BDO foresight

MAGAZIN №4

Cyber-Resilienz 2024

Wie sich Unternehmen gegen wachsende Bedrohungen aus dem Netz wappnen können

Staat of the Art?

Cyber-Fortschritt mit Hürden: Deutschlands Bemühungen um digitale Sicherheit

Up to Data

Die digitale Transformation meistern: Körbers Pionierarbeit in der Cyber-Sicherheit

BDO

Titelbild: Adobe Stock

BDO foresight …

Kennen Sie das auch? Ein Thema taucht scheinbar langsam auf und man plant, sich „irgendwann“ damit zu befassen. Plötzlich wird dieses Thema omnipräsent und die Erkenntnis stellt sich ein, dass man sich doch noch nicht ausreichend darum gekümmert hat.

Im digitalen Zeitalter betrifft dies häufig das Thema „Sicherheit“. In dieser Ausgabe von BDO foresight beleuchten wir, warum Unternehmen mehr denn je gegen Bedrohungen aus dem Netz geschützt werden sollten. Ich muss ehrlich sagen, ich war bei allem Bewusstsein doch erstaunt, über welch massive Bedrohungslage wir aktuell sprechen müssen. 137.000 gemeldete Fälle von Cyber-Crime im Jahr 2022 – die Dunkelziffer soll bei über einer Million liegen. Zwei von drei Spam-Mails sind heute Teil von Cyber-Angriffen. Etwa fünf bis zehn Millionen US-Dollar Lösegeld zahlten deutsche Unternehmen im Schnitt nach erfolgreichen Attacken für verschlüsselte Daten. Das sind besorgniserregende Werte, die guten Grund bieten, sich dem Thema von verschiedenen Seiten zu nähern.

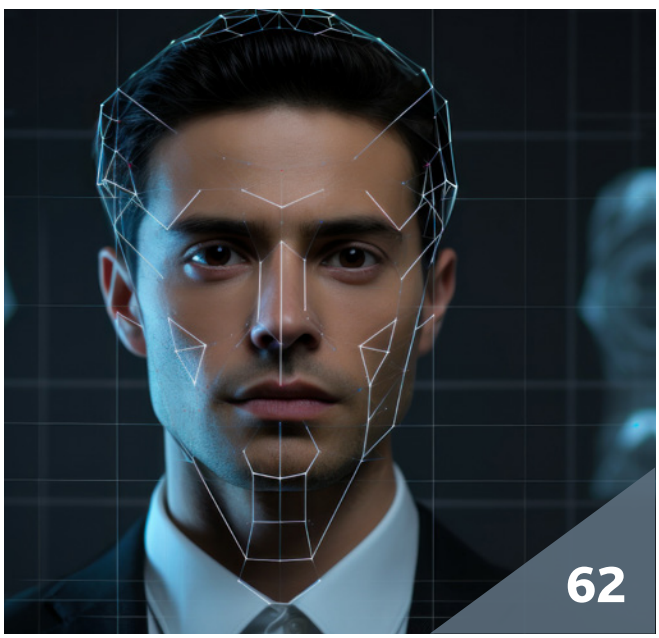
In unserer Titelstory sprechen wir mit Claudia Eckert, die zum Kreis der Cyber-Weisen gehört, darüber, wie es um die Cyber-Sicherheit in Deutschland steht. Daneben stellen wir vor, wie das Technologieunternehmen Körber es geschafft hat, zu den deutschen Pionieren in Sachen Cyber-Security zu gehören, befassen uns mit Cyber-Attacken auf die sogenannte „kritische Infrastruktur“, erfahren aus Sicht unserer Expertinnen und Experten, wie Unternehmen sich wirksam schützen können, und beleuchten die Relevanz von Cyber-Sicherheit aus der Perspektive des Accountings.

Neben einem umfassenden Blick auf unser Kernthema bietet Ihnen das BDO foresight Magazin – wie inzwischen schon gewohnt – auch in der vierten Ausgabe viele weitere Inspirationen. Zum Beispiel besuchte ich mit unserer Redaktion eines der bekanntesten deutschen Weingüter. Wir sprechen mit Winzer Markus Molitor darüber, wie er es geschafft hat, dass seine Weine in der ganzen Welt gefragt sind.

Ich wünsche Ihnen viel Spaß bei der Lektüre!

Herzlich
Ihr Parwäz Rafiqpoor

Inhalt



Staat of the Art?

Zwischen Tradition und Fortschritt: Deutschlands Ringen um digitale Souveränität und Cyber-Sicherheit

Foto: Adobe Stock

Rund eintausendmal pro Monat rauschen die Kapseln durch das 1.300 Meter lange Röhrensystem. Druckluft treibt die transparenten Zylinder voran, Röhre rauf und Röhre runter, mal links, mal rechts, bis sie in einer der insgesamt 36 Stationen ankommen, hinter den Türen rotbrauner Einbauschränke aus Holz, im Büro der Referatsleiterin, im Vorzimmer des Ostbeauftragten, im Kabinettssaal – oder beim Bundeskanzler höchstpersönlich.[1]

Anfang 2024 berichtete die Süddeutsche Zeitung, dass allem Fortschritt zum Trotz noch immer Büchsen mit wichtigen Inhalten durch das Kanzleramt in Berlin brausen. Eigentlich sollte dieses System bald Geschichte sein. Spätestens für 2025 war die Einführung der E-Akte in allen Behörden und politischen Institutionen des Landes geplant. Das Kanzleramt aber will jetzt doch noch an der guten alten Rohrpost festhalten. Die Begründung: Manche Dokumente würden der Geheimhaltung unterliegen oder müssten im Original unterschrieben werden. Sicher ist sicher?

20,9 Stunden

benötigen Unternehmen durchschnittlich, um auf einen Cyber-Angriff zu reagieren.[2]

Wenn in Zeiten der Digitalisierung selbst die Bundesregierung auf ein Informationssystem aus der Kaiserzeit setzt, kann es nicht gerade gut stehen um die Cyber-Sicherheit in Deutschland. Das belegen auch zahlreiche Studien und Statistiken. Im Jahr 2022 registrierte die Polizei in Deutschland rund 137.000 Fälle von Cyber-Crime[3] Das Bundeskriminalamt geht sogar davon aus, dass diese Zahl mit all den nicht registrierten Fällen auf fast anderthalb Millionen Fälle anwächst.[4]

Vor allem die Wirtschaft ist davon betroffen: Eine Studie des Digitalverbands Bitkom, die im September 2023 veröffentlicht wurde, offenbart, dass 72 Prozent der beinahe 1.000 befragten Unternehmen innerhalb der vergangenen zwölf Monate von IT-Ausrüstungs- oder Datendiebstahl, digitaler und analoger Industriespionage sowie Sabotage betroffen waren. 24 Prozent von ihnen mussten nach einem Cyber-Angriff ihren Betrieb komplett unterbrechen.[5] Und laut einer Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) rechneten sogar knapp zwei Drittel aller Befragten damit, in den kommenden zwölf Monaten Ziel eines Angriffs zu werden.[6] Die finanziellen Folgen sind jetzt schon enorm. Für das Jahr 2023 rechnet Bitkom auf Unternehmensseite mit einem Schaden von 206 Milliarden Euro.[7] Das entspricht fast 50 Prozent des Bundeshaushaltes für dasselbe Jahr.[8] Rund 150 Milliarden Euro davon entstanden allein durch Cyber-Attacken.[9]

Aber auch die kritische Infrastruktur kann Opfer einer Attacke werden. Das Ziel: die Wirtschaft indirekt schädigen, das soziale und gesellschaftspolitische Leben stören. Flughäfen und Bahnstrecken liegen lahm, Kraftwerke fahren runter, Notfall-OPs in Krankenhäusern finden nicht statt. Nur: Wie kann man das verhindern?

Teams-Call mit einer Expertin. Mulmiges Gefühl. Erst kürzlich haben russische Hacker einen alten Test-Account von Microsoft, dem Konzern hinter Teams, geknackt und sich so Zugang zu E-Mails ranghoher Manager verschafft.

Foto: Adobe Stock

Wer weiß schon, ob noch jemand dem Gespräch mit Claudia Eckert beiwohnt. Die 64-jährige Informatikerin ist nicht irgendjemand in der deutschen IT-Landschaft. An der Universität Darmstadt gründet sie 2008 ein eigenes Institut für IT-Sicherheit. 2011 zählt eine Fachzeitschrift Eckert zu den 100 bedeutendsten Persönlichkeiten der deutschen Informations- und Kommunikationstechnologie. 2019 wird

16 %

der deutschen Unternehmen haben ihr IT-Sicherheitsbudget während oder nach der Corona-Krise erhöht.[10]

sie als eine von nur sechs Personen in den Sachverständigenrat der Cyber-Weisen berufen. Hauptberuflich ist Eckert Leiterin des Fachgebiets Sicherheit in der Informatik an der Technischen Universität München und Leiterin des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit.

„Ein Großteil der kleinen und mittelständischen Betriebe kann die Risikolage für das eigene Unternehmen nicht bewerten."

Frau Eckert, ist so ein Teams-Call in Bezug auf Datenschutz überhaupt sicher? Eckert lacht. Sicherheit, vor allem

die im Internet, sei in Deutschland ein wichtiges Thema, das Misstrauen internationalen Technologiekonzernen gegenüber sei groß, staatlichen Institutionen gegenüber sowieso. „Gleichzeitig geben die Leute über Facebook und Instagram sehr viel über ihre Privatsphäre preis. Das ist schon etwas widersprüchlich", sagt Eckert. Und weil die Menschen so unsicher seien, wie man sich richtig verhält, würden sie häufig ein zu geringes Risikobewusstsein entwickeln, dazu einen Fatalismus, und so in ein Nichtstun verfallen. „Besonders häufig beobachte ich ein solches Verhalten bei kleineren Unternehmen. Das Ergebnis: Manche Akteurinnen und Akteure in der Wirtschaft sind sehr gut auf die Herausforderungen vorbereitet, während ein Großteil der kleinen und mittelständischen Betriebe nach wie vor überfordert ist."

Gerade die kleinen und mittleren Unternehmen trifft ein Angriff aus dem Netz besonders hart: Im Durchschnitt kostet sie ein Cyber-Angriff rund 95.000 Euro.[11] Zudem haben 38 Prozent der betroffenen Unternehmen in Deutschland Lösegeld für von Hackern erbeutete und verschlüsselte Daten bezahlt, durchschnittlich zwischen fünf und zehn Millionen US-Dollar.[12] Das kann langfristig den Ruin bedeuten.

Laut Claudia Eckert ist das föderale System in Deutschland mit seinen verzweigten und verworrenen Verantwortlichkeiten sowie widersprüchlichen Anforderungen eine große Hürde bei der Vermeidung von Sicherheitsvorfällen und deren Folgen. „Wenn ich einen Firmensitz in Bayern habe, einen Firmensitz in Nordrhein-Westfalen und dann noch ein Tochterunternehmen im Ausland, gelten überall andere Rahmenbedingungen", sagt Claudia Eckert.

„Um das Zuständigkeitswirrwarr aufzulösen, braucht es eine Sicherheitsstrategie aus einem Guss und flächendeckende Mindeststandards."

„Um das Zuständigkeitswirrwarr aufzulösen, braucht es eine Sicherheitsstrategie aus einem Guss und flächendeckende Mindeststandards", so Claudia Eckert. Sie wünscht sich den State of the Art der Technik als Must-have. Und eine Neuregelung von Zuständigkeiten, um das in der Fläche auch durchzusetzen.

Frankreich, Großbritannien, sogar Estland: Sie kenne viele Staaten, die von derartigen Zuständigkeitsstrukturen profitierten. Auch die USA, wo 2021 über einen Erlass von Präsident Joe Biden die Cyber-Sicherheit zur Chefsache erklärt wurde, seien in vielen Bereichen besser aufgestellt als Deutschland. Angesichts knapper Ressourcen könnte so eine zentrale Zuständigkeit auch in Deutschland so manches strukturelle Problem auflösen, so Eckert.

Das BSI, das Ansprechpartner für alle Fragen der IT-Sicherheit in der öffentlichen Verwaltung, bei Unternehmen und Privatpersonen ist, könnte so ein Organ sein. Aufgrund der strikten institutionellen Trennung zwischen äußerer und innerer Sicherheit darf die Bundesbehörde aber nur punktuell und über den Weg der Amtshilfe in die Sicherheitsmaßnahmen der Bundesländer eingreifen.

Foto: Adobe Stock

Claudia Eckert

„Unternehmen, die in Zukunft Geld verdienen wollen, müssen deshalb auch Geld in die Absicherung ihrer Geschäftsprozesse und Produkte investieren."

Auch die Wirtschaft brauche mehr Engagement und Willen zur Veränderung, so Eckert. „In Deutschland glaubt man immer noch, alles im eigenen Unternehmen regeln zu können." Die überwiegende Zahl der Geschäftsführerinnen und Geschäftsführer würde die Verantwortung für die IT-Sicherheit immer noch allein in den IT-Abteilungen verorten. Dabei entwickeln sich die Möglichkeiten von Hackern so rasant weiter, dass selbst Expertinnen und Experten kaum hinterherkommen. Das BSI schreibt in seinem Lagebericht 2023, dass im Berichtszeitraum täglich 250.000 neue Schadprogramme gefunden wurden, 15 Prozent davon sind kritisch.[13] „Ohne externe Hilfe und Expertise kann auf Dauer kaum ein kleineres und mittelständisches Unternehmen für das erforderliche Maß an Sicherheit sorgen", sagt Eckert. Es gebe bereits ein großes Angebot an Dienstleistungen, das von der Erstberatung bis hin zur gemanagten Sicherheit reiche. Dafür sollte man offen sein, wenn das Angebot denn vertrauenswürdig ist. „Unternehmen, die mit ihrem Kerngeschäft auch in Zukunft Geld verdienen wollen, müssen deshalb auch Geld in die Absicherung ihrer Geschäftsprozesse und Produkte investieren."

Bei den kleinsten Unternehmen müsse man noch viel früher ansetzen, sagt Claudia Eckert. „Der Fliesenleger von nebenan ist ja in den seltensten Fällen auch Cyber-Security-Profi." Sie meint damit vor allem die Betriebe mit bis zu zehn Mitarbeiterinnen und Mitarbeitern. Von den 3,4 Millionen Unternehmen in Deutschland sind das immerhin über 2,9 Millionen.[14] Für diese Betriebe sind technische Lösungen unerlässlich, um den Mangel an Fachkräften und spezifischem Know-how auszugleichen.

„Es gibt schon jetzt viele Werkzeuge oder Assistenzsysteme, die vollkommen automatisiert laufen."

Der Einsatz von künstlicher Intelligenz könne hier hilfreich sein, sagt Claudia Eckert. „Es gibt schon jetzt viele Werkzeuge oder Assistenzsysteme, die automatisiert im Hintergrund für eine grundlegende Sicherheitshygiene sorgen. Die bringen zum Beispiel Downloads erst einmal in Quarantäne und überprüfen sie dann oder unterziehen die Rechner einem Gesundheitscheck." Eine wirksame Sicherheitsmaßnahme, die Claudia Eckert hervorhebt, ist die Zwei-Faktor-Authentifizierung, die einen doppelten Identitätsnachweis erfordert: durch ein vom Nutzer festgelegtes Passwort und eine physische Karte, die beim Einloggen vorgelegt werden muss. Eine solche Karte kann nicht über das Internet abgefangen werden. „Beim Online-Banking sind wir alle bereits an diese Vorgehensweise gewöhnt. Der Aufwand hierbei ist überschaubar und gleichzeitig verhindert man so eine große Masse an gravierenden Sicherheitsproblemen, die ihren Ursprung darin haben, dass digitale Identitäten gestohlen und missbraucht werden."

5-10 Mio. US-Dollar

Lösegeld zahlen deutsche Unternehmen für verschlüsselte Daten. Im internationalen Durchschnitt werden 211.529 US-Dollar gezahlt.[15]

Ohne mehr Förderung vonseiten des Staates werde sich aber nichts bewegen. „Was kleinen und mittleren Unternehmen fehlt, sind nicht die Tipps für die letzte Meile, sondern die Tipps für die erste Meile, manchmal sogar für den ersten Meter." In Bayern gäbe es den sogenannten Digitalbonus, eine Förderung des Wirtschaftsministeriums für Digitalisierungs- und Cyber-Sicherheitsberatung. „Wenn man das im gesamten Bundesgebiet anbieten würde, könnte man mit verhältnismäßig geringen Investitionen in der Breite sehr viel erreichen", sagt Claudia Eckert. „Gezielte Hilfe zur Selbsthilfe."

„Es braucht mehr Schlüssel- und Zukunftstechnologien aus Europa – allein schon, um die technologische und wirtschaftliche Souveränität zu wahren."

Um die Wirksamkeit der zahlreichen Cyber-Sicherheitsmechanismen zu erhöhen, führe aber auch kein Weg an einheitlichen Standards und gesetzlichen Verpflichtungen vorbei – so wie die, die durch den Cyber Resilience Act

2 von 3 Spam-Mails

sind Teil von Cyber-Angriffen. 84 Prozent davon werden zur Erbeutung von Daten gebraucht.[16]

und die NIS2-Richtlinie der Europäischen Union auf den Weg gebracht wurden. Auch Cloud-Anbieter müssten in den kommenden Jahren mit strengeren Anforderungen rechnen. Das bedeute am Ende mehr Sicherheit für alle. Der Fliesenleger von nebenan müsste also immer seltener Cyber-Security-Profi sein. Wenn er seinen Mailverkehr über die zertifizierte Cloud eines professionellen Providers abwickelte, würden ihn viele infizierte Mail-Anhänge gar nicht mehr erreichen. Und selbst wenn er sich dann doch einen Virus einfinge, müsste er vielleicht seinen Rechner wegwerfen, hätte aber keine relevanten Daten verloren.

Grundsätzlich, so Claudia Eckert, brauche es aber dringend Schlüssel- und Zukunftstechnologien, die aus Europa stammten – allein schon, um die technologische und wirtschaftliche Souveränität zu wahren. Deutschland habe etliche Firmen mit hervorragenden Cyber-Sicherheitsprodukten, vor allem im Mittelstand. Auch die Forschung in Deutschland sei gut aufgestellt und könne in vielen Bereichen in der internationalen Spitzenforschung mithalten oder sogar den Ton angeben. Derzeit konzentrierten sich die Bemühungen auf die Produktion vertrauenswürdiger Elektronikkomponenten, die Etablierung kontrollierbarer Datenräume, die Zertifizierung von KI-Systemen oder Verschlüsselungstechnologien, die selbst von Quantencomputern nicht zu knacken sind. „Mit diesen Technologien haben wir eine Chance, uns im weltweiten Wettbewerb zu behaupten."

„Es ist klar, dass wir angegriffen werden. Um den Schaden zu begrenzen, sollten wir uns bestmöglich vorbereiten."

Alles, was es dazu braucht, sind Ideen, Konzepte und Lösungen, an denen möglichst viele Mitgliedstaaten, Forschungseinrichtungen oder Initiativen mitarbeiten können. Mehr Mut zur Transparenz im Zeitalter des Datenschutzes: was für ein Widerspruch. Oder etwa nicht? „Wir Deutschen müssen ein anderes Mindset etablieren", sagt Claudia Eckert. Es müsse allen bewusst sein, dass wir angegriffen würden. Um den Schaden zu begrenzen, sollten wir uns bestmöglich vorbereiten. „Technische Maßnahmen wie Kontrolle, Isolierung und Verschlüsselung sind entscheidend für Cyber-Sicherheit, ebenso wie Notfallpläne und Back-up-Strategien. Gleichzeitig ist es wichtig, zugängliche Aus- und Weiterbildungsangebote bereitzustellen, die Menschen im Umgang mit digitalen Technologien im Alltag und Berufsleben unterstützen."

Eins ist klar nach diesem Gespräch: Wenn Deutschland ist Sachen Cyber-Sicherheit so weitermacht wie bisher, sieht es düster aus, sehr düster. Blackout.

Vor allem muss die ganze Breite der Gesellschaft für dieses Problem sensibilisiert werden: Einzelpersonen, Unternehmen, Kommunen, aber auch die Bundespolitik. Für den Zugang zum Bundestagsnetz muss man zum Beispiel immer noch alle sechs Monate das Passwort wechseln, obwohl das längst keine empfohlene Praxis mehr ist. Je öfter man nämlich Passwörter wechselt, desto leichter sind sie auch zu knacken. Dann doch lieber weniger und umso stärkere Passwörter. Manche Standards sind aber anscheinend im Kanzleramt noch nicht etabliert. Der Staat, so scheint es, ist alles andere als State of the Art. LS

137.000 Fälle

von Cyber-Crime registrierte die deutsche Polizei im Jahr 2022. Die Zahl der nicht registrierten Angriffe soll neunmal so hoch sein.[17]

Wer es genauer wissen will: Quellenangaben siehe Seite 78

Up to Data

Die digitale Transformation meistern: Körbers Pionierarbeit in der Cyber-Sicherheit

In Deutschland gibt es nur wenige Unternehmen, die ganz vorn mitspielen in Sachen Cyber-Sicherheit. Der Technologiekonzern Körber zählt dazu. Wie man einem Traditionsunternehmen ein funktionierendes Update verpasst.

