AISEC und FOKUS einen Workshop für Unternehmen an. Hier erfahren Teilnehmende, was für eine erfolgreiche Zertifizierung und Teilnahme im IDS notwendig ist und gleichen dies mit dem aktuellen Entwicklungsstand ihres Produktes ab. Der Workshop findet auf Anfrage statt.

TEXT: Sascha Wessel, *Abteilungsleitung Sichere Betriebssysteme am Fraunhofer AISEC (sascha.wessel@aisec.fraunhofer.de)*
Monika Huber, *Wissenschaftliche Mitarbeiterin am Fraunhofer AISEC und Leiterin der Arbeitsgruppe Zertifizierung der International Data Spaces Association (monika.huber@aisec.fraunhofer.de)*
Nadja Menz, *Gruppenleiterin am Fraunhofer FOKUS (nadja.menz@fokus.fraunhofer.de)*

www.cybersicherheit.fraunhofer.de/ids-komponentenzertifizierung

Smart Work

Die Digitalisierung der Arbeitswelt verkürzt die Aktualität von Wissen und Kompetenzen zunehmend. Die Konsequenz: permanente Weiterbildung – und zwar eigenverantwortlich.

Julia Thiem / Redaktion

Unsere Arbeitswelt verändert sich – und das nicht erst seit Corona. Besonders deutlich wird das bei einem Blick auf aktuelle Stellenangebote. Dort werben Firmen neuerdings damit, ein CO_2-neutrales Unternehmen zu sein, über ein Craftbier-Abo zu verfügen oder Mitarbeitern freien Zugang zur weltweit größten Weiterbildungsplattform zu bieten. Vor allem letzterer Aspekt wird in einer sich permanent verändernden Welt immer wichtiger. Denn wer heute nicht wenigstens über ein grundlegendes technisches Verständnis oder Programmierkenntnisse verfügt, hat es in einer zunehmend digitalen Arbeitswelt schwerer. Für alle, die keinen Abschluss in Informatik haben, heißt die Konsequenz daher: Weiterbildung.

Das ist an sich nicht neu. Weiterbildung spielt in vielen Unternehmen seit jeher eine wichtige Rolle. Es gibt eigene Akademien oder zumindest ein von HR gesteuertes Angebot. Allerdings verändert sich die Art der Weiterbildung mit zunehmender Digitalisierung – und vor allem auch noch einmal durch den Ausbruch von Covid-19. Das verdeutlicht nun eine aktuelle, gemeinsame Studie der Bitkom Akademie und HRpepper Management Consultants. Eine wichtige Erkenntnis der Erhebung: Weiterbildungen werden kürzer, digitaler, effizienter sowie zielgerichteter und können leichter in den Arbeitsalltag integriert werden. Und ganz im Sinne der von Eigenverantwortung geprägten New-Work-Bewegung werden Angestellte in Zukunft ihre berufliche Weiterentwicklung zunehmend selbst steuern.

Wenn sich nämlich die Belegschaft im Sinne des „Job Craftings“ die Arbeit so formen soll, dass sie zu den eigenen Talenten und Ansprüchen passt, muss auch die passende Weiterentwicklung von den Angestellten selbst geplant werden können. Voraussetzung dafür sei, dass das Management den strategischen Wert von Weiterbildung deutlicher kommuniziert, glaubt Dr. Matthias Meifert, Managing Partner der HRpepper Management Consultants: „Es sollten Rahmenbedingungen geschaffen werden, in denen Mitarbeitende auch mehr Eigenverantwortung übernehmen dürfen.“ Solche Freiräume werden nämlich tatsächlich genutzt, wie die Studie weiter unterstreicht: Beinahe jeder Dritte setzt seit Beginn der Corona-Pandemie mehr Zeit für Weiterbildungen ein. Fast 90 Prozent der Befragten gaben an, kostenfreie Online-Seminare besucht zu haben.