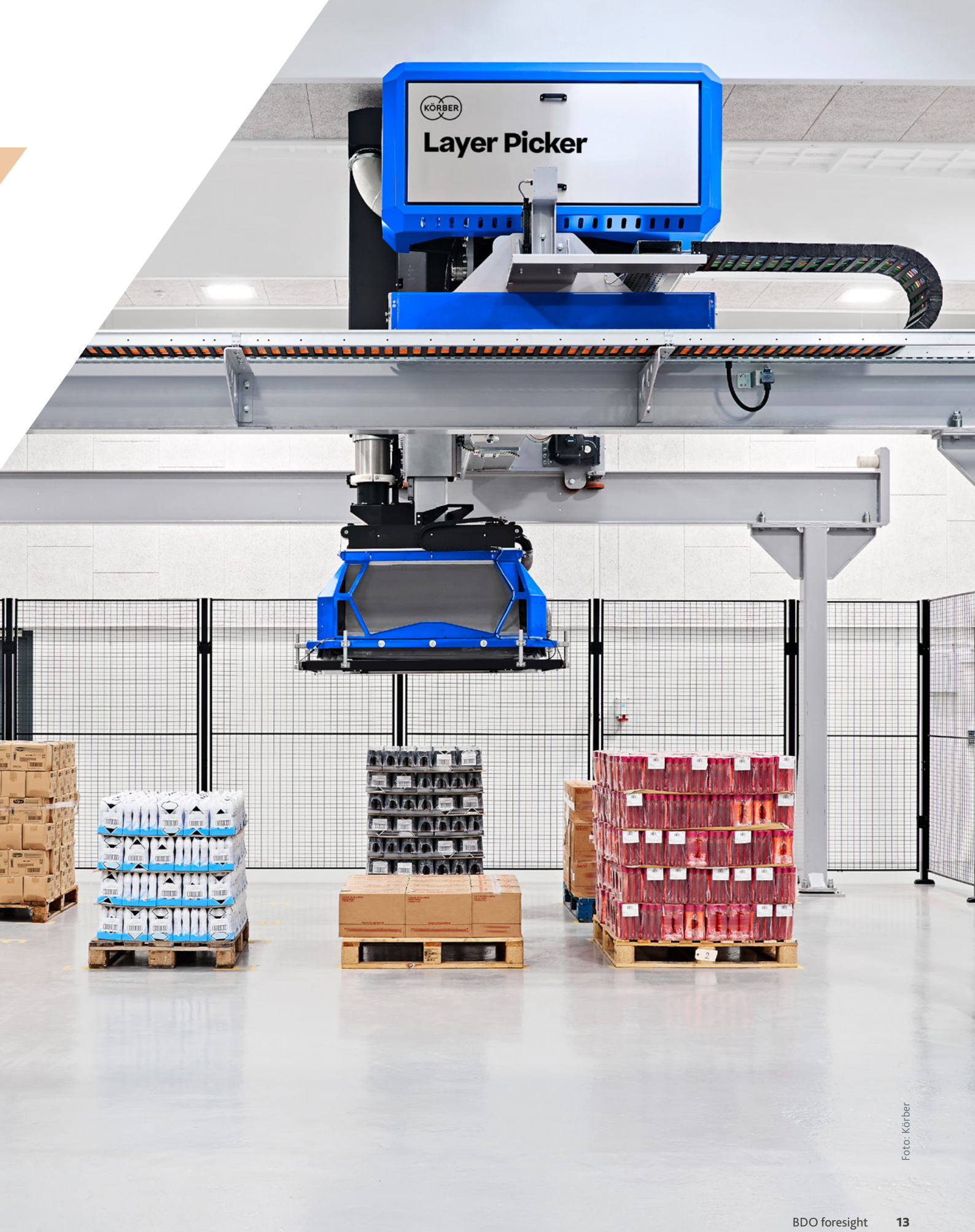


Foto: Körber

Foto: Körber

Die E-Mail, die Jan-Christian Kaiser anklickte, sah aus wie einer dieser Zahlungsbenachrichtigungen von PayPal. Nur eine Millisekunde dachte er nicht nach. Dann ging es ganz schnell: Neues Fenster öffnet sich, danach Kontakt mit der IT, dann durchatmen: ein interner Phishing-Test, den sein Arbeitgeber damals schon durchführte. Ein Glück. Der junge Mann kam gerade frisch von der Uni. Es war sein erster Job, gleich bei einer bekannten Unternehmensberatung – und dann auch noch im Bereich Informationssicherheit.

Heute würde Jan-Christian Kaiser so ein Fauxpas nicht mehr passieren. Aber es ist ein Erlebnis, das hängengeblieben ist – und inzwischen einen wertvollen Beitrag zu seiner Arbeit leistet. Mittlerweile ist Kaiser Head of Security Governance beim internationalen Körber-Konzern. Hier kümmert er sich um alle strategischen Aspekte der Cyber-Sicherheit. „Natürlich war das Thema auch schon vor 20 Jahren relevant für unser Unternehmen. In den letzten Jahren hat sich die Bedrohungslage aber verschärft. Und in zehn Jahren wird das Problem noch viel größer sein. Bei Körber wollen wir dem vorbeugen."

> IN ZEHN JAHREN WIRD DIE BEDROHUNGSLAGE NOCH VIEL GRÖSSER SEIN.

Vom Kellerstart zum Global Player: Körbers Evolution

Körber, gegründet 1946, ist als Maschinenbauunternehmen bekannt geworden. In einem Kellerraum im Hamburger Stadtteil Bergedorf fing alles an, ein kleines Stück die Elbe hoch. Hier machte Tüftler Kurt A. Körber schrottreife Zigarettenmaschinen wieder flott. 1956 erfand er seine eigene Anlage, die Filteransetzmaschine Max, mit der er Zigarettenhersteller in aller Welt ausrüstete – der internationale Durchbruch. Kurt A. Körber versteht es schon früh, unternehmerische Potenziale zu erkennen und außerhalb seines Gründungsgeschäfts aktiv zu werden – zunächst durch den Zukauf von Firmen aus der Papierverarbeitungs- und Werkzeugmaschinenbranche. Auch die Bereiche Pharma und Logistik gehören mit der Zeit zum Unternehmensportfolio. Inzwischen zählt der Konzern weltweit 100 Produktions-, Service- und Vertriebsstandorte und mehr als 12.000 Mitarbeiterinnen und Mitarbeiter. Im Geschäftsjahr 2022 lag der Umsatz bei rund 2,5 Milliarden Euro. Der Hauptsitz befindet sich nun mitten in der Hamburger City, in einem bogenförmigen Gebäude aus Glas.

Körber baut Hightech-Maschinen, deren Sensoren Ampullen mit Krebsmedikamenten, Corona-Impfstoffen oder Wirkstoffen gegen Multiple Sklerose auf Fremdpartikel und Produktionsfehler untersuchen können. Körber liefert Software-Lösungen für autonome mobile Roboter, die vollautomatisch durch Lager sausen und brausen, eigenständig schieben, ziehen, hieven, fahren. Körber bietet seinen Kundinnen und Kunden auch immer mehr digitale Services, die von einer künstlichen Intelligenz unterstützt werden und die das Personal an den Maschinen bei seiner Arbeit unterstützt. So muss man sich nicht mehr auf ein Bauchgefühl oder jahrelange Erfahrung verlassen, und teure Stillstandszeit von Maschinen und Anlagen wird minimiert. Über KI werden

direkt die fünf Parameter vorgegeben, die wirklich in der jeweiligen Situation relevant sind – und die KI fragt dann sogar noch nach einer Erklärung, wenn der Operator ihre Tipps ablehnt.

Die Digitalisierung hat aus dem traditionsreichen Maschinenbauer einen globalen Technologiekonzern gemacht. Und der Wandel geht weiter. Bis 2025 soll jedes Geschäftsfeld von Körber zwischen 25 und 30 Prozent des Umsatzes mit Softwarelösungen und digitalen Produkten erwirtschaften. Das Potenzial ist enorm, die Nachfrage auch. Doch die Entwicklung bringt auch viele Risiken mit sich. Je smarter die Fabriken sind und je vernetzter das Unternehmen ist, umso größer ist das Risiko für eine Cyber-Attacke, die gewaltigen Schaden hinterlassen kann.

Bei Körber habe man die Zeichen der Zeit zum Glück früh genug erkannt, erzählt Jan-Christian Kaiser. 2019, Kaiser ist erst kurz im Konzern tätig, trifft es ein anderes Unternehmen aus der Region. Das Unternehmen ist in einem ähnlichen Bereich tätig wie Körber, man kennt sich gut, arbeitet oft und eng zusammen. Der Name tue hier nichts zur Sache, sagt Kaiser. Aber der Cyber-Angriff sei erheblich gewesen, der Schaden groß. „Das hat vielen bei Körber zu denken gegeben, vor allem dem Vorstand." Seitdem wurden große Summen in Entwicklung und Etablierung effektiver Sicherheitsmaßnahmen investiert, nicht bloß in Verschlüsselungstools und Firewalls und regelmäßige Software-Updates.

Auf Nummer sicher gehen

Im Corona-Sommer 2020, als das flächendeckende Homeoffice die Angriffsmöglichkeiten für Hacker plötzlich um ein Vielfaches potenziert, baut Körber in der portugiesischen Hafenstadt Porto ein eigenes Cyber Defence Center (CDC) auf. „Die traditionellen Sicherheitsdienstleister arbeiten oft nur die Alarmmeldungen des Systems ab. Diese reaktiven Maßnahmen reichen heute nicht mehr aus", erklärt Jan-Christian Kaiser. „Deshalb beobachten wir die Entwicklungen im Netz proaktiv und kontinuierlich und versuchen, mögliche Cyber-Angriffe vorherzusehen und so zu verhindern."

> WIR VERSUCHEN, MÖGLICHE CYBER-ANGRIFFE VORHERZUSEHEN UND SO ZU VERHINDERN.

Das CDC-Team würde sich zum Beispiel mit folgenden Fragen beschäftigen: Welche Schadsoftware ist gerade besonders aktiv? Verschicken die Hacker ihre E-Mails von bestimmten Servern? Nutzen sie einen spezifischen Typ von Computerviren und -würmern oder Trojanern, die sich unbemerkt einschleichen? Gibt es vielleicht schon Systeme im eigenen Haus, die davon bereits betroffen sind? „Wenn wir das alles wissen, können wir diese Angriffe gleich in unseren Eingangskanälen blocken", erklärt Kaiser. Jede Woche bespricht das Team die aktuelle Sicherheitslage, bewertet sie aufs Neue, passt die Sicherheitsmaßnahmen entsprechend an. Und wenn es wirklich mal zu einem Sicherheitsvorfall kommt, werde dieser ganz genau untersucht.

Jan-Christian Kaiser, Head of Security Governance bei Körber

Foto: Körber

So wie im Sommer 2023. Das Unternehmen Progress veröffentlichte eine Schwachstelle in ihrer Software „MOVEit", die zu diesem Zeitpunkt bereits aktiv von Angreiferinnen und Angreifern ausgenutzt wurde. Die Clop Ransomware-Gang veröffentlichte eine Liste mit mehr als 260 Organisationen, von denen sie angeblich Daten erbeutet hatte. Neben Konzernen wie Sony, Shell und Siemens, dem US-Energieministerium, Kreditinstituten wie Deutsche Bank, Comdirect und ING, Krankenkassen wie AOK und BARMER stand auch der Bereich Software des Körber-Geschäftsfelds Pharma auf der Liste. „Eine penible Analyse solcher Vorfälle gibt Hinweise darauf, ob und auf welche Daten Angreiferinnen und Angreifer Zugriff hatten und ob sie eventuell eine Hintertür eingebaut haben."

Weil viele firmenbezogene Daten inzwischen oft in Drittsystemen wie einer Cloud abgespeichert sind, muss man auch diese Systeme in das Sicherheitskonzept des Unternehmens einbeziehen, sie überwachen und vorhandene Risiken identifizieren – und zwar geschäftsfeldübergreifend. Eine Menge Aufwand – der sich aber lohnt. „Das Cyber Defense Center steigert nicht direkt unseren Umsatz", sagt Jan-Christian Kaiser. „Es leistet aber einen positiven Beitrag zur Entscheidungsfindung bei Kundinnen und Kunden. Am Ende des Tages geht es darum, dass Körber ein vertrauenswürdiger Partner bleibt. Unsere Aktivitäten im Bereich Cyber-Sicherheit – wie das CDC – tragen dazu bei, dass wir auch langfristig erfolgreich sind."

Weil die technologischen Sprünge immer größer, immer schneller werden, vor allem im Bereich der künstlichen Intelligenz, gibt man sich bei Körber nicht damit zufrieden.

Im Bereich Sicherheit setzt man verstärkt auf Automatisierung, insbesondere in Form von KI-gestützten Tools. Sei es bei der Absicherung von Laptops, Handys und Tablets oder beim Schutz von E-Mail-Programmen und Datenautobahnen, überall helfen moderne Sicherheitstechnologien Angriffe zu erkennen und abzuwehren. „Wir sind in einem stetigen Wettrennen mit Kriminellen. Auch sie nutzen neueste Technologien und nur durch Automatisierung können wir bei wirklich kritischen Fällen schnellstmöglich reagieren", erzählt Jan-Christian Kaiser. „In unserem Outlook gibt es inzwischen auch einen Button, mit dem man verdächtige E-Mails vollkommen automatisiert prüfen lassen kann."

Ein Mix aus Mensch und Maschine

Trotz aller Innovationsfreude: Bei Körber halte man es für sinnvoll, die Erkenntnisse aus dem Machine Learning mit menschlicher Erfahrung zu kombinieren. „Am Ende des Tages braucht es noch oft einen Menschen, der die Masse an Daten interpretiert. Manchmal lässt sich nur so das Muster einer Angreiferin oder eines Angreifers erkennen."

Das internationale Cyber-Security-Team hat dabei eine große Bedeutung. „Hier sitzen Leute, die sich wirklich in eine Hackerin oder einen Hacker hineinversetzen können und die in der Lage sind, Angriffsszenarien möglichst realitätsnah zu erproben, unsere Abwehrmaßnahmen wirklich auf Herz und Nieren zu prüfen", erzählt Kaiser. Neue Software-Applikationen würden zum Beispiel noch während der Entwicklung systematisch auf Sicherheitslücken getestet, manchmal auch von externen Expertinnen und Experten. Offenheit und Transparenz wagen, zumindest bis zu einem gewissen Grad, das sei sehr wichtig, sagt Kaiser. Große Unternehmen wie Microsoft hätten sogar ein sogenanntes Bug-Bounty-Programm, bei dem Hackerinnen und Hacker eine Art Kopfgeld ausgezahlt bekommen, wenn sie Schwachstellen aufspüren. „Einfach die Schotten dicht machen: So funktioniert Cyber-Sicherheit nicht mehr", erklärt Jan-Christian Kaiser.

> EINFACH DIE SCHOTTEN DICHT MACHEN: SO FUNKTIONIERT CYBER-SICHERHEIT NICHT MEHR.

Man dürfe sich aber nicht der Illusion aussetzen, dass die Technik alle Probleme löse. Der beste Schutz nütze nichts, wenn eine einzige Person einem schädlichen Link folge. „So abgedroschen das klingen mag: Die Mitarbeiterinnen und Mitarbeiter sind die first line of defense." Aber: Das Thema Cyber-Security bekomme in vielen Unternehmen zu wenig Aufmerksamkeit.

Körber hat sich deshalb dazu entschlossen, die eigenen Mitarbeiterinnen und Mitarbeiter intensiv zu schulen und selbst zu Sicherheitsbotschafterinnen und -botschaftern zu machen, ob Finanzvorstand, Personalreferentin oder Mitarbeiter in der Produktion. In internen Awareness-Kampagnen geben sie dem Thema ein Gesicht, machen es nahbar, greifbar.

Ergänzt werden diese Kampagnen unter anderem durch einen Security-Newsletter mit kurzen, einfachen Wissenshappen aus dem Arbeitsalltag. In regelmäßigen Abständen veranstaltet Körber eine Cyber Security-Week, bei der in einer Reihe von Vorträgen und interaktiven Live Hacking Sessions unterschiedliche Teilaspekte beleuchtet werden. „Nur, wenn wir die Themen oft wiederholen und erlebbar machen, setzen sich unsere Mitarbeiterinnen und Mitarbeiter auch wirklich damit auseinander und bauen ein Verständnis dafür auf", sagt Jan-Christian Kaiser. „Das ist viel effektiver als irgendeine überladene Fortbildung, von der nur ein Bruchteil hängen bleibt."

Natürlich sei bei manchen die Verunsicherung noch groß, sagt Jan-Christian Kaiser. Und, klar, die zahlreichen Rückfragen bedeuteten einen großen Arbeitsaufwand. Aber genau das wolle seine Abteilung ja auch forcieren: lieber auf Nummer sicher gehen. „Man muss wirklich wachsam sein, jeden Tag, bei jeder E-Mail – auch oder gerade, wenn das Postfach überquillt." LS

Foto: Körber

„Ich gehöre zu den Guten!“ – Motive eines Hackers

Woher kommen die Angriffe aus dem Netz? Wer steckt dahinter? Und was treibt Menschen an, Unternehmen anzugreifen? Auf einen Kaffee mit einem White-Hat-Hacker

Foto: Adobe Stock

Es ist richtig kalt in Hamburg. Jeder Atemstoß wird zur kleinen Wolke, der Morgenreif glitzert auf dem Kopfsteinpflaster im Hamburger Oberhafen. Eifrig entladen zwei Handwerkerinnen einen Lastwagen voll Sperrholz. Die renovierten Warenhallen des stillgelegten Güterbahnhofs beherbergen heute Künstlerinnen oder Architekten, auch Design-Agenturen haben sich hier niedergelassen – und die Hobenköök, ein Restaurant mit eigener Markthalle für regionale Produkte.

Hier sind wir mit Pascal verabredet, dessen Namen wir geändert haben. Er ist bereits eine Viertelstunde zu spät. Über einen verschlüsselten Messenger-Dienst fragen wir, ob das Treffen noch zustande kommt. Er schreibt: „Ich bin schon in der Nähe." Kurz darauf betritt ein kleiner Mann den Oberhafen, Funktionsjacke, Schnurrbart, Bügelkopfhörer. Er wirkt unsicher, geht zunächst an uns vorbei, wirft uns nur einen schnellen prüfenden Blick zurück über die Schulter zu. „Pascal, bist du es?" Er richtet sich auf, kommt mit ausgestreckter Hand und einem Lächeln auf uns zu. Er antwortet: „Ja! Ich bins!". Wir lassen uns zum Kaffee in einer einsamen Ecke des Restaurants nieder.

„Cyber-Kriminalität ist ein Milliardengeschäft"

Pascal ist professioneller Penetration-Tester und IT-Sicherheitsberater in Festanstellung. Er lebt in Hamburg, hat ein geregeltes Einkommen und ein gepflegtes LinkedIn-Profil. Eigentlich wollen wir mit ihm über das Geschäft reden, etwas Licht ins Dark-net bringen und aufräumen mit Stereotypen. Denn Pascal wirkt auf uns wie der Gegenentwurf zum ewig studierenden Nerd im Hoodie, wie er so oft von den Medien nachgezeichnet wird. Doch der 31-Jährige wirkt unsicher, er behält seine Jacke erst mal an. Noch bevor uns der Kaffee und die Karaffe mit Wasser erreichen, sagt er, dass er eigentlich nicht mit der Presse sprechen darf. Zumindest nicht „über die eine Sache".

„Cyber-Kriminalität ist real! Es ist längst ein Milliardengeschäft und die Basis unzähliger Verbrechen. Es gibt Cyber-Wars, Heerscharen von Menschen, die zum Teil versklavt werden, um über Landesgrenzen hinweg Attacken durchzuführen", sagt er und nimmt einen Schluck Wasser. Und Pascal sei seit Neuestem mittendrin. „Ich war zur falschen Zeit am falschen Ort im Internet – es hätte jedem anderen Hacker auch passieren können!", sagt er zur Einordnung. Es gehe um internationale Ermittlungen gegen die Organisierte Kriminalität in Asien, weiter möchte er darauf nicht eingehen. Die Polizei habe ihm geraten, bis auf Weiteres zu schweigen. Wir bieten an, unser Smartphone auszuschalten. „Dann ist es noch lange nicht aus", sagt er.

Er blickt auf das ausgedruckte Schaubild zur Taxonomie von Cyber-Risks, das wir auf den Tisch gelegt haben. Wir geben ihm einen Kuli in die Hand. Auf dem Zettel mit der Hosentaschen-Faltung stehen ein paar Oberkategorien wie Threat, Vulnerability, Attack und Control. Darunter einsortiert sind zig Angriffspunkte und Techniken wie Encryption, SQL Injection oder Botnet. Pascal braucht nicht lange, um die Grafik zu durchdringen. Er erkennt die Offense- und Defense-Themen – und kringelt die Bereiche Hashing und APT als seine Stärken ein, also Advanced Persistent Threats. Laut dem Bundesministerium für Sicherheits- und Informationstechnik liegt ein APT vor, „wenn gut ausgebildete, typischerweise staatlich gesteuerte Angreiferinnen und Angreifer zum Zweck der Spionage oder Sabotage über einen längeren Zeitraum hinweg sehr gezielt ein Netz oder System angreifen, sich unter Umständen darin bewegen oder ausbreiten und so Informationen sammeln oder Manipulationen vornehmen". Pascal hackt sich beruflich in Unter-

nehmen ein. Meistens in deren Auftrag, aber nicht immer. „Ich greife Unternehmen an, um sie auf ihre Sicherheitslücken hinzuweisen, nicht, um sie zu erpressen“, sagt er.

Aufbruch in ein sicheres Land – um Sicherheit zu studieren

Der gebürtige Moldawier bekommt mit zehn Jahren seinen ersten Computer und wird schnell zum netten Nachbarn, der einem das neue Windows installieren – oder ein Local-Area-Netzwerk aufsetzen kann, wie er sagt. Er gilt als begabt, besucht sogar eine Förderschule „for gifted children“, erzählt er uns, mit Bestnoten in Mathe, Physik und Informatik. Doch nicht alles ist so einfach. Pascal wird zusammen mit seinem Bruder bei der Mutter groß. Zum Vater gibt es keinen Kontakt mehr. Seit dem Transnistrien-Konflikt und dem Eingriff Russlands gilt Moldawien als instabiles Land, „Ich glaube bis heute nicht, dass unser Land eine Zukunft hat“, sagt Pascal. Er verlässt damals das Land nach der Schule, erarbeitet sich noch das IT-Zertifikat CompTIA A+, dann macht er sich auf den Weg.

Dank seiner zweiten, rumänischen Staatsangehörigkeit kommt Pascal als EU-Bürger nach Hamburg. Seine Mutter und seinen Bruder lässt er mit dem festen Plan zurück, sie nachzuholen. Pascal beginnt, Information-Engineering zu studieren. Doch das ist ihm schnell zu Hardware-lastig und zu viel Elektronik. „Ich wollte lieber etwas über IT-Sicherheit lernen“, sagt er. Pascal bricht das Studium ab. Auch ein zweiter Anlauf, diesmal der Studiengang „System- und Software Entwicklung“ scheitert, denn das Studium wird nur auf Deutsch angeboten und die Gruppen sind viel zu groß, wie Pascal sagt. Er macht weitere IT-Zertifikate, zum Certified Network Analyst und zum Offensive Security Certified sowie Wireless Professional. Finanziell hält er sich mit Nebenjobs über Wasser, unter anderem arbeitet er für eine IT-Zeitschrift, einen Online-Übersetzungsservice oder einen Buchhandel. Dann sorgt er das erste Mal für Aufsehen. „Im Auftrag der Zeitschrift habe ich die Fotoautomaten einer Drogeriekette gehackt und mir so Zugang zu Nutzerdaten und Bildern verschafft – mit einem Raspberry Pi Einplatinencomputer und einem Teensy Arduino Microcontroller samt Wifi-Adapter“, sagt er und lächelt. Sein erster Angriff, über den sogar in großen Tagesmedien berichtet wird. Das Interesse der Headhunter ist geweckt – denn wer hacken kann, ist auch interessant für die Cyber-Security.

Foto: Adobe Stock

Die ersten Angriffe für die Reputation

Auch ohne Studium und verhandlungssichere Deutschkenntnisse sicherte sich Pascal schnell die erste Festanstellung. Und die wird zum nächsten Sprungbrett. Als IT-Sicherheitsbeauftragter eines Hamburger Mobilitätsanbieters entdeckt er eine Zero-Day-Lücke im „Spring Boot Framework“, während er ein Authentifizierungsprotokoll implementiert. Das ist ein Java-Open-Source-Webframework, das auf Microservices basiert und besonders für Softwareentwickler geeignet ist, die Web-Apps und Microservices entwickeln. „Es war möglich, die gesamte Authentifizierung zu umgehen, indem das Passwort ‚null‘ verwendet wurde!“, erklärt Pascal. Die Tragweite des Fehlers wird durch die US-amerikanische Regierungswebsite ‚National Vulnerability Database‘ (NVD) verdeutlicht, die den von Pascal entdeckten Fehler mit einem hohen Risiko und einer Bewertung von 7,3 von maximal 10 möglichen Risikopunkten einstuft.

Die Gratwanderung: White or Black Hat?

Pascals Entdeckung wirft ein Schlaglicht auf die zerbrechlichen Ränder unserer digitalen Infrastruktur – und erinnert an den Angriff auf das Netzwerkmanagement-Tool „Kaseya“ im Jahr 2021. Die Ransomware-Gruppe REvil nutzt eine ähnliche Schwachstelle, um – nach eigener Aussage – mehr als eine Million fremde Systeme zu verschlüsseln. Sie fordert anfänglich ein Lösegeld von 70 Millionen US-Dollar, um einen universellen Entschlüsselungscode

Foto: Adobe Stock

bereitzustellen, der alle betroffenen Systeme freischalten kann. Der digitale Erpressungsversuch hält die Geschäftswelt mitten in der Corona-Pandemie weltweit in Atem.

Auch Pascal könnte entscheiden, die gefundene Zero-Day-Lücke auszunutzen. Doch die Frage stellt er sich gar nicht. „Ich gehöre zu den Guten! Ich habe mich entschieden, die weiße Mütze zu tragen", sagt er. Während sogenannte White-Hat-Hacker ihre Fähigkeiten für ethische Zwecke einsetzen, zum Beispiel um Sicherheitssysteme zu testen und zu verbessern, nutzen Black-Hat-Hacker ihr Wissen für illegale oder schädliche Aktivitäten. Sie dringen in Systeme ein, stehlen Daten, verbreiten Malware, begehen Betrug oder verursachen vorsätzlich Schäden. Ihr Hauptantrieb ist oft die persönliche Bereicherung, die Verursachung von Schaden oder das Stiften von Chaos – im Gegensatz zu White-Hat-Hackern, die darauf abzielen, zur Sicherheit im Cyber-Space beizutragen.

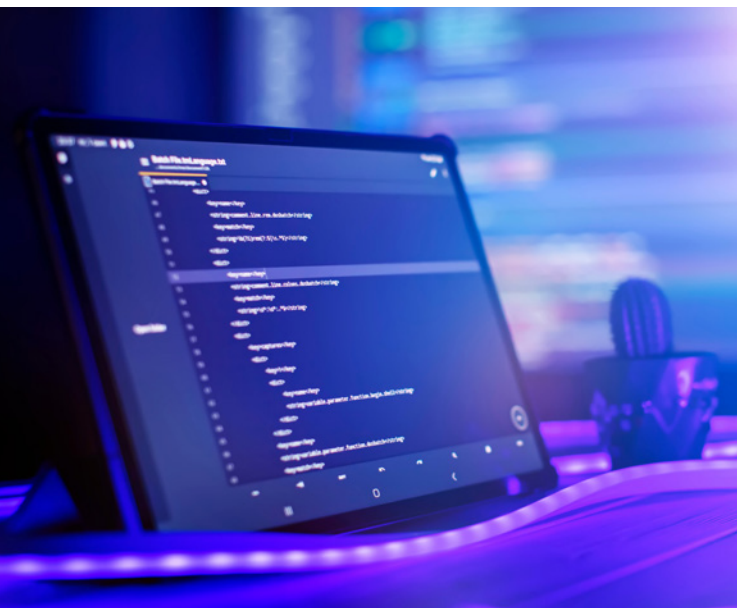


Foto: Adobe Stock

Das Motiv Menschlichkeit

Wir sprechen nun schon eine halbe Stunde, und er scheint Vertrauen zu uns aufzubauen. Er zieht seine Jacke aus und legt sie über die Stuhllehne. Dann hält er einen Moment inne. Sein Smartphone, das mit dem Display nach unten auf dem Tisch liegt, vibriert kurz. Die Marke ist für uns nicht direkt erkennbar. Auf unsere Nachfrage hin erzählt er, es sei ein OnePlus-Smartphone mit einem eigens aufgesetzten Android-System. In Deutschland ist das Gerät wegen eines Patentstreits nicht mehr erhältlich. „Als Hacker brauchst du neben einer Offense- immer auch eine Defense-Strategie", sagt Pascal. Darin steckt eine gewisse Ambivalenz, denn gute Sicherheitsexpertinnen und -experten müssen heute mit ähnlichen Fähigkeiten und Fertigkeiten ausgestattet sein wie kriminelle Angreiferinnen oder Angreifer. Pascals Philosophie: Zero Trust! Er vertraut keinem System, das er nicht selbst aufgesetzt hat. „Ich hoste meine eigene Cloud zur familieninternen Ablage von Dokumenten für meinen Bruder, meine Mutter und mich", sagt er.

Pascal, ein Hacker mit einer Vergangenheit, die sowohl Bewunderung als auch Misstrauen hervorruft, gewährt uns einen seltenen Einblick in seine Welt. In einer oft missverstandenen Branche wird seine Arbeit von einem feinen moralischen Kompass geleitet, der ihn deutlich von jenen abgrenzt, die ihre Fertigkeiten zu schädlichen Zwecken missbrauchen. Seine Motivation, Unternehmen anzugreifen, ist klar definiert: Es ist eine Art digitaler Altruismus – er möchte Schwachstellen aufdecken, bevor sie von böswilligen Akteurinnen und Akteuren ausgenutzt werden können. „Ich kann die Schwachstellen nicht übersehen", sagt er und erzählt von einem mehrwöchigen Krankenhausaufenthalt. Pascal ist an das Bett gefesselt und starrt auf das kleine Infotainment-System an der Bettkante. „Ich fixierte das Display und sah mir eine Sendung an, die gestreamt war – offensichtlich ein möglicher Angriffspunkt!" Vom Bett aus dringt Pascal über die virtuelle Tastatur des Geräts ins Krankenhausnetz ein. Vor ihm liegt nun der Zugang zu kritischer Infrastruktur. Pascal informiert die Krankenhausleitung per E-Mail über die Sicherheitslücke, doch erhält nie eine Antwort. „Vermutlich haben die das für Spam gehalten!", sagt er. Ob die Lücke geschlossen wurde? Pascal zuckt mit den Schultern.

Als wir uns zum Abschied erheben, rückt er seinen Stuhl behutsam an den Tisch und lässt sein Smartphone in die Jackeninnentasche gleiten. „Vielleicht hilft es", beginnt er noch einmal, „nicht alle Hacker als Kriminelle abzutun!" Er schaut uns direkt an, seine Stimme ist bestimmt, aber ruhig, als wolle er zum Abschluss eine Brücke zwischen den Welten bauen. „Dein nächstes Ziel?", fragen wir auf dem Weg nach draußen. „Ich weiß es noch nicht. Doch ich habe gerade meinen Einbürgerungstest gemacht – ich möchte die deutsche Staatsbürgerschaft beantragen", sagt er, „für ein bisschen mehr Sicherheit!" Er muss lächeln. Dann zieht er den Reißverschluss hoch bis zum Kinn, schwingt seinen Rucksack auf und verschwindet zwischen den parkenden Autos im Oberhafen. MB

Der Umbau von HRS ist ein Management-Lehrstück. Mit Innovationsgeist hat Tobias Ragge aus der väterlichen Hotelbuchungsagentur ein Traveltech-Unternehmen geformt. Es florierte – bis Corona grassierte. Dann hat Tobias Ragge alles infrage und vieles auf den Kopf gestellt.

„Du musst hier was Neues bauen, um global zu gewinnen“

Foto: Adobe Stock

So, wie der OTTO Versand mit einem dicken Katalog einst bequemes Einkaufen von zu Hause ermöglichte, hat der Hotelanbieter HRS das Suchen und Buchen von Hotels vereinfacht. Lang ists her. Weit weg. Welten, ach was, Galaxien. Die HRS Group ist heute, genauso wie die Otto Group, ein Tech-Unternehmen. Stets begierig auf Innovation.

Für diesen rasanten Wandel steht Tobias Ragge, Geschäftsführender Gesellschafter und CEO der HRS Group. Er hat vom Vater, der die analoge Reiseagentur in den Siebzigern gründete, 2010 im Alter von 34 Jahren ein einfaches E-Commerce-Unternehmen übernommen. Doch Ragge war und ist ambitioniert, will Vorreiter der Branche sein. Dafür krempelte er HRS gewaltig um. Er entwickelte neue Geschäftsfelder, veränderte die gesamte Tektonik, formte eine Gruppe von Unternehmen, die alle auf Travel Technology basieren, aber unterschiedliche Zielgruppen ansprechen. Und wirtschaftlich eigenständig agieren. „Wofür wir heute stehen? Make business life better", sagt Tobias Ragge, CEO der HRS Group.

Evolution und Revolution

Das Portalgeschäft für individuell buchende Geschäftsreisende gibt es noch. Aber es spielt inzwischen eine untergeordnete Rolle. Das größte Geschäftsfeld, Enterprise Solutions, beschäftigt sich mit End-to-End-Lösungen rund um Geschäftsreisen, kompletten Prozessketten für Großkonzerne – von A wie Allianz bis Z wie Zalando. Diesen großen multinationalen Playern geht es um Prozessvereinfachungen, und HRS bietet sie: durch individuelle Plattformen, Procure-to-Pay-Lösungen, Automation. Auch den CO_2-Fußabdruck eines Hotelaufenthalts ermittelt HRS für seine Kundinnen und Kunden mittlerweile. Ragge: „Unsere Kundinnen und Kunden können mit besseren Daten bessere Entscheidungen treffen, aber auch Kosten reduzieren und Anforderungen einfacher managen – beispielsweise beim Lieferkettengesetz und in der Nachhaltigkeit."

Auch hinter Booking und Airbnb steckt HRS

Das Geschäftsfeld Destination Solutions hält darüber hinaus Technologie für die Vermarkter von 60.000 Ferienhäusern und -wohnungen bereit, die die gesamte Verwaltung ihres Inventars über die HRS-Plattform abwickeln. Egal, ob Kundinnen und Kunden bei Booking oder Airbnb buchen, hinter dem ganzen Channel Management steckt HRS.

Zehn Fokusmärkte weltweit hat das in Köln ansässige Unternehmen, entsprechend unter anderem auch Offices in Australien, Brasilien, China, Indien, Japan und den USA. 150 Mitarbeiterinnen und Mitarbeiter waren es 2012, inzwischen sind es knapp 900. Über Umsatz und Gewinn schweigt sich Tobias Ragge aus. Aber er gibt im foresight-Interview Einblicke, warum er überzeugt ist, dass ein Unternehmen technologisch und strategisch immer wieder neu gedacht werden muss. Und er erzählt, wie erfinderisch HRS die Pandemie überlebte, die „wie ein Tsunami" eingeschlagen hatte.

HRS im Wandel der Zeit: von der analogen Reiseagentur zum großen Software-as-a-Service-Unternehmen.

Foto: HRS

Foto: HRS

Herr Ragge, wie oft haben Sie HRS schon neu erfunden, seit Sie 2010 von Ihrem Vater die Geschäftsführung übernommen haben?

Bei Innovationen gibt es selten Start- und Endpunkte. Letztlich befinden wir uns in einer Dauertransformation. Wir waren mal ein klassisches E-Commerce-Unternehmen, dessen Geschäft sehr viel lokaler war. Heute sind wir ein Software-as-a-Service-Unternehmen mit klarem B2B-Schwerpunkt, das global ausgerichtet ist. Auf diesem Weg gab es sehr viele Umbrüche, die aber alle nicht auf dem Reißbrett entstanden sind.

Haben Sie die Chancen der Innovation mit scharfem Blick erkannt oder passierten Umbrüche auch mehr oder weniger aus der Not heraus?

Ich glaube, den initialen Impuls gab die frühzeitige Erkenntnis, dass das Geschäft meines Vaters, das ich übernommen habe, zwar sicherlich noch viele Jahre gutes Geld verdienen kann, aber am Ende nicht global gewinnen wird. Ich sah, dass es im E-Commerce starke Netzwerkeffekte gibt und es irgendwann auf „The winner takes it all" hinausläuft. Deshalb sagte ich mir: Du musst hier was Neues bauen, was die Chance hat, global zu gewinnen. Aber um ehrlich zu sein: Wie das B2B-Geschäft funktioniert, welche Fähigkeiten es dafür braucht, davon hatte ich keine Ahnung. Was ich hatte, war eine Menge Enthusiasmus und den Willen, das anzu-gehen. So haben wir HRS Schritt für Schritt zu einem Technologieunternehmen transformiert.

Und dann kam im März 2020 Corona und hat alles infrage gestellt.

Wir haben binnen einer Woche 80 Prozent unseres Umsatzes verloren, das war existenzbedrohend. In einer Art Überlebensinstinkt haben wir auf die Schnelle Liquidität gesichert und Kosten gekürzt. Dann entwickelten wir einen Plan, wie wir nach und nach die Kontrolle zurückgewinnen können.

> CORONA WAR FÜR UNS EINE ONCE-IN-A-LIFETIME-CHANCE.

Wir sparten nicht bei der Technologie ein, sondern beim kundenseitigen Personal, automatisierten Prozesse. Wir mussten von 1.600 auf 600 Beschäftigte abbauen, was menschlich auch für mich hart war, weil ich alle unsere Leute eingestellt hatte. Aber der Personalabbau war unumgänglich, damit der Kosmos HRS überlebt. Bei der Frage, wie es weitergeht, waren wir extrem transparent. Die Mitarbeiterinnen und Mitarbeiter sollten wissen, welche Entscheidungen wir treffen und warum wir sie treffen.

Hatten Sie eine zündende Idee, um aus der Krise rauszukommen?

Wir haben uns tatsächlich wieder neu erfunden, wobei auch Zufall mit im Spiel war. Ein großes italienisches Kreuzfahrtunternehmen kam auf uns zu, das Corona-Kranke auf dem Schiff hatte und Quarantäne-Hotels suchte. Darin erkannten wir eine riesige Chance und haben mit unseren Plattformen global den Corona-Markt erschlossen.

Wie das?

Der gesamte Staat Kalifornien beispielsweise hat die Logis seines medizinischen Personals und von Armeeangehörigen über uns gesteuert und wir haben auditierbare Beschaffungs- und Bezahlprozesse entwickelt bis hin zur voll automatisierten Abrechnung. Das hat uns gerettet und es ist sogar ein dauerhaftes neues Geschäftsfeld entstanden: Disruption Management. Bei Fluten in Australien, bei Waldbränden in Kalifornien sind wir Partner von Regierungen, Hilfsorganisationen und Versicherungen.

Lassen Sie uns einen Blick in den Maschinenraum werfen: Wie hat sich HRS in der Krise intern verändert?

Wir sind noch mal sehr viel digitaler geworden. Heute arbeiten 55 Prozent unserer knapp 900 Beschäftigten im Produkt- und Engineeringbereich, vor der Pandemie waren es 25 Prozent. Wir erwirtschaften die gleiche Wertschöpfung mit sehr viel weniger Mitarbeiterinnen und Mitarbeitern. Und darüber hinaus haben wir die Krise genutzt, um eine neue Managementstruktur und ganz neue Ways of Working zu etablieren. Das war eine Once-in-a-lifetime-Chance.

Foto: HRS

Tobias Ragge, CEO der HRS Group, gibt Einblicke in die technologische Revolution des Geschäftsreise-Business

> VON ETABLIERTEN WETTBEWERBERN GEHT AM WENIGSTEN GEFAHR AUS.

Foto: Adobe Stock

Was haben Sie mit dem Management angestellt?

Wir hatten wie die meisten Unternehmen eine klassische Konzernmatrix. Aber da gewinnt immer das größte Geschäftsfeld, weil es die meiste Aufmerksamkeit bekommt. Wir wollten, dass die Business Units weitgehend autark agieren, mehr Freiräume haben und mehr Selbstverantwortung tragen. So haben wir die dezentrale Entscheidungsfindung forciert und die Abhängigkeiten und Komplexitätskosten reduziert. Inzwischen haben wir drei eigenständige Unternehmen mit eigenem CEO, eigenem Produktmanagement, IT Development, Vertrieb und Marketing und Supply Management. Lediglich Finance und HR sind noch Shared Services.

Ist die Art der Zusammenarbeit auch eine andere?

Wir versuchen, die strategische Umsetzung in die Teams zu bringen, sie besser zu beteiligen, um ein stärkeres Mitdenken zu fördern. Amazon stand hier Pate mit seinem Backwards-Ansatz.

Können Sie das konkreter verdeutlichen?

Wir pflegen in der Nach-Corona-Zeit einen sehr viel stärker partizipatorischen Stil – nicht in dem Sinne, dass jeder überall mitreden kann, aber wie wir beispielsweise Meetings gestalten und zu Entscheidungen kommen. Es gibt keine PowerPoint-Schlacht mehr, wo einer nach vorne kommt, alle anderen ewig lange zuhören und dann noch zwei, drei Fragen gestellt werden dürfen. Wir sind übergegangen zu Narrativen, maximal sechs Seiten lang, die in Realtime mit Fragen und Kommentaren beleuchtet werden. Dann wird diskutiert, und in einem anschließenden iterativen Prozess nutzen wir die Schwarmintelligenz verschiedener Funktionen. Generell steuern wir das Geschäft heute deutlich stärker über Input- statt über Outputmetriken. Natürlich sind am Ende auch Umsatz und Ergebnis wichtig, aber für die einzelnen Mitarbeiterinnen und Mitarbeiter geht es um den Purpose und seinen persönlichen Beitrag zum großen Ganzen.

Wie sehen innovative Mitarbeiterinnen und Mitarbeiter aus, die zu HRS passen?

Wir suchen Intrapreneurinnen und Intrapreneure, die was bewegen wollen. Deshalb kommt es zu 50 Prozent auf die fachlichen Fähigkeiten an und zu 50 Prozent auf den Cultural Fit. Für Letzteres dienen unsere neun Leadership Principles als Maßstab.

Gibt es aus Ihrer krisenhaften Corona-Zeit und der einschneidenden Transformation Erkenntnisse, die für nahezu jedes Unternehmen im Wandel relevant sind?

Was wir gemacht haben, kann letztlich jedes Unternehmen machen. Die wichtigsten Punkte: Erstens braucht es in der Krise ein klares Top-down-Management, damit schnelle Entscheidungen zu einem schnellen Impact führen. Zweitens ist es klug, unterschiedliche Businesses so autark wie möglich zu machen – inklusive aller Wertschöpfung, auch wenn man glaubt, es ist teurer. Drittens muss man sicherstellen, dass beim People Management die individuellen Wertvorstellungen des Hiring Managers neutralisiert werden und ein systemischer Ansatz für einen Cultural Fit gefunden wird. Und viertens sollte man fast allen Mitarbeiterinnen und Mitarbeitern im Doing abstrakte

Kennziffern wie Umsatz und Ergebnis ersparen und ihren Blick auf sinnstiftende Metriken richten, die die Teams im Tagesgeschäft beeinflussen können.

Auch die Konkurrenz versucht, innovativ zu sein. Von wem geht für Ihr Geschäftsmodell die größte Gefahr aus? Von Tech-Giganten wie Google und Amazon, von Branchenriesen wie BCD Travel oder von ambitionierten Start-ups?

Von den etablierten Wettbewerbern geht am wenigsten Gefahr aus. Die kenne ich und weiß, dass sie nicht durch bahnbrechende Innovationen auffallen. Die großen Tech-Player haben natürlich unfassbare Möglichkeiten, ich bezweifle aber, dass die in unser spezialisiertes und kleinteiliges Geschäft reingehen. Außerdem sind sie größere Margen gewohnt und ich vermute, dass ihnen unsere nicht groß genug sind. Von daher ist das Unbekannte die größte Gefahr – das kleine Start-up, das ich heute noch gar nicht kenne und das, gepaart mit AI, vielleicht ganz neue Ansätze findet. Deshalb bin ich in dieser Richtung sehr aufmerksam.

Woher holen Sie sich selbst Inspiration für Innovationen?

Ich habe den Anspruch, immer besser zu werden, ja der Beste zu sein. Wenn man so gestrickt ist, sucht man ständig nach neuer Inspiration. Ich lese viel …

… zum Beispiel?

„Working Backwards" von Colin Bryar, ein Insiderbericht über Amazons Kultur und Führung. Oder „Competing in the new World of Work" von Keith Ferrazzi, der sehr klug über das Antizipieren von Veränderungen und kreative Anpassungen schreibt. Spannend finde ich auch Biografien von Leuten, die wie Panasonic-Gründer Matsushita oder Elon Musk mutig waren und Konventionen ignoriert haben. Denn das ist die größte Kunst von Unternehmerinnen und Unternehmern: mutig zu sein und dort hinzugehen, wo andere nicht hingehen, weil sie Angst haben, Fehler zu machen.

Und außer der Lektüre?