Bei der Direktbank ING ist das lebenslange Lernen seit September dieses Jahres sogar im Tarifvertrag verankert. Den rund 4.000 Mitarbeitenden in Deutschland steht damit ab sofort ein individuelles Weiterbildungsbudget in Höhe von 500 Euro pro Jahr zu Verfügung. Damit soll es den Beschäftigten ermöglicht werden, in einer Arbeitswelt, die sich im digitalen Umbruch befindet, immer auf dem neusten Stand zu bleiben und lebenslang zu lernen. „Das ist einmalig in der Bankenbranche", erklärt der für Kreditinstitute zuständige Bundesfachgruppenleiter der Vereinten Dienstleistungsgewerkschaft (Verdi), Jan Duscheck, der den Zukunftstarifvertrag mit der ING ausgehandelt hat. Vermutlich wird dieses Konzept in Zukunft noch in Unternehmen anderer Branchen Schule machen.

STRATEGIEFORUM / IMPULSE

Worin liegen die Chancen für IT-Security und Cloud-Computing?

JOHANNES JUNG
Geschäftsführer ATLAS Intelligence GmbH

... haben Zukunftstechnologien schon immer fasziniert. Nach Abschluss der Studiengänge Wirtschaftsingenieurwesen und Rechtswissenschaften konnte er sein Hobby zum Beruf machen.

Wir haben eine einzigartige Chance, beim Thema IT-Sicherheit und Datenschutz eine globale Vorreiterstellung einzunehmen. In Zeiten der rasant zunehmenden Digitalisierung ist Cyber-Security längst zu einem entscheidenden Wettbewerbsvorteil geworden. Insbesondere deutsche Unternehmen sind ein attraktives Ziel für Industriespionage. Wir müssen unsere Wirtschaft vor Cyberangriffen proaktiv schützen und Deutschland als Zukunftsstandort für digitale Technologien sichern und ausbauen.

PROF. DR. JOCHEN DEISTER
CEO und Mitgründer Privacy Solutions GmbH, Partner bei DMZ Legal

... ist Jurist, Entrepreneur, Scrum Product Owner und Autor. Er l(i)ebt Datenschutz und Lean Startup, berät und lehrt mit allen Facetten seines kreativen Geistes, der auch vor Künstlicher Intelligenz nicht zurückscheut.

Chancen entstehen, wenn man Herausforderungen zu Möglichkeiten macht. Das sehe ich gerade für den Datenschutz, der als Innovationsbremse empfunden wird. Das verkennt aber die Chance, die ein respektvoller Umgang mit Kunden- und Mitarbeiterdaten bietet: Wer sich so profiliert, kann sich bei diesem wichtigen, weichen Punkt wirksam von anderen abheben, bindet Kunden und Mitarbeiter langfristig. Denn: Respekt kann man nicht mit Technologie erzwingen.

ARMANDO CHIODI
Partner Cyber Security, Q_PERIOR

... ist Familienmensch und Unternehmer sowie fasziniert von der Geschwindigkeit der derzeitigen Veränderungen.

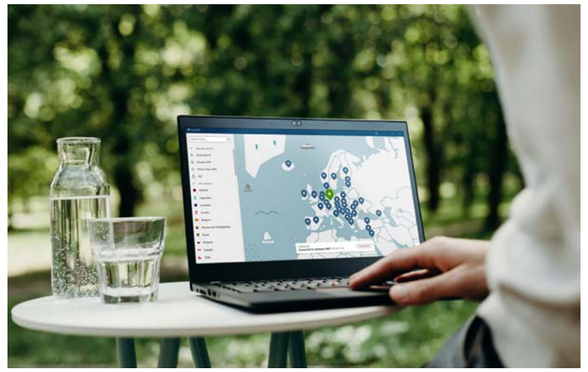
Wirtschaft und Gesellschaft verändern sich durch die digitale Transformation grundlegend. Daher muss IT-Security zu einem integralen Bestandteil der Geschäftsprozesse und der Client Journey werden. Dies gilt unabhängig von Branche und Produkt. Die Sicherheit der IT ist dabei kein Selbstzweck, sondern muss sich effizient und effektiv in alle Geschäftsprozesse integrieren und diese unterstützen. Dadurch können Unternehmen das Kundenvertrauen weiter steigern, um nachhaltig erfolgreich zu sein.