Ich orientiere mich auch an Entrepreneurinnen und Entrepreneuren und Unternehmen, die in ganz anderen Branchen unterwegs sind, blicke auf Hyperscaler wie Google und Amazon, und ich bin gerne im persönlichen Austausch mit Unternehmerinnen und Unternehmern, um zu erfahren, welche Herausforderungen sie haben und wie sie Probleme lösen.

Sie sind mit HRS erfolgreich. Aber Sie haben sicherlich auch Fehler gemacht. Was war Ihr größter?

Ach Gott, ich habe viele Fehler gemacht. Was war mein größter? Mein größter Fehler? Wahrscheinlich, dass ich zu Beginn meiner Karriere die Bedeutung von Personen und People Management für das Gesamte unterschätzt und mich zu sehr von großen CVs und Namen habe blenden lassen.

Tobias Ragge

Tobias Ragge, Jahrgang 1976, beschreibt sich selbst als „Disruptive Entrepreneur". Er studierte Internationale Betriebswirtschaftslehre an der European Business School in Oestrich-Winkel. Nach Abschluss seines Studiums startete der Diplom-Kaufmann 2002 bei der Lufthansa seine berufliche Laufbahn in den Bereichen CRM und Restrukturierung Kontinentalverkehr. Seine nächste Station führte ihn ins Allianz-Management in Atlanta/USA, bevor er 2004 als Assistent der HRS-Geschäftsleitung ins Reisegeschäft seines Vaters einstieg. 2005 übernahm er dort die Marketingleitung und 2010 die Führung des Familienunternehmens.

Als CEO und Gesellschafter treibt er seither die Digitalisierung und Internationalisierung von HRS voran und baut das Serviceangebot für Firmenkunden im Reisegeschäft stetig aus. Mit Innovationen sowie gravierenden Veränderungen in der Unternehmensstruktur und -kultur bewältigte Ragge die für HRS existenzbedrohende Corona-Krise. Seinen Leitspruch hat er Victor Hugo entlehnt: „Keine Armee kann der Kraft einer Idee widerstehen, deren Zeit gekommen ist."

Cyber-Resilienz 2024

Wie sich Unternehmen gegen wachsende Bedrohungen aus dem Netz wappnen können

Foto: Adobe Stock

Ransomware, Phishing, KI-Bedrohungen: Die Cyber-Gefahrenlandschaft ist im Wandel. Franziska Hain, Geschäftsführerin der BDO Cyber Security GmbH, erklärt im Interview, wie Unternehmen mit neuer Regulatorik umgehen und sich mit robusten Cyber-Resilienz-Plänen wappnen können.

Frau Hain, die Cyber-Angriffe auf Unternehmen häufen sich. Welche Bedrohungen sollten Unternehmen 2024 ins Visier nehmen?

Cyber-Bedrohungen sind in einer ständigen Evolution – das zeigen auch die Berichte des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA). Wir sehen eine Zunahme an raffinierten Angriffen, wie beispielsweise die persistenten Bedrohungen durch staatlich unterstützte Hackerinnen und Hacker, gezielte Ransomware-Attacken gegen lebenswichtige Infrastrukturen oder KI-gestützte Phishing-Operationen mit verblüffend authentischer Identitätstäuschung. Aktuell halte ich es für besonders wichtig, in die Sicherheit von Systemen künstlicher Intelligenz zu investieren, um die eigene digitale Souveränität zu stärken und neuen Bedrohungen wirksam entgegenzutreten.

Künstliche Intelligenz ist ein wichtiges Stichwort. Wie können Unternehmen denn die Sicherheit ihrer KI-Systeme garantieren und die Echtheit der generierten Daten verifizieren?

KI-Systeme basieren zwar auf komplexen Algorithmen, sind letztendlich jedoch nur Programmcode. Dieser muss wie jede kritische Software abgesichert werden. Darüber hinaus liegt die Herausforderung darin, die Integrität der Erzeugnisse der KI zu gewährleisten. Qualitätssicherung ohne Vergleichsmaßstab erfordert innovative Methoden, wie fortgeschrittene Anomalie-Erkennung, um Abweichungen schnell zu erkennen. Zudem ist es entscheidend, den Daten-Input vor ungewollten Veränderungen zu schützen, um die Verlässlichkeit der KI-Outputs zu gewährleisten. Die Sichtbarmachung von Verunreinigungen oder Manipulationen im Output erfordert Transparenz in den Verarbeitungsprozessen und fortgeschrittene Techniken zur Überprüfung.

Könnten Sie ein Beispiel geben, wie ein Angreifer oder eine Angreiferin die Funktion einer KI beeinträchtigen könnte und welche Schutzmaßnahmen dagegen ergriffen werden sollten?

Nehmen wir an, ein Angreifer oder eine Angreiferin infiltriert unerkannt ein KI-System mit manipulierten Daten und verfälscht damit die empirische Datengrundlage. Auf dieser fehlerhaften Grundlage generiert das KI-System dann Erkenntnisse – auf deren Basis kritische Entscheidungen getroffen werden könnten. Um das zu verhindern, müssen Unternehmen ihre Daten-Inputs absichern, zum Beispiel durch die Einführung von Kontrollmechanismen, die die Authentizität und die Qualität der Daten überprüfen. Weiterhin sollten sie ihre KI-Modelle regelmäßig rekalibrieren und auf Unregelmäßigkeiten in den Ergebnissen prüfen, um derartige Risiken zu minimieren.

Was würden Sie Unternehmen sonst noch raten, um sich vor Cyber-Angriffen zu schützen?

Unternehmen müssen erkennen, dass der klassische Ansatz der Risikoanalyse und -behandlung sowie die Implementierung eines Informationssicherheitsmanagementsystems nicht mehr ausreichen. Vielmehr ist heute gleichermaßen entscheidend, eine Widerstandsfähigkeit für den Ernstfall aufzubauen, sodass man schnell und effektiv auf Vorfälle reagieren kann – es gilt eine sogenannte Cyber-Resilienz herzustellen.

Foto: Adobe Stock

Wie baut man eine solche Cyber-Resilienz auf?

Zunächst einmal sehen wir, dass die Angst vor dem Cyber-Vorfall und seinen immer wieder verheerenden Auswirkungen groß ist. Gleichzeitig packen Unternehmen das Thema ungern und unzureichend an. Hier ist der erste Schritt zu tun. Entscheidungsträgerinnen und Entscheidungsträger müssen sich befähigen, das Cyber-Risiko als Business-Risiko wahrzunehmen, zu beurteilen und zu behandeln.

Die Zielsetzung, auf die Wirksamkeit seiner Cyber-Resilienz vertrauen zu können, korreliert mit der Bereitschaft, Investitionen zu tätigen.

Wie kann man sich dann einer Umsetzung schnell und unkompliziert nähern?

Wir raten unseren Kundinnen und Kunden immer dazu, den Ernstfall realistisch zu trainieren. Krisensimulationen sind nicht nur Übungen, sie stellen sich oft als Rehearsals für die Realität im Unternehmen heraus. Sie bereiten die Teams darauf vor, das Unvorhersehbare zu erkennen und zu managen. In unseren Simulationen stellen wir gemeinsam mit den CEOs zum Auftakt gern eine Schlüsselfrage: „Was tun, wenn morgen früh ein Cyber-Angriff meine IT lahmlegt und Daten kompromittiert werden?“ Die Beantwortung dieser Frage muss im Rahmen der Informationssicherheitsstrategie Vorrang haben und ist für den Ernstfall im Vergleich zum besten Richtlinien-Dokument wichtiger.

> KRISENSIMULATIONEN SIND NICHT NUR ÜBUNGEN, SIE STELLEN SICH OFT ALS REHEARSALS FÜR DIE REALITÄT IM UNTERNEHMEN HERAUS.

Apropos Richtlinien: Auf welche neuen Regularien und Gesetze müssen Unternehmen achten?

Unternehmen müssen sich jetzt vor allem mit den regulatorischen Vorgaben der Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS) und aus dem Digital Operational Resilience Act (DORA) auseinandersetzen. Auch der EU Data Act wird eine zentrale Rolle spielen. Das Gesetz wird künftig den fairen Zugang und die Nutzung von Daten regeln und die Datensouveränität stärken, was für Unternehmen bedeutet, dass sie nicht nur ihre Systeme schützen, sondern auch die Art und Weise, wie sie Daten verwalten und teilen, sorgfältig überdenken müssen.

Inwiefern wird DORA die Informationssicherheit in den Unternehmen beeinflussen?

Wenn es einer Hackerin oder einem Hacker, einer kriminellen Vereinigung oder einer staatlich organisierten Gruppe gelingt, einen Cyber-Angriff derart umzusetzen, dass eine kritische Menge von zunehmend digitalisierten Abläufen in den Finanzunternehmen beeinträchtigt ist und es aufgrund der Abhängigkeiten untereinander zur Instabilität der Finanzmärkte z. B. durch Liquiditätsengpässe oder zum Vertrauensverlust in die Finanzmärkte kommt, dann ist das Cyber-Risiko als Systemrisiko zu verstehen.

> WAS TUN, WENN MORGEN FRÜH EIN CYBER-ANGRIFF MEINE IT LAHMLEGT UND DATEN KOMPROMITTIERT WERDEN?

Der Digital Operational Resilience Act ist eine Antwort auf die Frage, wie es ein Cyber-Systemrisiko zu vermeiden gilt. Vor diesem Hintergrund ist es konsequent, dass DORA auch Anforderungen an die Informationssicherheit von kritischen IKT-Dienstleistern stellt, die durch die Finanzunternehmen beauftragt sind. Da nun erstmals kritische IKT-Dienstleister unter der Überwachung der EU-Aufsichtsbehörden (European Supervisory Authorities – ESAs) stehen, ist davon auszugehen, dass man dort noch konsequenter in die Herstellung und Aufrechterhaltung von Informations-sicherheit investiert. Davon profitiert nicht nur der Finanzsektor, sondern alle Unternehmen, die sich auf die gleichen IKT-Dienstleister stützen. Insgesamt ist eine relevant höhere Cyber-Resilienz durch DORA zu erwarten.

Die neuen Richtlinien mögen eine Hilfestellung für Unternehmen sein, sie bringen aber auch zusätzliche Hürden mit sich. Wird noch mehr Regulatorik nicht zum Problem für kleine und mittelständische Unternehmen?

Ich bin überzeugt, dass sich diese Investitionen lohnen. Davon profitieren nicht nur die Finanzunternehmen selbst, sondern auch mittelständische Unternehmen, die dieselben IKT-Dienstleister nutzen. Das könnte auch zu einer verbesserten Versicherbarkeit im Bereich der Cyber-Versicherungen führen. Gleichzeitig wird die Qualität der Umsetzung von den Prüfkapazitäten der Aufsichtsbehörden abhängen. Folglich wird sich die Herstellung von Konformität zu DORA über einen längeren Zeitraum, weit über Januar 2025 hinaus, erstrecken.

Gibt es für Unternehmen ein Hintertürchen, den Regularien zu entgehen – zum Beispiel durch ein Spiel auf Zeit?

Nein, bei der Regulatorik gibt es keinen Spielraum – sie muss budgetiert, umgesetzt und die Konformität muss sichergestellt werden. Es ist ratsam, den Mehrwert für das eigene Unternehmen herauszuarbeiten und sich die Regulatorik zunutze zu machen. Durch eine intelligente Nutzung regulatorischer Anforderungen können Unternehmen ihre Sicherheitsstandards verbessern und gleichzeitig Wettbewerbsvorteile erzielen. Hier geht es nicht nur um das Umsetzen von Richtlinien, sondern um eine nachhaltige Integration von Resilienz in die Unternehmenskultur.

Foto: Adobe Stock

Gehen wir davon aus, ich habe eine gute Cyber-Resilienz in meinem Unternehmen aufgebaut. Bin ich nun komplett sicher?

Leider ist es längst unmöglich geworden, Cyber-Angriffe gänzlich zu verhindern. Ich erinnere nochmals: Cyber-Resilienz bedeutet nicht nur Prävention, sondern gleichermaßen auch die Herstellung von Response-Fähigkeiten. Unternehmen müssen starke Detektions- und Reaktionsfähigkeiten entwickeln, um Cyber-Angriffe frühzeitig zu erkennen und abzuwehren, bevor es zu einem intolerablen Schadensereignis kommt. Zusätzlich braucht es aber oft auch Cyber-Spezialistinnen und -Spezialisten, die unterstützen können. Die dafür notwendigen Fähigkeiten und Kenntnisse sind umfangreich und hoch spezialisiert. Oft ist es nicht wirtschaftlich und praktikabel, diese im Unternehmen bereitzuhalten und in der sich ständig verändernden Angriffswelt auf dem aktuellen Stand zu halten. Umso sinnvoller ist es, sich dieses Spezialistenwissen von außen zu holen – etwa mit einem Angebot wie unseren Cyber Incident Response und Forensic Leistungen.

> CYBER-RESILIENZ BEDEUTET NICHT NUR PRÄVENTION, SONDERN GLEICHERMASSEN AUCH DIE HERSTELLUNG VON RESPONSE-FÄHIGKEITEN.

Was genau beinhaltet solch ein Spezialisten-Service?

Ich kann an dieser Stelle nur für BDO sprechen: Als Kundin oder Kunde unseres BDO Cyber Incident Response & Crisis Centers haben Unternehmen bei uns 24/7 Zugriff auf ein Cyber-Experten-Team mit technischem Spezialwissen und Krisenmanagement-Fähigkeiten sowie notwendige Rechtsberatung in Bezug auf datenschutz- und haftungsrechtliche Fragestellungen. Und unsere Spezialistinnen und Spezialisten sind erprobt. Sie sind oft vertraut mit den verwendeten Schadcodes, können Abläufe der Krisensituation vorhersehen und kennen Verhandlungsstrategien, um z. B. im Ransomware-Fall den Erpresserinnen oder Erpressern auf Augenhöhe zu begegnen.

Zusammengefasst, welche Schritte sind Ihrer Meinung nach für Unternehmen unerlässlich, um in der digitalen Welt souverän und autonom zu agieren?

Die zunehmende Digitalisierung und das Voranschreiten von Technologien wie KI prägen aktuell massiv gesellschaftliche Entwicklungen und sind ein wesentlicher Treiber von Innovationen. Unternehmen stehen damit aber auch vor der komplexen Herausforderung, sich in einer vernetzten und durch und durch technologisierten Welt zu behaupten. Es ist für sie essenziell, Daten und Know-how zu schützen und digitale Infrastrukturen sicher zu gestalten.

Ein wichtiges Schlüsselelement ist dabei die Transparenz von Softwarelieferketten, da sogenannte Supply-Chain-Attacken nach Ransomware-Angriffen die häufigste Art von Cyber-Angriffen darstellen. Die Technische Richtlinie (TR-03183) des BSI zur Cyber-Resilienz unterstützt dabei mit einem Konzept für eine „Software Bill of Materials" (SBOM) zur Dokumentation, welche kommerziellen und freien Softwarelösungen in Softwareprodukten eingesetzt werden und welche Abhängigkeiten zu Komponenten Dritter bestehen.

Neben der sicheren Gestaltung von Lieferketten trägt auch der Einsatz von Produkten mit dem Gütesiegel des Bundesverbands IT-Sicherheit e. V. (TeleTrusT – Vertrauenszeichen „IT Security made in Germany") zur sicheren Gestaltung von IT-Infrastrukturen bei. Produkte mit dieser Kennzeichnung wurden umfassend geprüft und als vertrauenswürdige IT-Sicherheitslösungen ohne verdeckte Backdoor eingestuft.

Darüber hinaus sollten Unternehmen bei der Gestaltung ihrer Prozesse und Infrastrukturen auch immer die Zero-Trust- Philosophie berücksichtigen. Anders als bei traditionellen Sicherheitsansätzen geht dieser Ansatz davon aus, dass prinzipiell keine Benutzerin, kein Benutzer, Gerät oder Netzwerk vertrauenswürdig ist und alle potenziell Sicherheitsrisiken darstellen. Daraus abgeleitet setzt dieses Konzept auf eine Minimierung von Berechtigungen, eine kontinuierliche Überprüfung von Identität und Status von Benutzerinnen und Benutzern sowie Geräten, eine strenge Authentifizierung und Autorisierung sowie auf eine konsequente Netzsegmentierung. MB

Mehr zum Thema:
www.bdosecurity.de

5 Schlüsselstrategien zur Stärkung der Cyber-Resilienz

Als strategische Entscheiderinnen und Entscheider stehen Aufsichtsräte und CEOs an der Frontlinie, wenn es um die Cyber-Sicherheit geht. Franziska Hain, Geschäftsführerin der BDO Cyber Security GmbH, gibt fünf Handlungsempfehlungen, um die digitale Abwehrkraft zu stärken.

1 **Eine Cyber Attack Response Strategie entwickeln lassen:** Eine gut durchdachte Strategie ist elementar, um auf Cyber-Angriffe zu reagieren. Die Unternehmensführung sollte einen Plan erarbeiten lassen, der klar definiert, wie auf verschiedene Arten von Cyber-Angriffen reagiert wird. Dieser umfasst die Identifizierung von Schlüsselpersonal, die Zuweisung von Rollen und Verantwortlichkeiten sowie das Aufstellen eines Kommunikationsplans, der sowohl interne als auch externe Kommunikation abdeckt. Dazu gehört auch der Umgang mit einer Lösegeldforderung.

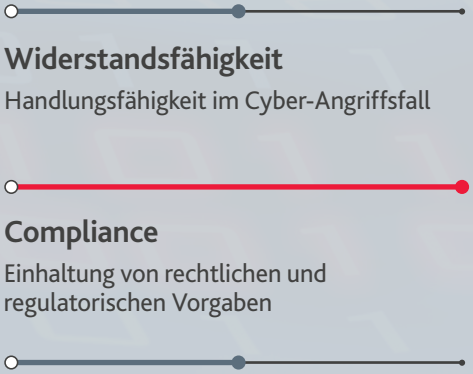
2 **Regelmäßige Cyber-Angriffssimulationen umsetzen:** Unternehmen sollten den Ernstfall simulieren und die Response-Strategie üben. Cyber-Simulationen helfen dabei, die Response-Fähigkeit des Unternehmens zu testen und Reaktionspläne zu schärfen. Diese Übungen sollten unter möglichst realistischen Bedingungen durchgeführt werden, um die Wirksamkeit der Notfall- und Reaktionsstrategien zu überprüfen und kontinuierlich zu verbessern.

3 **Konformität zur Regulatorik einfordern:** Es gilt einmal mehr, Führungskräfte für die Umsetzung von Anforderungen z. B. aus dem Digital Operational Resilience Act (DORA) oder der Netz- und Informationssysteme-Richtlinie (NIS2) zu sensibilisieren. Um die Konformität zu gewährleisten, können interne Audits helfen, die Einhaltung des DORA zu überprüfen, während gezielte Schulungen das Team mit den Anforderungen der Regulatorik vertraut machen.

4 **Kosten-Nutzen-Effizienz aufzeigen lassen:** Die Wirksamkeit von implementierten Sicherheitsmaßnahmen sollte im Verhältnis zu getätigten Investitionen stehen. Hier kann z. B. mittels einer Business-Impact-Analyse das finanzielle Schadenspotenzial unter Annahme eines IT-Ausfalls über einen definierten Zeitraum ermittelt und gegen die Kosten der Präventionsmaßnahmen gelegt werden.

5 **Ein Cyber Resilience Dashboard etablieren und berichten lassen:** Um eine Aussage über den Reifegrad der Cyber-Resilienz treffen zu können, sind die folgenden drei Themenfelder mittels KPIs im Rahmen eines Dashboards auszugestalten.

Cyber Resilience Dashboard



Widerstandsfähigkeit
Handlungsfähigkeit im Cyber-Angriffsfall

Compliance
Einhaltung von rechtlichen und regulatorischen Vorgaben

Kosten-Nutzen-Verhältnis
Wirksamkeit von implementierten Sicherheitsmaßnahmen im Verhältnis zu getätigten Investments

Foto: Adobe Stock

Regulatorik Deep Dive

Foto: Adobe Stock

Verschärfte europäische Anforderungen zur Cyber-Security treffen viele deutsche Unternehmen

Foto: Adobe Stock

In Zeiten kontinuierlich zunehmender Internetkriminalität hat sich die Europäische Union nochmals dem Thema Cyber-Sicherheit zugewandt. Anfang 2023 traten gleich zwei neue europäische Rechtsakte in Kraft: die zweite Fassung der Network and Information Security Richtlinie (NIS2) und der Digital Operational Resilience Act (DORA).

Zahlreiche Unternehmen erstmals von NIS betroffen

Als europäische Richtlinie gilt NIS2 nicht unmittelbar, sondern ist bis zum 17. Oktober 2024 in nationales Recht umzusetzen. In Deutschland soll dies durch eine Neufassung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) geschehen. Die umfassenderen Cyber-Sicherheitsanforderungen des neuen BSIG werden einen erweiterten Kreis von Einrichtungen und Unternehmen treffen. Bei Verstößen gelten erheblich verschärfte Sanktionen, die nicht nur die regulierten Unternehmen selbst, sondern auch deren Leitungsorgane persönlich treffen können.

Da die Zeit drängt, sollten Unternehmen bereits jetzt prüfen, ob sie den neuen Cyber-Regeln unterfallen. Dies ist allerdings nicht immer leicht zu beantworten.

Pflichtig sind zunächst Unternehmen, die bereits unter KRITIS Adressat von Cyber-Anforderungen waren. Hier ändert sich nichts. Darüber hinaus können Unternehmen oder Betriebsteile der neuen Regelung unterfallen, die in einem der in § 28 BSIG aufgeführten Sektoren tätig sind. Insbesondere durch die Aufnahme der neuen Sektoren „verarbeitendes Gewerbe/Produktion und Ernährung" fallen bis zu 30.000 deutsche Unternehmen erstmals unter die Regulierung der Cyber-Sicherheit und die Sanktionen.

Von der konkreten Tätigkeit und weiteren Kennzahlen (Mitarbeiterzahl/Umsatz-/Bilanzsumme) hängt dann ab, welche Cyber-Anforderungen bestehen. Erleichterungen und Ausnahmen sieht der Gesetzentwurf für kleinere Unternehmen vor.

Cyber-Regulierung des Sektors Finanzwesen durch DORA

Der direkt anwendbare DORA weist viele Parallelen zu NIS2 auf, beschränkt sich aber auf den Finanzsektor. Betroffen sind nicht nur Kreditinstitute, Handelsplätze und Versicherungen, sondern z. B. auch Versicherungsvermittler, Verwaltungsgesellschaften oder Einrichtungen der betrieblichen Altersversorgung sowie deren digitale Dienstleister (sog. IKT-Drittdienstleister). Auch hier gilt es für betroffene Unternehmen, die konkreten Anforderungen von DORA an die Cyber-Sicherheit zu prüfen.

Interdependenzen DORA und NIS2

Während NIS2 durch einen einheitlichen Governance-Rahmen ein hohes digitales Sicherheitsniveau für betroffene Unternehmen in der EU schafft, ist DORA eine Ableitung der NIS2-Richtlinie für den Finanzsektor mit sektorspezifischen Cyber-Sicherheitsanforderungen. Als speziellere Regelung geht DORA den Vorschriften von NIS2 vor.

Kurze Umsetzungsfristen und gestiegene Cyber-Anforderungen verlangen von Unternehmen ein strategisches Vorgehen. Der Status quo der aktuellen Sicherheitseinrichtungen und der geschützten Geschäftsprozesse ist zu erheben und mit den Vorgaben von DORA und NIS2 abzugleichen. Hieraus ergibt sich der dringende Handlungsbedarf.

Pflichten aus NIS2

NIS2 teilt betroffene Unternehmen in drei Kategorien ein: Betreiber kritischer Anlagen, die die härtesten Cyber-Anforderungen treffen, sowie besonders wichtige und schließlich wichtige Unternehmen, bei denen die Cyber-Anforderungen jeweils graduell abgeschwächt werden.

Die Anforderungen aus NIS2 zielen darauf ab, Netzwerk- und Informationssysteme und deren physische Sicherheit vor Störungen zu schützen – basierend auf Cyber-Security-Standards wie:

- Richtlinien zur Risikoanalyse und Informationssystemsicherheit
- Umgang mit IKT-Vorfällen mit Aspekten erhöhter operationaler Resilienz
- BCM mit Disaster Recovery und Crisis Management
- Sicherheit der IKT-Lieferkette bezogen auf unmittelbare Dienstleister oder Lieferanten
- Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netzwerk- und Informationssystemen,
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Maßnahmen des Risikomanagements der Cyber-Sicherheit
- grundlegende Stärkung der „Human Firewall“ über bspw. Cyber-Sicherheitsschulungen
- Konzepte und Verfahren bezüglich der Verwendung von Kryptografie und Verschlüsselung
- Personalsicherheit über Zugangskontrollrichtlinien,
- Benutzerberechtigungsmanagement mit Verwendung von Multi-Faktor- oder kontinuierlichen Authentifizierungsmethoden

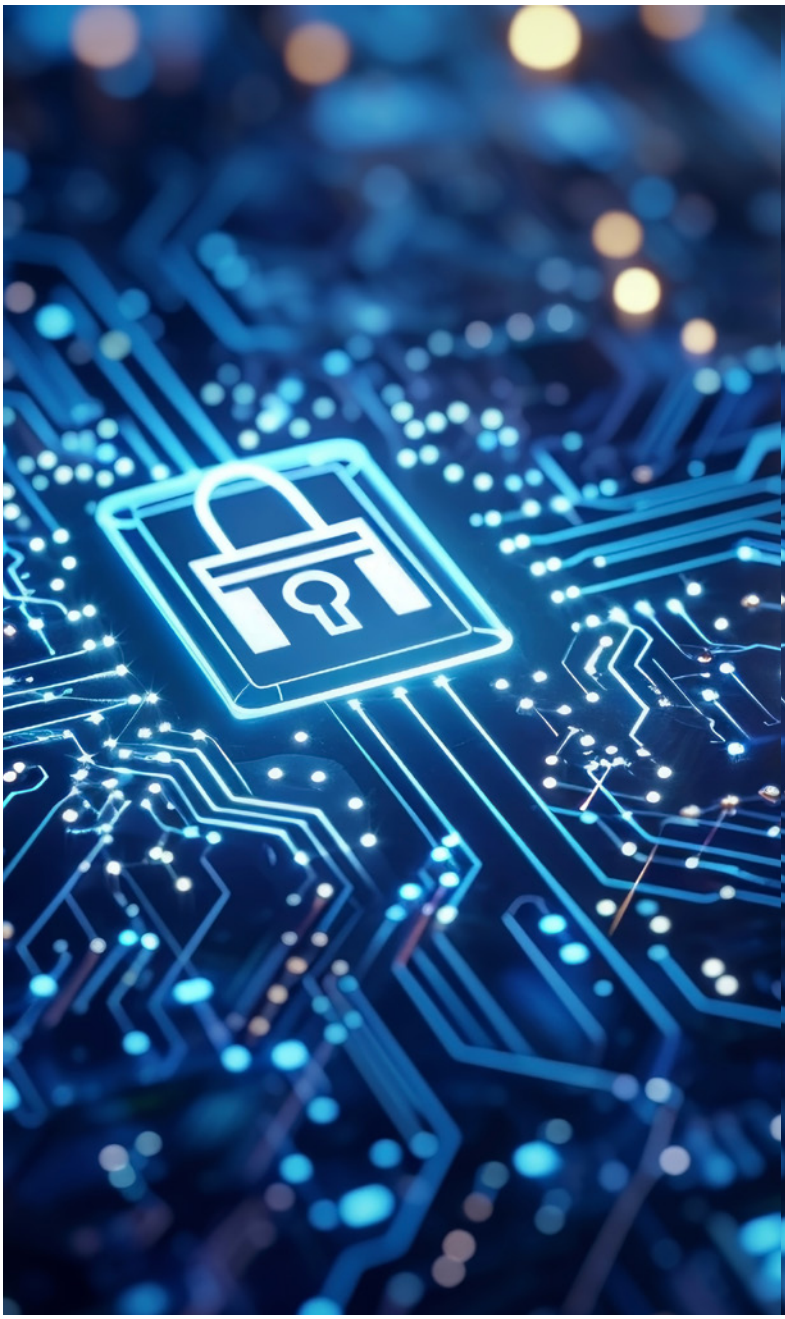
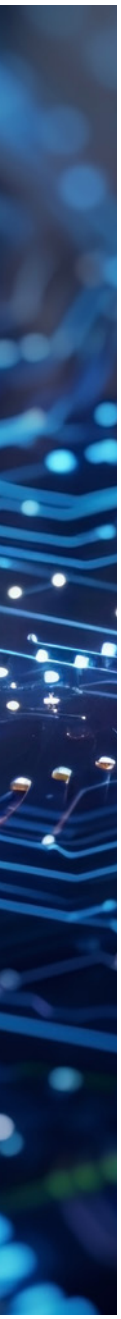


Foto: Adobe Stock



Pflichten aus DORA

Die Vorgaben aus DORA sehen vor, dass betroffene Unternehmen einen Governance- und Kontrollrahmen in entsprechenden Leitlinien definieren, um einen sicheren Betrieb der IKT-Systeme und Informationen zu ermöglichen. Große Bedeutung kommt dabei dem Risikomanagement zu. Die Gesamtverantwortung liegt beim Leitungsorgan des Unternehmens. Fachliche Schulungen müssen die Verantwortlichen in die Lage versetzen, die IKT-Risiken und deren Auswirkungen auf die Geschäftstätigkeit bewerten zu können.

Besonderes Augenmerk gilt dem Management von IKT-Dienstleister-Risiken, für die das beauftragende Unternehmen jederzeit verantwortlich bleibt.

Der Nachweis zur Einhaltung der DORA-Vorgaben soll einmal jährlich durch interne oder externe Stellen erfolgen, wobei eine Auslagerung der Überprüfung das Finanzunternehmen nicht von der Verantwortung über die Einhaltung entbindet.

Zu den bereits aufgeführten DORA-Schwerpunkten werden zudem noch strengere Vorgaben für folgende Bereiche definiert:

- Erweiterung des IKT-Vorfallsmanagements durch Meldewesen-Prozesse mit vorgegebener Klassifizierung
- freiwillige Meldung von erheblichen Cyber-Bedrohungen
- verbessertes Schwachstellenmanagement durch Basis-Tests sowie fortgeschrittenen Threat Led Penetration Tests (TLPT)
- Einrichtung der Risk-Management-Control-Funktion wie CISO, ISO oder ISB
- Asset Management unter Berücksichtigung von sicherer und autorisierter Soft- und Hardware
- Source-Code-Analyse und -Testing von proprietärer Software
- verbesserte Netzwerksicherheit durch sichere Prozesse und Verfahren
- Erhöhung der Betriebsstabilität durch umfassende BCM-Vorgaben
- Vorgaben für das Identity Access Management
- strengere Vorgaben für den Einsatz von Verschlüsselungen

Behördliche Aufsicht, Bußgelder und Schadensersatz

NIS2 flankiert die verschärften Cyber-Anforderungen mit einer Registrierungspflicht für alle betroffenen Unternehmen, erweiterten Aufsichtsbefugnissen der Behörden und schärferen Sanktionen von Verstößen.

Bei Verstößen gegen Cyber-Pflichten drohen Unternehmen Bußgelder bis zu einer Höhe von zehn Millionen Euro oder zwei Prozent des weltweiten Umsatzes, wenn dieser höher ist. Der Sanktionskatalog ähnelt damit dem der DSGVO.

Außerdem verpflichtet NIS2 den nationalen Gesetzgeber erstmals, eine direkte persönliche Haftung der zuständigen Leitungsorgane für Folgen der Nichteinhaltung von Cyber-Sicherheitspflichten einzuführen. Führungskräfte haften u. U. neben dem Unternehmen direkt gegenüber Betroffenen.

Zeit zu handeln

Mit NIS2 und DORA wird Cyber-Sicherheit in Deutschland zu einer zentralen Aufgabe für Unternehmen und deren Leitungsorgane. Die neuen Cyber-Anforderungen treffen einen erheblich größeren Kreis von Unternehmen und zwingen diese, ihre bisherige Cyber-Sicherheitspraxis zu überdenken und zu verbessern. ■

Experten:

Hans-Peter Toft
Rechtsanwalt, Partner
BDO Legal Rechtsanwaltsgesellschaft mbH

Johannes Helke
Partner, Financial Services
BDO AG Wirtschaftsprüfungsgesellschaft

Stephan Halder
Senior Manager, Forensic, Risk & Compliance
BDO AG Wirtschaftsprüfungsgesellschaft

Lücken im System

Viele Krankenhäuser sind gegen Cyber-Attacken nicht gut gerüstet. Unzureichende Vernetzung, zu wenig IT-Fachkräfte, kein 24/7-Monitoring – das alles kann bitter enden. Obendrein wird KI zur neuen Herausforderung für Klinikmanager.

Foto: Adobe Stock

Foto: Adobe Stock

Im ZDF lief neulich der Thriller „Whistleblower". Unbekannte Hackerinnen oder Hacker sind in die Steuerungen des fiktiven Zentralklinikums Berlin eingedrungen. Nach einem Systemausfall verstirbt ein Patient. Eine russische Whistleblowerin behauptet, sie habe den rettenden Code und könne weitere Attacken vereiteln. Vorausgesetzt, sie bekomme einen Millionenbetrag, Asyl in Deutschland und die Aufnahme in ein Zeugenschutzprogramm.

Das Drehbuch basiert nicht auf einem wahren Fall, und man muss dafür auch nicht zwingend dunkle Mächte in Russland, China oder Nordkorea bemühen. Aber weit hergeholt sind Cyber-Attacken auf Krankenhäuser ganz gewiss nicht. Es gibt ständig Angriffe von Cyber-Kriminellen, die häufig nicht öffentlich bekannt werden. Besonders dramatisch war im September 2020 ein Hackerangriff auf die Uniklinik Düsseldorf. Rund 30 Server wurden über Nacht verschlüsselt, das Klinikpersonal hatte keinen Zugriff mehr auf Patientendaten, die Kommunikation war komplett stillgelegt und die Technik in den OPs fiel größtenteils aus. Die Folge: Notfallpatientinnen und -patienten konnten nicht mehr aufgenommen und versorgt werden, es herrschte Stillstand. Keine Notarzt- und Krankenwagen kamen mehr an, keine Hubschrauber.

BSI spricht von einer großen Gefahr

Das Bundeskriminalamt, das Hackeraktivitäten im Darknet überwacht, stellt eine deutliche Zunahme der weltweiten Angriffe auf medizinische Einrichtungen fest. Und die Präsidentin des Bundesamts für Sicherheit in der Informationstechnologie (BSI), Claudia Plattner, nennt Cyber-Angriffe auf die knapp 1.900 deutschen Krankenhäuser „eine große Gefahr". Das gilt für das ganze Gesundheitswesen und lässt sich an zahlreichen Überschriften der vergangenen zwei Jahre ablesen: „Medizinischer Dienst in Niedersachsen von Hackerangriff betroffen" … „Caritas rechnet nach Hackerangriff mit längeren Einschränkungen" … „Cyber-Attacke gegen Internationales Rotes Kreuz" … „Hackerangriff auf CompuGroup Medical" …

Es gibt große Unterschiede, wie gut Krankenhäuser gegen Cyber-Attacken gerüstet sind. Leider müssen wir jedoch feststellen, dass das Informationssicherheitsniveau in vielen Kliniken nicht entlang der Bedrohungslage aufgestellt ist. Provokant gesagt: Die Branche hat jeden Tag damit zu tun, Leben zu schützen und zu retten; Daten konsequent und permanent zu schützen, ist in diesem Bewusstsein nachgeordnet und hat häufig nicht den Stellenwert, der ihm gebührt. Maßgabe sollte sein: So wie ein steriles Skalpell im OP müssen auch IT-Sicherheitssysteme „steril" und ihre Sicherheit gegen Kompromittierung eine Selbstverständlichkeit sein.

Denn Hackerinnen und Hacker sehen es auf wertvolle personenbezogene Patientendaten ab. Zum einen, weil Kliniken eine große Bedeutung für die gesundheitliche Versorgung der Gesellschaft haben und Cyber-Kriminelle davon ausgehen, dass das Management bei Erpressung lieber bezahlt, als seine Patientinnen und Patienten zu gefährden und obendrein einen öffentlichen Vertrauensschaden zu riskieren. Zum anderen, weil sich private Gesundheitsdaten nach einer Erpressung auch noch an Dritte weiterverkaufen lassen. In renommierten Kliniken kommt ein weiterer, spezieller Grund dazu: Dort, wo Prominente aus aller Welt behandelt werden, ist das Erpressungspotenzial noch größer.

Zahlreiche Einfallstore für Hackerinnen und Hacker

Einfallstore gibt es für Hackerinnen und Hacker in Krankenhäusern ganz viele. Die Kritische Digitale Infrastruktur (KDI) umfasst alle digitalen Systeme und Netzwerke, die für den Betrieb und die Sicherheit der Kliniken wichtig sind. Dazu zählen elektronische Gesundheitsakten, medizinische Geräte, Laborinformationssysteme, Krankenhausinformationssysteme und mehr (siehe Kasten „Kritische Digitale Infrastruktur" auf S. 42). Der Ausfall oder die Beeinträchtigung dieser Systeme kann verheerende Auswirkungen auf die Patientenversorgung und die allgemeine Funktionsfähigkeit eines Krankenhauses haben.

So vielseitig die Angriffspunkte sind, so vielfältig sind auch die Risiken und Gefahren.

- **Datendiebstahl und -manipulation:** Cyber-Kriminelle können versuchen, auf Patientendaten zuzugreifen, um sie zu stehlen oder zu manipulieren.
- **Ransomware-Angriffe:** Cyber-Kriminelle können – verbunden mit Forderungen nach Lösegeld (ransom) – anhand von Schadprogrammen Krankenhausdaten verschlüsseln und damit den Zugriff auf lebenswichtige Patientendaten blockieren. So drohen erhebliche Verzögerungen bei der Behandlung und potenziell lebensgefährliche Situationen für Patientinnen und Patienten.
- **Angriff auf medizinische Geräte:** Manipulationen an medizinischen Geräten können zu falschen Diagnosen und in der Folge zu falschen Behandlungen führen. Da viele Geräte untereinander vernetzt sind, um den Informationsaustausch zu erleichtern, kann ein Angriff auch zu einem Totalausfall führen.
- **Angriff auf Krankenhausinformationssysteme:** Durch Eingriffe in die Organisationsabläufe kann der gesamte Betrieb erheblich gestört werden. Patientenversorgung, Terminplanung und andere wichtige Prozesse stehen auf dem Spiel.

Foto: Adobe Stock

Kritische Digitale Infrastruktur

Die Kritische Digitale Infrastruktur (KDI) in Krankenhäusern umfasst eine Reihe von Systemen und Technologien, die für den reibungslosen Betrieb und die verlässliche Patientenversorgung entscheidend sind. Dazu zählen die folgenden.

- **IT-Infrastruktur:** Netzwerke, Server und Speicherinfrastruktur zum Datenaustausch und zur Kommunikation zwischen verschiedenen Systemen.
- **Elektronische Patientenakten (EPA):** digitale Systeme zur Speicherung und Verwaltung von Patienteninformationen, die vertrauliche medizinische Daten enthalten und daher besonders geschützt werden müssen.
- **Krankenhausinformationssysteme:** Systeme zur Verwaltung und Organisation von Krankenhausabläufen, von der Personal- und Terminplanung bis zur Abrechnung.
- **Laborinformationssysteme:** Systeme, die Labordaten erfassen, verwalten und analysieren, um medizinische Tests zu unterstützen.
- **Medizinische Geräte und Netzwerke:** digitale Steuerungssysteme für Beatmungsgeräte, Infusionspumpen und Monitore sowie für die Vernetzung dieser Geräte im Internet der Dinge (IoT).
- **Bildgebende Diagnostik:** digitale Röntgen-, CT- und MRT-Systeme, die eine entscheidende Rolle bei der Diagnose und Behandlung von Patientinnen und Patienten spielen.
- **Telemedizinische Geräte:** digitale Plattformen, die die Fernüberwachung von Patientinnen und Patienten sowie Telekonsultation ermöglichen.

Foto: Adobe Stock

Das Problem ist, dass die KDI aus vielen Einzelsystemen besteht, die oftmals nicht lückenlos vernetzt sind und intern auch nicht Tag und Nacht überwacht werden. Auf externe Lösungen, von der Security-Beratung über das -Testing und Notfallübungen bis hin zum 24-Stunden-Monitoring, wie es auch BDO Cyber Security anbietet, wird häufig verzichtet. Es besteht die feste Überzeugung, alles selbst im Griff zu haben und sich fremde Unterstützung ersparen zu können. Aber die Technologisierung des Gesundheitswesens erfordert eben auch eine kontinuierliche Verbesserung der Sicherheitssysteme, und die ist kostspielig.

Finanzielle Misere der Krankenhäuser

Das ist bei Krankenhäusern der wunde Punkt. Viele haben 2023 Fehlbeträge erwirtschaftet. Nach Corona sind die Fallzahlen zurückgegangen und damit Einnahmen weggefallen, die Kosten geblieben. 60 Prozent auf der Ausgabenseite eines Klinikbudgets sind Personalkosten, und diese steigen nun aufgrund von Inflationsausgleich und Personalwettbewerb deutlich. Die Bundesländer wiederum vernachlässigen ihre Pflicht zur Investitionsfinanzierung seit Jahren. So werden notwendige Investitionen in IT-Sicherungssysteme oftmals gestreckt oder für gewisse Zeit einfach ausgeblendet.

Es gibt zwar Fördermittel für die Digitalisierung in Krankenhäusern. Aber dabei geht es in erster Linie um eine Initialförderung für die Anschaffung von Hard- und Software. Angesichts des hohen Innovationsgrads sind jedoch schon nach relativ kurzer Zeit Updates und – gerade mit Blick auf die Systemsicherheit – Neuanschaffungen notwendig, für die es dann keine Fördermittel mehr gibt.

BDO Studie: IT-Fachkräftemangel

Verschlimmert wird die Misere durch den IT-Fachkräftemangel, wie eine neue Studie[1] von BDO in Kooperation mit dem Deutschen Krankenhausinstitut offenlegt. Sie basiert auf einer repräsentativen Krankenhausbefragung und kommt zu dem Ergebnis, dass drei Viertel der Kliniken Probleme haben, offene Stellen für IT-Fachkräfte zu besetzen. Im Mittel können dort 14 Prozent der IT-Stellen nicht besetzt werden. Hauptgründe sind Mängel in der Vergütung, etwa die wenig flexiblen Tarifstrukturen im Krankenhaus und eine schlechtere Bezahlung als in anderen Branchen.

Das erklärt, weshalb Krankenhäuser vergleichsweise wenig IT-Mitarbeiterinnen und -Mitarbeiter beschäftigen. Rund ein Viertel müssen mit vier IT-Vollzeitkräften auskommen. Und die Krankenhausmanager sind mit Blick auf die Zukunft eher pessimistisch. Rund die Hälfte der Befragten erwartet, dass sich in ihren Häusern die Stellensituation im IT-Bereich verschlechtern werde. Nur rund ein Fünftel der Krankenhäuser geht von einer Besserung aus.

KI verlangt neue Konzepte

Die personellen Herausforderungen in der IT werden wachsen. Der Einsatz von KI wird die Digitalisierung beschleunigen und, wie in vielen Branchen, auch in der Medizin ganz neue Chancen bieten. Doch was passiert gegenwärtig? Die Euphorie in der Wirtschaft ist so groß, dass sie sich mit den Gefahren nicht genügend auseinandersetzt. Die Anwendung von KI schreitet rasant fort, während über Regelwerke jetzt erst nachgedacht wird. Diese Lücke ist gefährlich. Möglicher Schaden, der durch KI-Irrtümer und -Fehler in der Industrie und in anderen Branchen entsteht, kostet vielleicht viel Geld. Der Schaden im Gesundheits- und insbesondere im Krankenhauswesen kann Leben kosten.

Darum sollten die Spitzen der Gesundheitsbranche und speziell die Manager in den Krankenhäusern Konzepte entwickeln, wie KI in der Patientenversorgung geregelt zum Einsatz kommen kann. Und sie sollten jetzt an den Aufbau von Cyber-Security-Maßnahmen denken, bevor sie von der Technik überrollt werden.

Wer es genauer wissen will: Quellenangaben siehe Seite 78

Experten:

Prof. Dr. Volker Penter
Wirtschaftsprüfer, Steuerberater, Partner,
Advisory, Gesundheitswirtschaft
BDO AG Wirtschaftsprüfungsgesellschaft

Franziska Hain
Geschäftsführerin
BDO Cyber Security GmbH

Mehr zum Thema:
www.bdo.de/gesundheitswirtschaft

Foto: Adobe Stock

Hat auch jemand an die Finanzbericht-erstattung gedacht?