— Beitrag NordVPN —

Wie VPN eine Schlüsselrolle in der Online-Sicherheit übernahm

Daniel Markuson, Experte für digitale Privatsphäre, erläutert die Auswirkungen der weltweiten Pandemie auf die Cyber-Sicherheit der Firmen und der Homeoffice-Mitarbeiter.

Während die Fallzahlen in Europa steigen, sehen sich viele Firmen erneut gezwungen, ihre Mitarbeiter die Arbeit von zu Hause aus erledigen zu lassen. Das Risiko von Datenlecks in Unternehmen ist damit weiter präsent. Sowohl Arbeitgeber wie auch Arbeitnehmer sind angreifbarer denn je. Kann ein VPN, also ein virtuelles privates Netzwerk, Menschen im Homeoffice davor bewahren, zu einer Schwachstelle in der Netzsicherheit des Unternehmens zu werden? Wir fragen Daniel Markuson, den Experten für digitale Privatsphäre bei NordVPN, nach den besten Sicherheitspraktiken.



Laut NordVPN ist die Nutzung von VPN während der Pandemie drastisch gestiegen.

Wann steigt die Gefahr für Arbeitgeber und Arbeitnehmer, Opfer von Internetkriminalität zu werden?

Internetkriminelle neigen dazu, die Menschen dann zu attackieren, wenn sie am stärksten angreifbar sind. Die Anzahl an Betrügereien und Sicherheitsvorfällen, die mit dem Coronavirus zusammenhängen, ist stetig gestiegen. Hacker nutzen die Angst der Menschen aus, verbreiten Falschinformationen und machen aus der Panik Geld.

Unternehmen haben im Homeoffice nicht mehr die Kontrolle über die Infrastruktur ihrer Mitarbeiter. Jeder Internetkriminelle weiß das ganz genau. Mitarbeiter verwenden ihre persönlichen Geräte, um auf das Firmennetzwerk zuzugreifen, es gibt schwache Passwörter und ungesicherte WLAN-Verbindungen. Das sind nur einige Gründe für ein erhöhtes Risiko, Ziel eines Hacker-Angriffs zu werden.

Wie stark haben die Lockdown-Maßnahmen und das mobile Arbeiten die VPN-Nutzung weltweit ansteigen lassen?

Im März, als die weltweite Pandemie begann, hatten wir bei unserem VPN für Unternehmen – NordVPN Teams – eine Nutzungssteigerung von 165 Prozent. Weltweit sind die Verkäufe um 600 Prozent gestiegen. Das kann man ohne Zweifel darauf zurückführen, dass Unternehmen ihre Angestellten verstärkt ins Homeoffice geschickt haben. Gleichzeitig verzeichnet NordVPN einen enormen Anstieg bei den mobilen Downloads.

Keiner konnte mit so einem schnellen und gewaltigen Ausbruch rechnen, daher waren viele Unternehmen nicht vorbereitet. Doch VPN wurde schnell zur favorisierten Lösung, als es um den Schutz des Firmen-Netzwerkes ging. Ein VPN gewährt Angestellten, die zu Hause arbeiten, sicheren Zugang zu Servern, Systemen und Datenbanken, auf die sie sonst nur vom Büro aus Zugriff hätten.

Der VPN-Markt ist riesig und unerfahrene Nutzer können schnell überfordert sein, wenn sie nach einem Anbieter suchen. Wie hebt sich NordVPN aus der Menge an VPNs ab?

Mit einem einzigen Klick bekommen unsere Nutzer für ihren Online-Verkehr eine Verschlüsselung nach dem neuesten Technologiestandard. Die Kombination aus Benutzerfreundlichkeit unserer App und dem hohen Sicherheitsstandard hat uns dabei geholfen, weltweit mit Empfehlung der Profis aus der Technologiebranche der führende VPN-Anbieter zu werden.

Dieses Jahr haben wir unser eigenes VPN-Protokoll – NordLynx – eingeführt. Es ist die schnellste und sicherste VPN-Lösung auf dem Markt und wurde auf der Basis der Technologie von Wireguard® aufgebaut. Zudem bietet NordVPN das umfangreichste Netzwerk an Servern auf dem Markt. Unsere Nutzer können aus mehr als 5300 Servern in 59 Ländern wählen. Das hilft, eine Überlastung des Netzwerks zu vermeiden und gewährleistet die beste VPN-Verbindung.

Wir wissen, dass Vertrauen die wichtigste Rolle für VPN-Nutzer spielt. Daher haben wir eines der führenden Wirtschaftsprüfungsunternehmen – Pricewaterhouse-Coopers AG aus der Schweiz – gebeten, unseren No-Logs-Grundsatz einer in dieser Branche erstmaligen Prüfung zu unterziehen. Der Bericht bestätigt die Tatsache, dass NordVPN keine privaten Daten seiner Nutzer nachverfolgt, sammelt oder teilt.

Wie kann ein VPN einem Unternehmen helfen? Was sind derzeit die größten Risiken für Firmen?

90 Prozent der Datenpannen in der Cloud bei Unternehmen passieren, weil Hackerattacken auf Angestellte abzielen. Im Büro benutzt jeder dieselbe Internetverbindung. Deswegen ist es einfacher, sicheren Zugang zu allen internen Ressourcen zu gewährleisten. An so vielen verschiedenen Homeoffice-Standorten kann der Sicherheitsstandard nicht aufrechterhalten werden.

Mit Hilfe eines VPN entsteht ein sicherer, verschlüsselter Tunnel für den Online-Verkehr. Keiner kann durch den Tunnel sehen und sensible Unternehmensdaten abgreifen. Angestellte können sich von jedem Gerät aus sicher mit dem Unternehmensnetzwerk verbinden. Das ist vor allem dann wichtig, wenn öffentliche Hotspots genutzt werden, die von Hackern überwacht werden können.

Eine Studie von NordVPN hat ergeben, dass 62 Prozent der Menschen persönliche Geräte im Homeoffice nutzen. Das ist besorgniserregend, denn die meisten privaten Laptops sind nicht mit angemessener Sicherheitssoftware ausgerüstet. Außerdem tendieren die Menschen zu Hause dazu, nachlässiger zu sein und sie greifen auf Websites zu, die möglicherweise unsicher sind. Ein Klick auf einen bösartigen Link kann Hackern Zugriff auf den Computer des Angestellten geben – und auf alle Konten und Systeme, die damit verbunden sind. Weil ein VPN Schutz in all diesen Fällen bietet, ist die Nachfrage nach dem Dienst so stark wie nie.

Unsere Lösung für Unternehmen nutzen bereits mehr als 10.000 Kunden, obwohl NordVPN Teams erst letztes Jahr eingeführt worden ist. Es sind sowohl kleine Unternehmen als auch global tätige Großfirmen. Wir möchten jedem, der online nach Sicherheit und Privatsphäre sucht, den besten Service bieten.

Daniel Markuson, Experte für digitale Privatsphäre bei NordVPN.

Eine abschließende Frage: Ist VPN eine kurz- oder langfristige Sicherheitslösung?