Cyber-Sicherheit aus Accounting-Sicht

Die digitale Transformation ist unstrittig einer der großen Megatrends der Gegenwart. Sie bietet sowohl im privaten, aber vor allem auch beruflichen Kontext immense Vorteile – kann jedoch auch gleichzeitig große Risiken für die Datensicherheit bergen. Immer dann, wenn Unternehmen nicht ausreichende und/oder wirksame Schutzvorkehrungen getroffen haben, kann die Digitalisierung – neben gestiegener Effizienz und Flexibilität in den Betriebsabläufen – auch schnell zum Einfallstor für Cyber-Angriffe werden. Die Motivation für solche Handlungen ist vielfältig und reicht von persönlichen über rein kriminelle bis hin zu politischen Beweggründen.

Für betroffene Unternehmen können Cyber-Attacken weitreichende Eigen- und Fremdschäden bedeuten. Welche Ausmaße es annehmen kann, wenn Cyber-Kriminelle sich beispielsweise Zugang zu medizinischen Geräten eines Krankenhauses verschaffen, haben wir in einem anderen Beitrag dieser Magazinausgabe bereits anschaulich beschrieben. Aber was ist eigentlich mit der Finanzberichterstattung von Unternehmen oder den zuvor beschriebenen Krankenhäusern – wie werden Ausgaben für Cyber-Sicherheit und vor allem Risiken sowie Schäden aus Cyber-Angriffen bilanziell abgebildet bzw. berichtet (nach IFRS und HGB)?

Implikationen für die Finanzberichterstattung vor einem Cyber-Angriff

Geeignete Schutzmaßnahmen für Cyber-Sicherheit können in Abhängigkeit von der Ausgangssituation kostspielig sein und umfassen nicht nur Risikoanalysen, das Nachrüsten der unternehmenseigenen Systemlandschaft oder die Implementierung eines Informationssicherheitsmanagementsystems, sondern auch die Sensibilisierung der Belegschaft sowie Einstellung bzw. Beauftragung von Spezialistinnen und Spezialisten für das Thema. Während Ausgaben für Schulungsmaßnahmen, interne Personaleinstellungen und/oder Beauftragungen von externen Spezialistinnen und Spezialisten periodengerecht als (Personal-)Aufwand erfasst werden, besteht Aktivierungspotenzial für Ausgaben der Informationstechnologie.

Entgeltlich erworbene Software für Cyber-Sicherheit erfüllt regelmäßig die Ansatzkriterien für einen immateriellen Vermögenswert bzw. Vermögensgegenstand. Entwicklungskosten für selbst geschaffene Cyber-Sicherheitssoftware sowie Weiterentwicklungen von bestehenden Applikationen können unter bestimmten Voraussetzungen ebenfalls aktiviert werden. Hierüber ist in der Bilanz sowie im Anhang zu berichten.

Auch wenn ausreichende Maßnahmen zur Cyber-Resilienz, d. h. Prävention von Cyber-Angriffen sowie Widerstandsfähigkeit für den Ernstfall, im Unternehmen implementiert wurden, verbleibt immer ein Restrisiko. Nicht alle Szenarien oder etwaige Sicherheitslücken können antizipiert werden, insbesondere wenn das Vorgehen und die Techniken von Cyber-Kriminellen sich schneller weiterentwickeln als die eigenen Schutzmaßnahmen. Sofern Unternehmen zunehmend einzelne Applikationen oder sogar ganze Bereiche der kritischen Infrastruktur nicht mehr auf eigenen Servern betreiben (on-premise), sondern Cloud-Dienste in Anspruch nehmen oder umfangreiches Outsourcing betreiben (z. B. Software as a Service, Platform as a Service, Infrastructure as a Service), können sich hieraus weitere Sicherheitsrisiken aufseiten des IT-Dienstleisters ergeben.

Foto: Adobe Stock

Des Weiteren verbleibt immer ein Restrisiko durch die handelnden Personen im Unternehmen, wenn beispielsweise Mitarbeiterinnen und Mitarbeiter in der Hektik des Arbeitsalltags eine eingehende Spam-Mail nicht richtig deuten und schädliche Anhänge öffnen oder sich mit unternehmenseigener Hardware, außerhalb der klassischen Büroräume, in unsichere Netzwerke einwählen.

Diese (Rest-)Risiken gilt es laufend zu identifizieren und zu beurteilen. Hierüber ist neben einer Erläuterung der getroffenen Schutzmaßnahmen im Chancen-Risiken-Bericht innerhalb des Lageberichts zu berichten. Für einige Branchen bestehen weitere (Mindest-)Anforderungen an das Risikomanagement und die Berichterstattung (z. B. Kreditinstitute). Wirft man einen Blick in die Jahresabschlüsse von DAX-Unternehmen, fällt schnell auf, dass über das Thema mit unterschiedlicher Intensität berichtet wird. Die im vergangenen Jahr in Kraft getretene EU-weite Gesetzgebung zur Cyber-Sicherheit (NIS2-Richtlinie) verpflichtet Unternehmen zu Maßnahmen der Resilienz. Damit steigt auch die Relevanz für effiziente Notfallbewältigung und die Einführung eines sogenannten Business Continuity Managements.[1] Konkrete Vorgaben zur Offenlegung von Mindestinformationen im Umgang mit Cyber-Risiken bestehen damit (noch) nicht. Die US-amerikanische Wertpapier- und Börsenaufsichtsbehörde SEC hat das Thema bereits weiter in den Fokus gerückt und ebenfalls im vergangenen Jahr erste Vorschriften zur Verbesserung und Standardisierung der Offenlegung von Informationen zum Risikomanagement, zur Strategie, Governance und zu Vorfällen im Bereich der Cyber-Sicherheit durch börsennotierte Unternehmen erlassen, die den Meldevorschriften des Securities Exchange Act von 1934 unterliegen.[2]

Implikationen für die Finanzberichterstattung nach einem Cyber-Angriff

Viele Cyber-Angriffe fallen in die Kategorie der sogenannten Ransomware-Angriffe, wobei Cyber-Kriminelle ausgewählte Unternehmensdaten mittels Schadprogrammen verschlüsseln und damit den Zugriff blockieren. Die Herausgabe bzw. Entschlüsselung der Daten ist dabei an eine Lösegeldforderung (ransom) gekoppelt. Kommt das Unternehmen der Lösegeldforderung nicht (zeitnah) nach oder kann es die Daten mithilfe von Expertinnen oder Experten wieder

Foto: Adobe Stock

zugänglich machen, können in Abhängigkeit von Daten und Branche erhebliche Störungen der Betriebsabläufe drohen.

Die Zahlung von Lösegeld schlägt sich unmittelbar liquiditätsmindernd im Zahlenwerk nieder, sofern in Abhängigkeit von der Lösegeldhöhe nicht sogar kurzfristig Kredite aufgenommen werden müssen (eine etwaige Strafbarkeit von Lösegeldzahlungen ausgeklammert). Auch ohne Lösegeldzahlung oder -forderung können erhebliche Schäden für das betroffene Unternehmen entstehen:

Nach Wiederherstellung des Datenzugriffs verbleiben potenzielle Verpflichtungen zur Begleichung von Eigen- und Fremdschäden (z. B. Ausgaben zu Wiederherstellung/Ersatz der Infrastruktur, Ausgaben für behördliche Untersuchungen und Strafzahlungen, Schadensersatz für Kundinnen und Kunden und Geschäftspartnerinnen und -partner), für die die Bilanzierung einer finanziellen Verbindlichkeit bzw. (Verbindlichkeits-)Rückstellung zu beurteilen ist.

Gestohlene Daten können bei Verwendung (z. B. Forschungsergebnisse) zu Wettbewerbsnachteilen oder in den Händen Unbefugter bzw. bei Veröffentlichung (z. B. sensible

Kundendaten) zu Datenschutzverletzungen führen. Werden durch den Cyber-Angriff Vermögenswerte bzw. Vermögensgegenstände der Produktion manipuliert, z. B. patentierte und aktivierte Software zum Betrieb einer Windenergieanlage oder der Elektronik eines Kraftfahrzeugs, können erhebliche Betriebsstörungen drohen und Kundenaufträge mitunter nicht pünktlich erfüllt werden. Wird die jeweilige Software ausgetauscht, ist mitunter eine Vollabschreibung der manipulierten Software geboten. Ein solcher Vorfall gibt in jedem Fall Anlass für einen Werthaltigkeitstest von einzelnen (immateriellen) Vermögenswerten bzw. -gegenständen oder der zugrunde liegenden zahlungsmittelgenerierenden Einheit.

Der durch einen Cyber-Angriff zusätzlich verursachte Image-Verlust ist schwer in Geldeinheiten zu messen. Börsennotierte Unternehmen werden erste Reaktionen unmittelbar nach Bekanntgabe der Ad-hoc-Mitteilung aus dem Aktienkurs ableiten können. Letztendlich kann der kumulierte Eigen- und Fremdschaden so materiell sein, dass mitunter die Fortführung der Unternehmenstätigkeit gefährdet ist und folglich besonderer Berichterstattungserfordernisse bedarf.

Die aufgeführten Implikationen für die Finanzberichterstattung stellen keine abschließende Liste dar, sondern werden vielmehr durch das Ausmaß und die durch den Cyber-Angriff betroffenen Bereiche sowie branchenspezifischen Besonderheiten des Unternehmens bestimmt. Es bedarf daher auf den Fall zugeschnittener Angaben im Jahresabschluss und Lagebericht unter Wahrung der Mindestberichterstattungserfordernisse nach IFRS und HGB. Voraussetzung dafür ist, und hier schließt sich der Kreis, dass die Aufbereitung von vollständigen Finanzdaten und Erfüllung von Dokumentationserfordernissen nicht durch die Auswirkungen des Cyber-Angriffs nachhaltig gestört sind.

Die gestiegene Bedrohung durch Cyber-Kriminelle soll keinen Anlass geben, die digitale Transformation nicht (wie geplant) voranzutreiben. Hierzu gehört aber nicht nur die Standardisierung und Automatisierung von Unternehmensprozessen, Harmonisierung der IT-Landschaft oder Bereitstellung von virtuellen Arbeits- und Kommunikationsmöglichkeiten. Einen ebenso hohen Stellenwert sollte dabei die Datensicherheit durch die Implementierung von ausreichenden und vor allem wirksamen Schutzmaßnahmen einnehmen, die es regelmäßig zu überprüfen und an sich ändernde Rahmenbedingungen anzupassen gilt. Letztlich stehen die zusätzlich einzuplanenden Budgets für Cyber-Sicherheit in keinem Verhältnis zu den sich aus einem Cyber-Angriff ergebenden (nicht-) monetären Eigen- und Fremdschäden.

Foto: Adobe Stock

Wer es genauer wissen will: Quellenangaben siehe Seite 78

Expertin:

Melanie Schunk
Wirtschaftsprüferin, Partnerin,
Accounting & Reporting Advisory Group

BDO AG Wirtschaftsprüfungsgesellschaft

Mehr zum Thema:
www.bdo.de/accounting-reporting

Die transformative Kraft des Internet der Dinge (IoT)

Foto: Adobe Stock

Chancen, Herausforderungen und die Notwendigkeit robuster Cyber-Sicherheit

Die fünf wichtigsten Kategorien von IoT-Geräten im Überblick

Smart-Home-Geräte: Diese Kategorie umfasst Geräte, die den Komfort und die Effizienz in Haushalten steigern sollen. Smart-Home-Geräte reichen von intelligenten Thermostaten, Beleuchtungssystemen, Schlössern und Heimsicherheitskameras bis hin zu sprachgesteuerten Assistenten wie Amazon Echo oder Google Home. Mit diesen Geräten können Benutzerinnen und Benutzer verschiedene Aspekte ihres Zuhauses aus der Ferne steuern und automatisieren und so den Komfort, die Sicherheit und die Energieeffizienz verbessern.

Tragbare Geräte: Tragbare Technologien haben an Bedeutung gewonnen und umfassen Geräte wie Smartwatches, Fitness-Tracker, Gesundheitsmonitore und intelligente Kleidung. Diese Geräte sammeln Daten über den Gesundheitszustand, das Fitnessniveau, die Aktivitätsmuster und die Vitalfunktionen der Benutzerinnen und Benutzer. Wearables bieten Einblicke in persönliche Gesundheitskennzahlen, fördern Fitnessziele und erleichtern die Fernüberwachung des Gesundheitszustands.

Industrie- und Fertigungssensoren: IoT-Geräte spielen eine wichtige Rolle in industriellen Umgebungen einschließlich Fertigung, Logistik und Lieferkettenmanagement. Sensoren und angeschlossene Geräte in Fabriken, Lagern und Produktionslinien sammeln Daten, um Prozesse zu optimieren, den Gerätezustand zu überwachen, vorausschauende Wartung zu ermöglichen und die Gesamtbetriebseffizienz zu verbessern.

Vernetzte Fahrzeuge: Die Automobilindustrie hat einen Anstieg der IoT-Integration erlebt, wobei Fahrzeuge mit Sensoren, GPS-Systemen und Konnektivitätsfunktionen ausgestattet sind. Diese vernetzten Autos sammeln und übertragen Daten für Navigation, Sicherheitsfunktionen, Fahrzeugdiagnose und Unterhaltungssysteme. IoT im Transportwesen erstreckt sich auch auf das Flottenmanagement und ermöglicht die Verfolgung und Optimierung der Fahrzeugleistung in Echtzeit.

Gesundheitsgeräte: IoT-Geräte im Gesundheitswesen umfassen eine breite Palette medizinischer Geräte und Systeme, wie z. B. Tools zur Fernüberwachung von Patientinnen und Patienten, intelligente medizinische Implantate, Medikamente-Management-Systeme und Telemedizin-Lösungen. Diese Geräte erleichtern die Gesundheitsüberwachung aus der Ferne, verbessern die Patientenergebnisse und ermöglichen es medizinischem Fachpersonal, eine individuellere und effizientere Pflege zu leisten.

Foto: Adobe Stock

Wir leben in einer Zeit des ständigen Wandels. Technologischer Fortschritt hat es uns über Jahrzehnte ermöglicht, unseren Wohlstand als Gesellschaft zu sichern und weiter auszubauen. Das „Internet der Dinge“ (IoT) stellt dabei einen Paradigmenwechsel im Bereich vernetzter Technologie dar und kündigt eine Zukunft an, in der Alltagsgegenstände kontinuierlich miteinander verbunden sind. Doch wo große Chancen auf uns warten, sind typischerweise auch Risiken nicht weit. Es entstehen neue Bedenken hinsichtlich Informationssicherheit, Datenschutz und Interoperabilität. Wenn immer mehr Geräte miteinander verbunden werden, steigt gleichzeitig die Anfälligkeit für Cyber-Bedrohungen. Und im Internet der Dinge warten Millionen neuer Geräte nur darauf, vernetzt zu werden. Allzu oft wird dabei aber Funktionalität und schnelle Markteinführung vor Sicherheit gestellt.

IoT – Was steckt dahinter?

Das „Internet of Things“ bezieht sich auf ein riesiges Netzwerk vernetzter Geräte, Maschinen und Objekte, das die generelle Effizienz verschiedener Anwendungsfälle, den Komfort für Anwenderinnen und Anwender und die Funktionalität in mehreren Domänen verbessern kann. Im Kern basiert es dabei auf dem Konzept der direkten Kommunikation zwischen (End-) Geräten, was auch Alltagsgegenstände einschließt. Es ermöglicht jenen Geräten, Daten zu sammeln, zu übertragen und auf deren Inhalt zu reagieren, ohne dass direkte, menschliche Interaktion notwendig wäre. So diente in den 2000er-Jahren u.a. der „smarte Kühlschrank“, der selbstständig Milch nachbestellen sollte, als plakatives Beispiel. Tatsächlich haben sich mittlerweile auf breiter Front „smarte“ Produkte durchgesetzt, die von Haushaltsgeräten über tragbare Geräte und Automobile bis hin zu Industriemaschinen, Infrastrukturkomponenten und vielem mehr reichen. Nicht nur gibt es für alles eine „App“, nein: Nahezu alles scheint heutzutage auch mit einer „App“ ausgeliefert zu werden. Es entstehen vernetzte, in Teilen beinahe eigenständig erscheinende Ökosysteme, die viele Vorteile mit sich bringen.

Immense Chancen durch IoT

Typischerweise unterscheiden sich dabei die „moderneren“ Varianten von zuvor bereits existierenden Produkten primär durch die Integration von Sensoren, Softwarelogik und Netzwerkkomponenten. Sensoren können je nach Verwendungszweck des Geräts verschiedene Umgebungsparameter erfassen, messen und überwachen – darunter Temperatur, Luftfeuchtigkeit, Bewegungen, den Standort und vieles mehr. Dadurch erhalten diese Geräte eine Form des „Bewusstseins“ für ihre Umgebung. Im vernetzten Schwarm können so riesige Datenmengen generiert und genutzt werden, die wiederum weitreichende Erkenntnisse, Muster und Analysen für eine fundierte Entscheidungsfindung liefern können. Beispielsweise können im Smart Home-Bereich IoT-fähige Geräte wie Thermostate, Lichter und Sicherheitskameras miteinander kommunizieren, um den Energieverbrauch zu optimieren, Sicherheitsprotokolle zu verbessern und den Bewohnerinnen und Bewohnern Komfort zu bieten, indem sie lernen und sich an ihre Vorlieben anpassen. Kombiniert man diese Fähigkeiten mit denen künstlicher Intelligenz, geraten Zukunftsforscherinnen und -forscher gerne ins Schwärmen. Ein Stück weit verbindet

Foto: Adobe Stock

das Internet der Dinge künstliche Intelligenz mit der realen Welt.

Darüber hinaus treiben auch bereits heute viele Unternehmen durch diese Technologie tragfähige Verbesserungen bei Effizienz und Funktionalität voran und sichern sich so Wettbewerbsvorteile. Im Rahmen der sogenannten Industrie 4.0 zum Beispiel revolutioniert das IoT Fertigungsprozesse durch den Einsatz vernetzter Maschinen und Systeme. Fabriken, die mit IoT-fähigen Sensoren und Geräten ausgestattet sind, können Abläufe rationalisieren, den Gerätezustand in Echtzeit überwachen, Wartungsbedarf vorhersagen und Produktionsabläufe optimieren, was letztlich zu einer höheren Produktivität und kürzeren Ausfallzeiten führt. Oft wird hier das Bild der sich selbst optimierenden Fabrik gezeichnet.

IoT als Sicherheitsrisiko

Auch wenn im IoT enormes Potenzial steckt, sind Sicherheitsrisiken, die die Technologie mit sich bringt, nicht zu vernachlässigen. Grundsätzlich steigt die Anfälligkeit für Cyber-Bedrohungen. Je mehr Produktkategorien sich vernetzen, umso exponentieller erhöht sich das damit verbundene Risiko. Und je mehr relevante Lebens- und Arbeitsbereiche von dieser Vernetzung betroffen sind, umso größer sind die potenziellen Auswirkungen im Schadensfall.

Es sind bereits mehrere Cyber-Sicherheitsvorfälle mit IoT-Geräten aufgetreten, die die Schwachstellen und Risiken im Zusammenhang mit vernetzten Systemen verdeutlichen. Ein Vorfall, der im Jahr 2021 besonderes Aufsehen erregt hat und das Ausmaß solcher Vorfälle verdeutlicht, war der „Hack" einer Wasseraufbereitungsanlage in Florida, USA: Dort verschafften sich Hacker mutmaßlich unbefugten Zugriff auf die Kontrollsysteme der Anlage und versuchten, den Gehalt an Natriumhydroxid (Lauge) in der Wasserversorgung auf gefährliche Werte zu erhöhen. Glücklicherweise wurde der Angriff erkannt und vereitelt, bevor Schaden entstand.

Dieser und viele weitere Vorfälle unterstreichen, wie wichtig es ist, IoT-Geräte und -Netzwerke vor Cyber-Bedrohungen zu schützen. Da sich das Internet der Dinge immer weiter ausdehnt und sich in verschiedene Aspekte des täglichen Lebens integriert, erreichen hierüber zuvor rein digitale Bedrohungen die reale Welt. Diese können diverse Lebensbereiche betreffen:

- **Datenschutzverletzungen:** z. B. Identitätsdiebstahl, unbefugte Überwachung oder Manipulation personenbezogener Daten
- **Cyber-Angriffe und Schwachstellen in der Infrastruktur:** z. B. Cyber-Angriffe auf kritische Infrastrukturen wie Stromnetze, Transportsysteme oder Wasseraufbereitungsanlagen
- **Gesundheits- und Sicherheitsrisiken:** z. B. falsche Diagnosen, Manipulation von Patientendaten oder Sabotage lebensrettender Geräte
- **Physische Sicherheit:** z. B. unbefugter Zugriff auf die Systeme vernetzter Autos

Foto: Adobe Stock

Experten:

Markus Diederichs
Partner, Converged Security, Cloud Security, Managed Detection & Response

Dr. Antje Winkler
Senior Managerin, Operational Technology (OT) Security

BDO Cyber Security GmbH

Mehr zum Thema:
www.bdosecurity.de

Sicherheitsrisiken vorbeugen, um Chancen zu nutzen

Auf Basis unserer Erfahrungen empfehlen wir Kundinnen und Kunden folgende Vorgehensweisen und Strategien, um kritische Cyber-Angriffe und -Bedrohungen zu verhindern.

1 **Security by Design:** Implementierung von Sicherheitsmaßnahmen in der Entwurfsphase von IoT- und OT-Systemen, einschließlich Verschlüsselung, Authentifizierung und regelmäßiger Updates.

2 **Segmentierung und Zugriffskontrolle:** Eine sinnvolle Netzwerksegmentierung und strenge Zugriffskontrolle begrenzen die Gefährdung und verhindern die Ausbreitung von Cyber-Bedrohungen innerhalb miteinander verbundener Systeme.

3 **Kontinuierliche Überwachung und Reaktion:** Einsatz von Echtzeit-Überwachungstools und Reaktionsplänen für Vorfälle, um Cyber-Bedrohungen umgehend zu erkennen und abzuwehren.

4 **Datenschutz und Privatsphäre:** Implementierung von Sicherheitsprotokollen, um Daten sowohl während der Übertragung als auch bei der Speicherung vor unbefugtem Zugriff oder Manipulationen zu schützen.

5 **Schwachstellenmanagement und Patching:** IoT-Geräte verfügen häufig über begrenzte Rechenressourcen, was Sicherheitspatches und -updates erschweren kann. Gerade deswegen kann eine kontinuierliche Überwachung auf Schwachstellen von entscheidender Bedeutung sein, um potenzielle Sicherheitslücken zu schließen, die Cyber-Kriminelle ausnutzen könnten. Regelmäßige Updates und Wartungsroutinen tragen dazu bei, die Sicherheitslage von IoT-Geräten und -Netzwerken zu stärken.

IoT-Technologie mit Sicherheit implementieren

Zusammenfassend lässt sich sagen, dass das Internet der Dinge eine transformative Kraft in der Technologielandschaft darstellt und eine Zukunft verspricht, in der vernetzte Geräte verschiedene Aspekte des täglichen Lebens, der Industrie, des Gesundheitswesens, des Transportwesens und darüber hinaus revolutionieren. Allerdings müssen die Herausforderungen in den Bereichen Sicherheit, Datenschutz und Interoperabilität sorgfältig berücksichtigt werden, um dieses Potenzial voll auszuschöpfen.

Die Konvergenz von IoT-Geräten und -Netzwerken bietet enorme Möglichkeiten für Innovation und Effizienz. Unternehmen und unsere Gesellschaft können stark vom Einsatz der IoT-Technologie profitieren, wenn sie das Potenzial einer enger vernetzten Welt erkennen und nutzen, ihre eigene IoT-Landschaft dabei sicher gedeihen lassen und sich vor möglichen Cyber-Bedrohungen schützen. Für eine sichere digitale Zukunft.

Wie Unternehmen von der nächsten Dimension der digitalen Transformation profitieren können

Metaversum: transformative Chance oder temporärer Hype?

Foto: Adobe Stock

Das Metaversum ist mehr als nur ein Hype: Es ist eine transformative Technologie, die das Potenzial hat, verschiedene Aspekte des täglichen Lebens und der Geschäftsabläufe von Unternehmen erheblich zu beeinflussen. Es kann die Art und Weise verändern, wie Unternehmen mit Kundinnen und Kunden in Kontakt treten, interne Prozesse verbessern und neue Geschäftsstrategien hervorbringen.

Die Ursprünge des Metaversums

Das sich rasch entwickelnde digitale Ökosystem hat die Aufmerksamkeit großer Technologieunternehmen auf sich gezogen. Seine Entwicklerinnen und Entwickler haben den Anspruch, die Zukunft der Wirtschaft damit maßgeblich zu beeinflussen. Obwohl die Idee einer virtuellen Realität wie des Metaversums nicht neu ist und bereits auf Ansätze aus den 1980er- und 1990er-Jahren zurückgeht, haben erst der technologische Fortschritt in den Bereichen hochleistungsfähiger Rechner sowie künstlicher Intelligenz und Internetbandbreite der letzten Jahre das Metaversum Wirklichkeit werden lassen. Seit Meta (vormals Facebook) im Jahr 2021 seine Metaversum-Plattform Horizon vorgestellt hat, sind zahlreiche weitere virtuelle Welten von verschiedenen Plattformentwicklern entstanden, die oft auch über eigene Kryptowährungen wie MANA oder SAND verfügen.

Das Metaversum ist ein digitaler Raum, der über Plattform- und Spielegrenzen hinausgeht und nahtlose Interaktionen ermöglicht, indem es virtuelle Realität (VR), erweiterte Realität (AR) und andere immersive Technologien miteinander kombiniert. So können Unternehmen das Metaversum beispielsweise nutzen, um Kundinnen und Kunden durch immersive Erlebnisse anzusprechen, Abläufe durch virtuelle Simulationen effizienter zu gestalten und Mitarbeiterinnen und Mitarbeiter durch virtuelle Kooperationsräume weiterzubilden. Konkret kann das Metaversum das Einkaufserlebnis revolutionieren, indem es Kundinnen und Kunden exklusive und ansprechende Räume bietet, in denen sie Produkte erkunden und Einkäufe tätigen können. Auch für Spiele und Social Media bietet das Metaversum neue Möglichkeiten der Nutzerbindung und der Monetarisierung von Diensten. Durch personalisierte und immersive Erlebnisse kann das Engagement gesteigert und die Kundenakquise und -zufriedenheit verbessert werden. Unternehmen können virtuelle Konferenzen, Meetings und Events im Metaversum abhalten und so ein interaktiveres und intensiveres Erlebnis für die Teilnehmerinnen und Teilnehmer schaffen. Angesichts dieser Vielfalt an Möglichkeiten für Unternehmen verwundert es nicht, dass der Finanzdienst Bloomberg das weltweite Geschäft im Bereich Metaversum für 2030 bereits auf rund 800 Mrd. US-Dollar schätzt [1].

Die unendlichen Möglichkeiten der virtuellen Welt

Menschen betreten das Metaversum aus verschiedenen Gründen, motiviert durch die einzigartigen Möglichkeiten, die es bietet. Für Unternehmen bzw. deren erfolgreiche Präsenz im Metaversum ist das Wissen über die Motivationslage der eigenen Zielgruppe von großer Bedeutung. Folgende Handlungsmotive begegnen uns in der Beratungspraxis und können unterschieden werden.

- **Chancen für Unternehmen und Marken:** Für Unternehmen bietet das Metaversum die Möglichkeit, digitale Inhalte zu erstellen und zu vermarkten, auf neue Weise mit Kundinnen und Kunden in Kontakt zu treten und innovative Marken- und Marketingstrategien zu erproben.
- **Handel mit digitalen Assets (z. B. Kryptowährungen):** Die Möglichkeit, im Metaversum in Kryptowährungen und andere digitale Assets zu investieren, zieht viele Nutzerinnen und Nutzer an.
- **Live-Unterhaltung und Kunst:** Ein beträchtlicher Prozentsatz der Menschen betritt das Metaversum, um Kunst und Live-Unterhaltung zu erleben, die oft auf immersive und interaktive Weise präsentiert werden.
- **Einzigartige Erlebnisse:** Menschen werden vom Metaversum angezogen, um Dinge zu erleben, die in der physischen Realität nicht möglich sind, wie z. B. virtuelle Reisen, Erkundungen und Aktivitäten.
- **Soziale Interaktion und Gemeinschaft:** Das Metaversum bietet eine Plattform für Menschen, um sich in einer virtuellen Umgebung zu vernetzen, Kontakte zu knüpfen und Gemeinschaften zu bilden, die neue Möglichkeiten der Interaktion mit anderen bieten.
- **Langlebige Plattform:** Im Gegensatz zu Web 2.0 und Social Media bietet das Metaversum eine langlebige Plattform, auf der Kreationen und Erlebnisse über einen längeren Zeitraum bestehen bleiben, was das Wachstum eines virtuellen Fußabdrucks und langfristiges Engagement ermöglicht.

- **Innovation und Technologie:** Das Metaversum stellt eine neue Grenze für Innovation, Technologie und die Entwicklung des Internets dar und zieht Menschen und Organisationen an, die daran interessiert sind, in diesem Bereich Pionierarbeit zu leisten.

Metaversum ist nicht gleich Metaversum

Im Laufe der bisherigen Entwicklung des Metaversums haben sich verschiedene Arten von Metaversen herausgebildet, jede mit ihren eigenen Eigenschaften und Anwendungsfällen. Die Kenntnis der Spezifika kann einen entscheidenden Erfolgsfaktor für Unternehmen darstellen. Die Haupttypen von Metaversen im Überblick.

- **Handels-Metaversum:** Diese Metaversen ermöglichen den Kauf und Verkauf von virtuellen Waren und Dienstleistungen, bieten Plattformen für Marken und Unternehmen und beinhalten oft virtuelle Währungen.
- **Bildungs-Metaversum:** Bildungs-Metaversen bieten immersive und interaktive Lernerfahrungen, virtuelle Klassenzimmer und Trainingssimulationen, um traditionelle Lernmethoden zu verbessern und fesselnde Bildungsumgebungen zu schaffen.
- **Soziales Metaversum:** Hier werden soziale Interaktionen und Verbindungen zwischen Benutzerinnen und Benutzern durch virtuelle Räume, individualisierbare Avatare, Chatsysteme und virtuelle Veranstaltungen gefördert.
- **Spielbasiertes Metaversum:** Dieser Typ konzentriert sich auf Spiele und interaktive Unterhaltungserlebnisse, in denen Spielerinnen und Spieler verschiedene Aktivitäten in virtuellen Universen durchführen können.
- **Dezentrales Metaversum:** Diese Art von Metaversum nutzt die Blockchain-Technologie und dezentralisierte Systeme, um Nutzerinnen und Nutzern die Möglichkeit zu geben, Anteile an der Plattform selbst zu erwerben und dadurch mehr Kontrolle und Transparenz zu erhalten.

Aktuelle Use Cases

Aktuelle Anwendungsbeispiele unterstreichen das Potenzial, das für Unternehmen im Metaversum steckt.

Siemens: Gemeinsam mit Nvidia strebt Siemens eine Vorreiterrolle auf dem Gebiet der industriellen Anwendung im Bereich Metaversum an. Dazu werden Industrieanlagen als digitaler Zwilling („digital twin") auf der eigens dafür entwickelten Xcelerator-Plattform abgebildet und für Schulungen, Wartungsarbeiten und Ähnliches genutzt. Zudem ermöglicht der digitale Zwilling ein kosteneffizientes Ausprobieren und Testen neuer Abläufe und dadurch wichtige Rückschlüsse für reale Anlagen.

Nike: Nike nutzt in Roblox seine virtuelle Präsenz als Nikeland, um für seine Produkte zu werben und mit der Gaming-Community in Kontakt zu treten. Das Unternehmen sponsert virtuelle Veranstaltungen und gibt exklusive virtuelle Gegenstände heraus, wie z. B. digitale Turnschuhe für Roblox-Avatare, die auch in der Offline-Welt erworben werden können. Nike unterstreicht dadurch den Ansatz einer Verzahnung zwischen Online- und Offline-Welten für Kundinnen und Kunden.

Foto: Adobe Stock

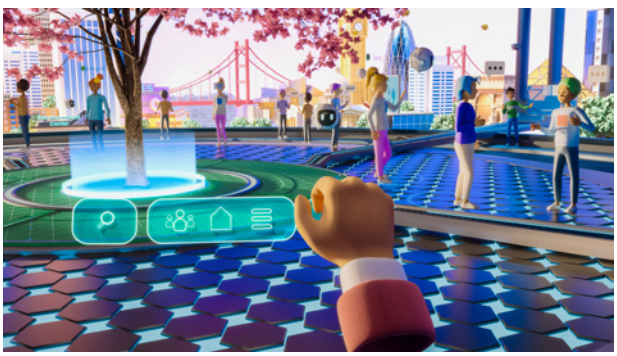


Foto: Adobe Stock

Foto: Adobe Stock

Erfolgreiches Community-Management im Metaversum

Durch den aktiven und sozialen Charakter des Metaversums und die verbundenen Implikationen für das Nutzungsverhalten ist ein kontinuierliches Community-Management essenziell. Erfolgreiches Community-Management im Metaversum erfordert ein Verständnis der besonderen Gegebenheiten und Möglichkeiten dieser neuen Umgebung, um stärkere Beziehungen zwischen den Mitgliedern aufzubauen und eine lebendige Community zu schaffen. Die virtuelle Welt bietet neue Möglichkeiten für den Aufbau von Markenbekanntheit und Kundenbindung, indem Community-Manager rinnen und -Manager eine positive und ansprechende Erfahrung für die Mitglieder schaffen, die sie dazu bringt, sich mit der Marke zu identifizieren.

Der erste Schritt ins Metaversum

Einige der wichtigsten Lektionen aus unserer Beratungspraxis für Unternehmen, die eine erfolgreiche Präsenz im Metaversum anstreben, sind die folgenden.

- **Frühzeitige Investition:** Trotz des Potenzials des Metaversums sind einige Unternehmen nach wie vor mit Investitionen zurückhaltend. Eine frühzeitige Investition kann jedoch entscheidend sein, um zu vermeiden, dass man im Vergleich zur Konkurrenz zurückfällt. Wesentlich ist hier fundierte Beratung bei der Auswahl selektiver Ansatzpunkte für die ersten Schritte im Metaversum – diese ermöglicht gleichzeitig einen objektiven Blick auf mögliche Cyber-Risiken, die es mit fundierten Präventionsmaßnahmen zu minimieren gilt.
- **Strategische Partnerschaften:** Unternehmen sollten in Erwägung ziehen, ihre Markenpartnerschaften aufeinander abzustimmen und in das Metaversum zu expandieren, um virtuelle Erlebnisse und Interaktionen zu schaffen. Ein strategischer Aufbau von Ökosystemen inklusive der Identifizierung und Auswahl geeigneter Partner (z. B. Technologie-Partner) unterstützt dieses.
- **Diversifizierung der Angebote:** Da sich das Metaversum weiterentwickelt, sollten Unternehmen verschiedene Angebote wie immersive soziale Interaktionen, NFT-VR-Erlebnisse und Virtual-Reality-Umgebungen erkunden, um den sich ändernden Bedürfnissen der Nutzerinnen und Nutzer gerecht zu werden. Expertinnen und Experten mit fundiertem Marktwissen und fortlaufende Analyse der Metaversen können helfen, ein differenziertes Bild zum Markt als Grundlage für eigene Ansätze zu gewinnen.
- **Marketing und Markenbildung:** Unternehmen sollten in Erwägung ziehen, das Metaversum für Marketinginitiativen und den Markenaufbau zu nutzen, und einen entsprechenden Marketingansatz für das Metaversum zielgerichtet entwickeln – von der ersten Idee bis zum fertigen Konzept.
- **Aufbau Community:** Der Aufbau einer Gemeinschaft (Community) im Metaversum ist ein entscheidender Aspekt bei der Schaffung einer erfolgreichen und ansprechenden virtuellen Umgebung. Es geht darum, ein Gefühl der Zugehörigkeit, der Akzeptanz und des Wachstums für die Teilnehmerinnen und Teilnehmer zu fördern.

Wer es genauer wissen will: Quellenangaben siehe Seite 78

Experten:

Dr. Roger Rihmland
Partner, Corporate Finance/Advisory

Dr. Oskar Colombo
Senior Consultant, Corporate Finance/Advisory

BDO AG Wirtschaftsprüfungsgesellschaft

Mehr zum Thema:
www.bdo.de/fintech

Auch Hacker nutzen ChatGPT

Generative KI kann für die Cyber-Security ein Segen sein. Sie wird aber zum Fluch, wenn Unternehmen und Personal nachlässig agieren

Foto: Adobe Stock

Seit der Veröffentlichung von ChatGPT sind noch nicht einmal eineinhalb Jahre vergangen. Aber generative KI, die ein enormes disruptives Potenzial für viele Bereiche in Unternehmen bietet, hat sich wie ein digitales Lauffeuer verbreitet. Eine Bitcom-Studie[1] gerade mal neun Monate später veröffentlicht, konstatierte einen „spürbaren Schub" für die deutsche Wirtschaft. 15 Prozent der befragten Unternehmen hatten bereits begonnen, generative KI tatsächlich anzuwenden. 68 Prozent halten KI für die wichtigste Zukunftstechnologie.

Von zentraler Bedeutung ist dabei auch der Bereich Cyber-Security, wo der Einsatz generativer KI sowohl Chancen für neue Anwendungsfälle bietet als auch eine sorgfältige Prüfung der Risiken erfordert. Bei der Integration dieser Technologien müssen hohe Sicherheitsstandards beachtet werden, um Innovationen sicher umzusetzen und effizient vor potenziellen Bedrohungen zu schützen.

Generative KI-Systeme verkörpern eine revolutionäre Entwicklung für Cyber-Security, weil sie das Potenzial haben, Schutzmechanismen neu zu definieren und anwenderorientiert anzupassen. Es gibt eine ganze Reihe von Bereichen, in denen generative KI signifikanten Cyber-Security-Mehrwert für Unternehmen bieten kann. Einige Beispiele im Überblick.

Phishing-Erkennung und -Abwehr

Phishing-Angriffe gelten als eine der am häufigsten auftretenden Cyber-Bedrohungen, da sie vor allem den Faktor Mensch als Angriffsziel wählen. Generative KI-Modelle sind durch ihr umfangreiches Sprachverständnis in der Lage, potenzielle Phishing-Mails kritisch zu hinterfragen und zu erkennen. Damit wird es möglich, immer besser werdende Phishing-Methoden zu erkennen, die bisherigen Filtermechanismen noch entgehen. Unternehmen stellen damit sicher, dass ihre Mitarbeiterinnen und Mitarbeiter vor solchen Angriffen besser geschützt sind, während gleichzeitig die Wahrscheinlichkeit von Datendiebstahl und anderen sicherheitsrelevanten Vorfällen minimiert wird.

Threat-Intelligence

Die Fähigkeit, aus einer Flut von Sicherheitsdaten relevante Informationen herauszufiltern und zu interpretieren, ist entscheidend, um einem Cyber-Angriff voraus zu sein. Generative KI kann hier als eine Art „intelligenter Assistent" fungieren und Sicherheitsanalystinnen und -analysten unterstützen, aus verschiedenen Quellen stammende Threat-Intelligence zusammenzufassen. Auch hier hilft wiederum das umfassende Sprachverständnis der KI, um allen voran auch unstrukturierte Daten wie Social-Media-Posts und News auszuwerten und in die Threat-Intelligence zu integrieren.

Automatisierung der Incident Response

Kein Unternehmen ist immun gegen Angriffe, doch die schnelle und effektive Reaktion kann das Ausmaß eines Schadens erheblich reduzieren. KI kann hierbei als Assistent eingesetzt werden, um menschliche Analystinnen und Analysten zu unterstützen, indem sie beispielsweise viele gleichzeitig eintretende Sicherheitswarnungen verarbeitet und priorisiert. Dank ihrer Fähigkeit, Quellcodes zu verstehen und zu schreiben, kann KI Entwicklerinnen und Entwickler unterstützen, vorhandene Sicherheitslücken schneller und effizienter durch Software-Patches zu schließen.

Ein regelmäßiges Thema für Aufsichts- und Beiräte

Die Potenziale von generativer KI in der Cyber-Security bedeuten erhebliche Chancen für Unternehmen, ihre Sicherheitsarchitektur zu festigen. Aufsichtsräte müssen sich heute bereits regelmäßig ein Bild von der Angemessenheit und Funktionsfähigkeit des Risikomanagements und des internen Kontrollsystems machen. Durch entsprechende Investitionen und einen sachgerechten Einsatz von KI-Technologien können Risiken gemindert und Wettbewerbsvorteile erzielt werden. Daher gehört das Thema regelmäßig auf die Agenda von Gremiensitzungen.

Neue Risiken im Bereich Cyber-Security

Das für die Cyber-Security typische Katz-und-Maus-Spiel setzt sich auch mit KI-Technologie fort. Denn auch Angreiferinnen und Angreifer setzen die Möglichkeiten der generativen KI ein, um etwa immer bessere Phishing-Mails zu generieren, die sprachlich nahezu perfekt erscheinen und gleichzeitig nicht mehr nur den typischen Fall von „Ihr Paket kann nicht zugestellt werden – bitte klicken Sie hier!" abdecken, sondern äußerst kreativ vorgehen. Ein Einsatz von KI aufseiten der Verteidigung wird damit unumgänglich. Denn auch die ausgeprägtesten Awareness-Schulungen werden künftig nicht mehr verhindern können, dass Beschäftigte auf eine nahezu perfekte Angriffsmail hereinfallen. Wohl aber ist KI in der Lage, die typischen Kommunikationsmuster eines Individuums zu erkennen, und damit auch Nachrichten, die nicht in das Muster passen.

Der Fall Samsung: geheime Daten öffentlich

Das Unternehmen Samsung musste bereits im April 2023 die Erfahrung machen, dass Ingenieurinnen und Ingenieure geheime Daten in ChatGPT übergeben hatten, um Fehlerbehebung im Quellcode vorzunehmen. Dabei gelangten diese Informationen unbeabsichtigt an die Öffentlichkeit. Vielen Mitarbeiterinnen und Mitarbeitern ist nicht bewusst, dass Daten, die in generische KI-Modelle eingegeben werden, in manchen Situationen zu Trainingszwecken verwendet und außerhalb der EU verarbeitet werden. Dies geschieht beispielsweise, wenn Mitarbeiterinnen und Mitarbeiter ihren privaten ChatGPT Account nutzen und darüber Mails oder Texte für ihre berufliche Tätigkeit generieren lassen. So haben laut einer Studie von CISCO bereits 62 Prozent der Befragten Informationen über interne Prozesse in generative KI Tools eingegeben.[2]

Sicherheitsrelevante Daten können auf diese Weise kompromittiert werden. Eine Angreiferin oder ein Angreifer kann ein KI-Modell mit spezifischen Inputs füttern und aus den Outputs Rückschlüsse auf die ursprünglich trainierenden Daten ziehen. Dennoch ist es unverzichtbar für Unternehmen, Mitarbeiterinnen und Mitarbeitern die Möglichkeit zu geben, mit KI zu arbeiten. Gebannt werden kann dieses Risiko durch einen „Inhouse-GPT-Ansatz". Er stellt sicher, dass alle Daten innerhalb der sicheren Grenzen des Unternehmensnetzwerks bleiben und nicht für externe Trainingszwecke genutzt oder außerhalb der EU verarbeitet werden.

Dadurch ist es möglich, Mitarbeiterinnen und Mitarbeitern den Zugang zu generativer KI zu eröffnen und gleichzeitig Risiken zu vermeiden. E.ON beispielsweise bietet seinen 74.000 Beschäftigten das „E.ON GPT" [3] an, womit unter anderem aufwendige Rechercheprozesse zu energiewirtschaftlichen Fragestellungen deutlich vereinfacht werden.

Foto: Adobe Stock

Foto: Adobe Stock

Ein Blick in die Zukunft

Im Rahmen der fortschreitenden Entwicklung der KI wird Cyber-Security noch wichtiger werden, als sie es ohnehin bereits ist. Je stärker wir generative KI in unsere Unternehmensprozesse integrieren, umso stärker müssen wir dabei auch auf die Integrität und Sicherheit von Unternehmensdaten achten.