Ich denke, dass viele Unternehmen nach dem Ende der Pandemie weiterhin mobiles Arbeiten ermöglichen werden. Die Arbeitgeber werden nicht nur akut ihre Netzwerke schützen wollen, sondern Internetsicherheit zu einem wesentlichen Teil ihrer Business-Pläne machen müssen. Und VPNs spielen eine große Rolle, um mobiles Arbeiten sicher zu machen.

www.nordvpn.com

Digitale Souveränität

Wer Datenschutz ernst nimmt und innovationsfähig bleiben will, muss volle Kontrolle über Datenströme besitzen.

Interview: Klaus Lüber / Redaktion

Kaum ein Konzept ist in der Diskussion um die Digitale Transformation unserer Gesellschaft gerade so präsent wie das der Datensouveränität. Gemeint ist „die vollständige Kontrolle über gespeicherte und verarbeitete Daten sowie die unabhängige Entscheidung darüber, wer darauf zugreifen darf", wie es ein im Rahmen des Digitalgipfels 2018 veröffentlichtes Paper beschreibt. Was das konkret bedeutet, zeigt folgendes „Schichtenmodell":

GRAD DIGITALER SOUVERÄNITÄT	NIEDRIGE AUSPRÄGUNG (= HOHE ABHÄNGIGKEIT)	MITTLERE AUSPRÄGUNG	HOHE AUSPRÄGUNG (= KEINE ABHÄNGIGKEIT)
DATEN	Der Anbieter und nicht der Anwender entscheidet, welche Daten er wem zur Verfügung stellt und wie er diese nutzt.	Anwenderorganisation hat vollständige Kontrolle darüber, wer Zugriff auf Daten hat und kann diese jederzeit löschen.	Daten können unabhängig von der eingesetzten Softwarelösung gelesen, geändert und gelöscht werden.
SCHNITTSTELLEN	Keine oder nur proprietäre Schnittstellen verfügbar	Unterstützung einer hohen Anzahl offener Standards und Schnittstellen	Zugriff auf alle Daten und Funktionen über offene, frei nutzbare Schnittstellen mit quelloffener Referenzimplementierung
QUELLCODE	Quellcode nicht verfügbar	Quellcode prüfbar/Quellcode bei Ausfall des Herstellers verfügbar („Escrow")	Quellcode veränderbar/verändert nutzbar
HARDWARE	Muss komplett zugekauft werden	Bestehende Lösungen können durch eigene Hardware ergänzt werden.	Alle Hardware-Komponenten können selbst produziert und beeinflusst werden.
KONTROLLE	Die Lösung ist nur bei einem einzigen Anbieter verfügbar, es gibt keine Kontroll- oder Migrationsmöglichkeiten.	Wichtige Teile können kontrolliert und zu anderen Anbietern migriert werden, der Aufbau einer selbst betriebenen Lösung ist möglich.	Anwenderorganisation betreibt Lösung selbst und hat Kontrolle über alle Komponenten (Quellcode, Hardware, ...).
KOMPETENZEN	Kein Verständnis für Prozesse und Datenverwendung, keine Kompetenz zur Anpassung vorhanden	Verständnis von Daten und Prozessen ist vorhanden, Möglichkeiten zur Anpassung existieren in begrenztem Rahmen.	Kompetenzen für Veränderung von Daten, Programmcode und Prozessen sind vorhanden und verfügbar.
JURISDIKTION	Anbieter untersteht Nicht-EU-Recht.	Anbieter untersteht Nicht-EU-Recht, aber es bestehen verlässliche Verträge, welche die Einhaltung europäischer Standards sicherstellen.	Anbieter befindet sich in Deutschland bzw. in der Europäischen Union und untersteht ausschließlich dieser Jurisdiktion.

Quelle: „Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen." Digital Gipfel Nürnberg 2018

— Beitrag PRIVACY SOLUTIONS GMBH —

Datenschutz und Künstliche Intelligenz – Kein Widerspruch

Risikoeinschätzung im Datenschutz neu gedacht

Herr Prof. Deister, Sie sind seit über 20 Jahren im Datenschutz tätig, bei großen Kanzleien und internationalen Unternehmen, jetzt bei der Privacy Solutions GmbH und DMZ Legal. Was hat sich durch die Datenschutzgrundverordnung geändert?

Die DSGVO bewegt Unternehmen zum respektvollen Umgang mit personenbezogenen Daten, ob sie es wollen oder nicht. Wer sich darauf einlässt, wird zukunftsfähig.

Datenschutz als geschäftsfördernd – ist das nicht eine steile These?

Nur vordergründig. Vor Amazon existierte Kundenservice nur als Kostenfaktor. So ist es auch mit dem Datenschutz, der oft als mühsam und kostenintensiv gesehen wird. Aber: Worüber wollen Sie sich denn differenzieren in unserer dynamischen Welt? Über Ihr in einem Jahr veraltetes Produkt, ihre in sechs Monaten überholte Technologie? Langfristigen Erfolg haben Sie nur, wenn Sie Ihre Kunden und Mitarbeiter respektvoll behandeln. Und dazu gehört heutzutage eben der respektvolle Umgang mit deren Daten.

In meinen Lean-IT-Startup-Seminaren wird Datenschutz inzwischen ganz selbstverständlich von Beginn an mitgedacht und als respektvoller Umgang mit Kunden und Mitarbeitern verstanden.

RA PROF. DR. JOCHEN DEISTER
CEO,
Privacy Solutions GmbH

Wir leben in einer Welt der künstlichen Intelligenz und Big Data. Daten gelten als die Währung der Zukunft. Ist das nicht ein Widerspruch?

Das muss es nicht sein. Ich bin Mitgründer der Privacy Solutions GmbH, einem erfolgreichen, internationalen Startup. In unserer Datenschutzmanagementsoftware Privacy Suite nutzen wir künstliche Intelligenz, um datenschutzrechtliche Risiken besser zu erkennen. KI und Datenschutz sind bei uns also kein Widerspruch, sondern gehen Hand in Hand.

Wie soll das gehen?

Das Land Hessen hat uns nach einem zweistufigen Experten-Auswahlprozess für eine Innovationsförderung ausgewählt, damit wir eine Wissensbasis über datenschutzrechtliche Bewertungen aufbauen. Die Einschätzungen aller beteiligten Datenschutzexperten fließen ein, das Wissen wird mit KI gebündelt und steht damit auch kleineren Unternehmen zur Verfügung, ohne dass auch nur die kleinste vertrauliche Information offenbar wird. Ein Win-Win für alle.

So technologisch wird Datenschutz aber bisher selten betrieben.

Richtig – und gerade deshalb ist es eine große Chance. Wer den respektvollen Umgang mit Daten ernst nimmt, der muss erst einmal genau wissen, wo welche Daten warum und wie verarbeitet werden. Das geht nur mit hochspezialisierter Software wie der Privacy Suite.

Was leistet denn Ihre Datenschutzmanagementsoftware?

In der Privacy Suite werden Datenverarbeitungsprozesse erfasst. Das kann durch Datenschutzbeauftragte, Fachabteilung oder betreuende Juristen geschehen. Diese Prozesse werden regelbasiert analysiert und bewertet, zukünftig zudem unter Einsatz von KI. Bei datenschutzrechtlich riskanten Prozessen werden Maßnahmen zur Risikominimierung vorgeschlagen. So hat man jederzeit einen guten Überblick über die eigene Datenverarbeitung – und erkennt, wo Verbesserungspotenziale liegen.

www.privacy-solutions.org

Noch mehr Inhalte in der App!

www.inpactmedia.com

AVAILABLE ON

in|pact mediaverlag

MEHR
Zusätzliche Inhalte plus Multimedia-Content

THEMEN
Kostenloser Zugriff auf alle Publikationen

AKTUELL
Per Push-Nachricht immer informiert