Sowohl Aufsichtsräte als auch Vorstände werden sich verstärkt mit Trends und Innovationen im Bereich KI beschäftigen müssen und die damit verbundenen Chancen und Risiken bewerten. Ihre Verantwortung wird nicht nur in der Überwachung und Begleitung der Transformation durch KI liegen, sondern auch darin, sicherzustellen, dass die Cyber-Security-Strategie ihres Unternehmens mit den technologischen Weiterentwicklungen Schritt hält.

Das Management wird aktiv zur Gestaltung einer Firmenkultur beitragen müssen, die die Dualität von Innovation und Sicherheit harmonisiert und das Unternehmen sowohl wettbewerbsfähig als auch resilient gegenüber Cyber-Bedrohungen macht.

Wer es genauer wissen will:
Quellenangaben siehe Seite 78

Experte:

Philipp Tiedt
Partner
BDO AG Wirtschaftsprüfungsgesellschaft
Managing Director
VICO Research & Consulting GmbH

Mehr zum Thema:
www.bdo.de/ai-sm-intelligence

Anruf vom Fake President

Deep Fakes: zwischen Faszination und Bedrohung – Einblicke in die Welt der digitalen Illusionen

Foto: Adobe Stock

In einem Vorstandsbüro eines britischen Energieunternehmens klingelt 2019 das Telefon. Der CEO erhält einen Anruf vom Chef der deutschen Muttergesellschaft. Die Stimme, so authentisch und vertraut, instruiert die dringende und diskrete Überweisung von 220.000 Euro – und verspricht die Erstattung derselben Summe wenige Tage später. Der britische Manager überweist das Geld, doch erhält es nie vom Chef zurück. Stattdessen kommt einige Zeit später die Versicherung der Bank für den Schaden auf, wie die Süddeutsche Zeitung damals berichtet.[1] Es ist ein perfekt inszenierter Betrug – ein Deep Fake, eine synthetisch erzeugte Stimme*, geschaffen von einer neuen Generation Cyber-Krimineller.

„Deep Fakes markieren den Anfang einer neuen Ära der digitalen Täuschung. Sie vermischen Realität und Fiktion auf eine Weise, die nicht nur beeindruckend, sondern auch beängstigend ist", sagt Jannis Frech, Medienforscher in der Journalistik und Kommunikationswissenschaft an der Universität Hamburg. Die Ursprünge der Technologie liegen in der Kombination von künstlicher Intelligenz und maschinellem Lernen. Entwickelt für harmlose Anwendungen wie Filmproduktion und Spiele, ermöglicht der technologische Fortschritt die Erstellung täuschend echter Bilder, Videos und Audiodateien. Algorithmen werden eingesetzt, um gefälschte E-Mails oder Phishing-Nachrichten zu verfassen, die auf den ersten Blick authentisch wirken – Schreibstil, Ausdrucksweise und Sprachmuster einer bestimmten Person können analysiert und imitiert werden.

Belastbare Zahlen vom Bundesamt für Sicherheit in der Informationstechnik für eine Zunahme der Deep-Fake-Attacken gibt es bislang nicht. Das Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS führt das in seinem White Paper 2021[2] darauf zurück, dass viele Wirtschaftsstraftaten ohne polizeiliche Beteiligung bearbeitet werden. Das Bundeskriminalamt schreibt in seinem Lagebericht zur Wirtschaftskriminalität 2022[3] nur: „Die technische Entwicklung im Bereich der künstlichen Intelligenz dürfte den Tätergruppierungen neue Möglichkeiten zur Tatbegehung eröffnen."

Millionenbeute mit Fake-Anrufen und E-Mails

Ein deutlicheres Bild zeigt die Jahresstatistik der Allianz Versicherung[4]. Demnach sei die Fallzahl 2022 um 17 Prozent gestiegen – noch vor dem Launch von ChatGPT, in dessen Folge ein Sprecher der Versicherung einen weiteren Anstieg der Fälle befürchtet. Die Schadenssummen beim sogenannten „Fake President"-Betrug belaufen sich laut dem Bericht bei den meisten Fällen auf „hohe sechsstellige Summen" oder einen „niedrigen einstelligen Millionenbetrag". Das zeugt von einem Rückgang. Zwischen 2014 und 2017 verursachen Betrügerinnen und Betrüger laut der Versicherung häufig noch Schäden zwischen zehn und 50 Millionen Euro. Die Gesamtschadensumme der deutschen Wirtschaft durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage – worunter auch die Deep Fakes fallen – beziffert der Branchenverband Bitkom im Jahr 2023 mit 206 Milliarden Euro.

Besondere Aufmerksamkeit erlangt ein Fall während der Weihnachtsfeiertage im Jahr 2015. Betrüger erbeuten damals mit einer vermeintlichen Mail des Vorstands 53 Millionen Euro beim chinesisch-österreichischen Luftfahrtzulieferer FACC, wovon lediglich elf Millionen Euro zurückverfolgt und wiedererlangt werden können. In Deutschland fällt der Automobilzulieferer LEONI auf einen ähnlichen Trick herein und überweist 2016 40 Millionen Euro nach China und Hongkong, was zu einem Kurssturz der Aktie im M-Dax führt – wegen „offenbar fehlenden Sicherheitssysteme bei LEONI", wie das Manager Magazin damals schreibt[5].

*** Synthetisch erzeugte Stimme**

Die Software Lyrebird ermöglicht es, mittels künstlicher Intelligenz die eigene oder eine andere Stimme so zu speichern, dass über die Tastatur eingetippte Sätze in gewünschter Stimmfarbe maschinell nachgesprochen werden.

Foto: Adobe Stock

Die Angreiferinnen oder Angreifer werden selten ausgemacht – oder aus ermittlungstaktischen Gründen nicht genannt. Doch hinter vielen Deep Fakes werden gut organisierte Cyber-Kriminelle oder staatlich gesponserte Hackergruppen vermutet, die auf finanziellen Gewinn oder geopolitische Destabilisierung abzielen. RA Prof. Dr. Hendrik Schneider, Rechtswissenschaftler und Kriminologe, unterscheidet zwischen Gelegenheitssuchern und Gelegenheitsgreifern sowie unterschiedlichen Tätertypen, die zum Beispiel auf Krisen reagieren, in einer Abhängigkeit stehen oder bislang völlig unauffällig waren. „Wirtschaftsstraftäterinnen und -täter sind ‚Latecomer to crime', also Spätzünder bei der kriminellen Karriere", sagt er in einem Interview mit der Allianz Versicherung [4]. „Das hat mehrere Gründe. Ein Uni-Absolvent hätte zum Beispiel gar nicht die Befugnisse, Transaktionen mit hohen Geldbeträgen anzuweisen. Ein Manager mit langer Betriebszugehörigkeit weiß hingegen, wie der Hase läuft, wo Nischen und Kontrolldefizite sind, und hat die notwendigen Befugnisse. Da ist bei dem einen oder anderen die Verlockung groß, eine günstige Gelegenheit auszunutzen. In eine solche Führungsposition kommen allerdings nur selten Menschen, deren polizeiliches Führungszeugnis Eintragungen aufweist. Das heißt: Eine bis dato weiße Weste ist für die Weiße-Kragen-Täter die Grundvoraussetzung."

Gegenmaßnahmen und Chancen

Die Weiterentwicklung von Deep-Fake-Technologien stellt eine anhaltende Herausforderung für die Wirtschaftswelt dar. Experten wie Jannis Frech betonen die Bedeutung von Aufklärung und technologischen Gegenmaßnahmen: „Es ist entscheidend, dass wir fortschrittliche Erkennungstechnologien entwickeln und gleichzeitig die Öffentlichkeit über die Risiken von Deep Fakes aufklären." Eine wirksame Strategie im Kampf gegen Deep-Fake-Attacken ist das Training von Angestellten, um ein kritisches Verständnis für die Identifikation von Fälschungen zu entwickeln. Das Bewusstsein über die Merkmale von Deep Fakes – wie inkonsistente Gesichtstexturen oder unpassende Lichtverhältnisse – hilft, Echtheit von Täuschung zu unterscheiden. Besonders bei Live-Anwendungen, wo Angreiferinnen und Angreifer keine Chance zur Nachbearbeitung haben, kann solches Wissen Fälschungen entlarven.

Gleichzeitig ist es unerlässlich, vorausschauend zu agieren und potenzielle Risiken, die sich aus der fortschreitenden Digitalisierung, steigenden Cyber-Kriminalitätsraten und neuartigen Technologien wie etwa fortschrittlichen KI-Systemen ergeben, zu antizipieren. Die Generationenfrage wird dabei immer wichtiger, wie Prof. Schneider sagt. „Das ist tatsächlich auch ein Generationenthema: Es wichtig, auch junge, technologieaffine Mitarbeiterinnen und Mitarbeiter im Boot zu haben, die sich der damit verbundenen Risiken bewusst sind. Das gilt im Übrigen sowohl für Compliance als auch für Aufsichtsräte. Man kann auch einfach

einen Selbsttest machen und es ausprobieren. Schicken Sie doch mal eine ChatGPT-Mail in die eigene Organisation. Damit identifizieren Sie gnadenlos die eigenen Schwachstellen bei Prozessen und Kontrollmechanismen. Sie können dann nachjustieren, bevor es zu finanziellen Schäden kommt."

Fake Presidents lassen Aktienkurse einbrechen, ruinieren Karrieren und manipulieren Menschen in Form von falscher Propaganda. Doch es gibt auch positive Anwendungen der Technologie. „Während wir sehen, wie Deep Fakes für unlautere Zwecke missbraucht werden, dürfen wir nicht vergessen, dass sie auch großes Potenzial für positive Anwendungen haben. Eine solche Dualität finden wir häufig bei technologischen Durchbrüchen", sagt Frech. So hat zum Beispiel die Nachrichtenagentur Reuters begonnen, Deep Fakes zu nutzen, um Nachrichten in verschiedenen Sprachen zu synchronisieren – und damit einer größeren Öffentlichkeit zugänglich zu machen; eine Modekette bietet digitale Anproben neuer Kleidung am eigenen digital erstellten Abbild an – und auch die Werbung hat das Potenzial erkannt: Eine Kampagne zur Aufklärung über Malaria lässt David Beckhams Avatar in neun Sprachen über die Krankheit aufklären.

Die Verantwortung für die Nutzung dieser Technologie liegt jedoch nicht allein bei den Führungskräften, sondern erfordert ein kollektives Bemühen aller gesellschaftlichen Ebenen. „Die Herausforderungen, die Deep Fakes mit sich bringen, sind nicht nur technischer Natur, sondern betreffen unsere gesamte Gesellschaft. Es liegt in der gemeinsamen Verantwortung von Unternehmen, Behörden sowie jeder und jedem Einzelnen, diese Technologie verantwortungsvoll zu nutzen und ihre Integrität zu wahren – das ist auch eine neue Chance für den Online-Journalismus", betont Jannis Frech. Abschließend fügt er hinzu: „Die digitale Revolution fordert uns heraus, aber sie bereichert auch unser Potenzial – es ist an uns allen, diesen Weg nachhaltig zu gestalten." MB

Wer es genauer wissen will: Quellenangaben siehe Seite 78

Foto: Adobe Stock

„Gutes Handwerk ist die Grundlage“

Foto: © offenblende.de

Foto: © offenblende.de

Direkt an der Mosel liegt eines der berühmtesten deutschen Weingüter: Die Rot- und Weißweine von Winzer Markus Molitor sind in der ganzen Welt bekannt und begehrt. Wie hat er das geschafft? Ein Treffen.

Markus Molitor führt das Weingut in achter Generation.

Es geht nach Rheinland-Pfalz. Vorbei an verschiedenen kleinen Orten mit hübschen Namen wie Traben-Trarbach oder Bernkastel-Kues, dann über mehrere Landstraßen – bis man schließlich um eine Kurve biegt und da liegt es dann: ein großes Anwesen aus hellem Stein.

Die Fassade glitzert in der Sonne, eine große Treppe führt zum Hauseingang hinauf. Das ist das Weingut Markus Molitor – eines der bekanntesten deutschen Weingüter, geführt von Markus Molitor persönlich. Molitor selbst ist aber noch nicht zu sehen, er sei gerade noch bei der Arbeit, komme aber gleich nach, lässt er ausrichten. So lange könne man gern in der Vinothek warten.

Die Vinothek ist ein Raum, in dem für mögliche Interessierte – etwa Sommelièren und Sommeliers – die verschiedenen Weine des Guts zur Verkostung angerichtet sind. Auf einem länglichen Tisch stehen hier Weinflaschen und Gläser bereit, dazu Listen, auf denen die verfügbaren Flaschen vermerkt sind. Über allem liegt ein leichter und angenehmer Geruch nach Wein. „Es riecht gut, oder?“, sagt Markus Molitor.

Mitten in der Hauptsaison

Molitor steht plötzlich – begleitet von einem großen grau-weißen Hund – mitten in der Vinothek, hat den Raum offenbar über eine schmale unauffälligere Seitentür betreten. Er schmunzelt: „Ich finde: Genau so sollte es auch riechen – dann weiß man immerhin direkt, wo man ist. In einem Haus, in dem sich wirklich alles um den Wein dreht."

Molitor ist um die 60, groß und schlank. Er hat dunkle Haare und ein freundliches Gesicht mit Lachfalten. Er ist direkt von der Arbeit gekommen. „Wir sind gerade mitten in der Saison", erklärt er, „für uns sind diese Wochen die wichtigsten im Jahr." Erst die Traubenernte, „dann verarbeiten wir die Trauben, füllen den Wein ab …".

All das geschehe in diesem Zeitraum. „Deswegen ist aktuell viel zu tun." Denn Molitor ist derjenige, der für alles hier verantwortlich ist. Er führt das Weingut – schon in achter Generation. „Ach, ob achte, zehnte oder zwölfte Generation, das ist doch egal", sagt er. Er legt offensichtlich keinen Wert auf solche Superlative. „Wichtig ist nicht, aus welcher Familie man stammt, sondern wie man sein Handwerk versteht", erklärt er.

Und er ist jemand, der sein Handwerk grandios versteht. So hat er mit seinen Weinen schon diverse Auszeichnungen gewonnen. Was ist es also, das er so besonders gut macht? „Ob ich irgendwas besonders gut mache, müssen andere beurteilen", sagt er und winkt ab. „Aber ich kann erzählen, was ich genau wie und warum gemacht habe." Er setzt sich hin und deutet seinem Hund, sich neben ihn zu setzen. „Riesling, sitz!", sagt er.

Und dann erzählt er.

Foto: © offenblende.de

> ICH HABE GEDACHT: ICH GEBE NICHT AUF. ICH PROBIERE ES TROTZDEM.

Die Weine von Molitor haben zahlreiche Auszeichnungen gewonnen.

„Der Junge ist durchgedreht, haben sie gedacht"

„Ich bin auf dem elterlichen Weingut aufgewachsen", sagt Molitor und räuspert sich: „Aber das war damals ein wenig anders als dieses Gut heute." Damals – in den 70er- und 80er-Jahren – war das familiäre Weingut deutlich kleiner, gerade mal einen Hektar groß und umgeben von vielen weitläufigeren Gütern. „Aber dann kam eine Krise für den Moselwein, für den Riesling. Er war nicht mehr so beliebt, hatte kein gutes Image mehr, galt plötzlich nicht mehr als fein."

Die Moselweine wurden nicht mehr gut verkauft und viele größere Güter mussten aufgeben. Molitor selbst war damals gerade 20 Jahre alt und frisch zum Chef des Familienguts ernannt worden – und er sah natürlich, dass die Weine in der Krise steckten. „Ich habe aber gedacht: Ich gebe nicht auf. Ich probiere es trotzdem. Ich glaube noch an unsere Weine. In denen steckt eine tolle Qualität." Viele hätten ihn für verrückt gehalten.

„Der Junge ist durchgedreht, haben sie gedacht", erinnert sich Molitor und schmunzelt, „und vielleicht sah es damals auch wirklich so aus." Aber er ließ sich von all den Unkenrufen nicht beirren. Im Gegenteil: Er nahm Kredite auf und pachtete – zusätzlich zu den eigenen Anbauflächen seines Weinguts – noch weitere Flächen von den anderen Gütern, die aufgegeben hatten.

„Diese Flächen sind beim Weinanbau entscheidend“, sagt er.

Er pachtete immer mehr dazu und so wuchs sein Weingut schnell an, „bald waren es ungefähr acht Hektar, dann zehn, dann zwanzig.“ Und damit machte sich Molitor an die Arbeit. „Ich hatte schon damals eine ziemlich klare Vorstellung davon, was ich mit dem Weingut und den Flächen machen wollte: Ich wollte gute Handwerksarbeit leisten und damit wirklich guten Wein herstellen. Hervorragenden Wein. Den besten Wein, der mir möglich war.“

Arbeit, Disziplin und Durchhaltewillen

Um den bestmöglichen Wein zu produzieren, legte Molitor dabei schon damals großen Wert auf die Art der Herstellung. „Alles sollte manuell geschehen. Unsere Mitarbeiterinnen und Mitarbeiter gingen in den Weinberg und sortierten die Trauben händisch. Sie schauten sich jede Traube genau an und nur die wirklich guten Trauben wurden dann von uns weiterverarbeitet.“ Diese Art der Traubenernte war zwar komplizierter, kostenintensiver und anstrengender.

Aber sie brachte auch deutlich bessere Ergebnisse. „Das war entscheidend. Denn die Trauben, also das Grundprodukt, mussten stimmen“, sagt Molitor, „nur dann konnte daraus auch etwas wirklich Gutes entstehen.“ Die Verarbeitung der Trauben danach habe er ebenfalls möglichst naturbelassen haben wollen – ohne stabilisierende Zusätze. „Das hört sich alles einfach an, aber es steckte gerade deshalb so viel Arbeit drin“, fügt er hinzu.

Foto: © offenblende.de

Das Weingut hat mittlerweile viele Fans gewonnen.

Und vor allem auch Arbeit, Disziplin und Durchhaltewillen von ihm persönlich. Er hatte schließlich immer das Risiko im Hinterkopf, das er auf sich genommen hatte, um seinen Wein herzustellen. Er sei jeden Morgen der erste Mensch gewesen, der in die Weinberge gegangen sei, und abends der letzte, der sie wieder verlassen habe. Genau diese Leidenschaft sorgte dafür, dass seine Weine tatsächlich von hervorragender Qualität waren.

„Das war ernüchternd“

Allerdings bemerkten das zuerst nur wenige Menschen. „Das war ein wenig ernüchternd. Ich legte mein ganzes Herzblut in meine Weine und irgendwie schien das trotzdem niemanden zu interessieren“, erinnert sich Molitor. Anfang der 90er sei er etwa in Bordeaux auf einer zehntägigen Weinmesse gewesen und dort seien die Menschen einfach an seinem Stand vorbeiflaniert. „Sie wollten nicht einmal probieren, sind direkt weitergegangen“.

Nur einmal seien zwei Journalisten bei ihm stehen geblieben, hätten Interesse bekundet und gesagt, sie wollten „um die Osterzeit herum“ mal vorbeischauen bei ihm auf dem Weingut an der Mosel. „Ich habe mich sehr über diese Ankündigung gefreut, schon alles für die beiden vorbereitet und stand die gesamte Osterzeit bereit für deren Besuch“, erinnert sich Molitor und runzelt die Stirn: „Aber es tauchte nie irgendjemand auf.“

Das habe ihn damals sehr getroffen und ihm schlaflose Nächte beschert. Aber er ließ sich nicht davon niederdrücken, machte weiter wie bisher. Mit der Leidenschaft für sein Handwerk, mit möglichst natürlichen Prozessen, mit qualitativ hochwertigen Trauben. Und er wurde dafür belohnt: Im Laufe der Zeit kamen zwar die beiden Journalisten nicht vorbei, dafür aber immer mehr andere Menschen – und sie mochten seine Weine.

Immer mehr kauften bei ihm ein. Und auch einige sehr gute Restaurants in der Umgebung nahmen seine Flaschen mit in ihre Karte auf. Und dann kam das Jahr 1998 – und der „Gault-Millau“-Guide für die Wein-Jahrgänge 1997. Der Gault-Millau – eine Bibel für alle Feinschmeckerinnen und Feinschmecker – erwähnte in dieser Ausgabe die Weine von Molitor – und das Weingut Molitor wurde dort zu einem der besten deutschen Weingüter gekürt.

„Ich habe den Anruf bekommen und konnte es zuerst gar nicht glauben“, sagt Molitor und schmunzelt: „Und dann, als ich es geglaubt habe, war ich einfach nur noch glücklich.“

In der Vinothek des Weinguts werden Sommelièren und Sommeliers aus aller Welt empfangen.

Foto: © offenblende.de

Das Weingut Molitor liegt im kleinen Örtchen Bernkastel-Wehlen, direkt an der Mosel, und produziert rund 80 verschiedene Weinsorten. Die Preise variieren zwischen 11,90 Euro beispielsweise für einen Pinot blanc oder einen Riesling – und 85 Euro für eine 2015 Bernkasteler Lay Auslese ***. Alle Weine sind im Online-Shop www.markusmolitor.com erhältlich.

Zur Preisverleihung sei er dann nach Hamburg gefahren – und „erst da, als ich dort stand mitten auf dieser Gala, erst da konnte ich wirklich glauben, was gerade passierte. Mein Weingut gehörte nun tatsächlich zu den besten in ganz Deutschland!“

„Der Wein war ein absolutes Erlebnis“

Nach der Auszeichnung war dann auch offiziell, was zuvor nur einem kleinen Kreis aus Insidern bekannt gewesen war: Die Weine von Markus Molitor waren herausragend und Molitor selbst als Winzer extrem gut. So etwas würde Molitor zwar nicht sagen, er ist zu bescheiden, um sich selbst zu loben – aber das muss er auch gar nicht, das tun andere für ihn. „Ich habe schon vor Jahren einen Molitor-Wein geschenkt bekommen“, erinnert sich Parwäz Rafiqpoor, Vorstandsvorsitzender von BDO.

Foto: © offenblende.de

Die Weine werden in 65 Länder geliefert, sind weltweit begehrt.

Zuerst habe er nichts mit dem Namen anfangen können, aber dann habe er irgendwann gemeinsam mit seiner Frau die Flasche geöffnet und probiert. Beide seien begeistert gewesen. „Bei wirklich guten Weinen schmeckt es nicht nur, man hat eine richtige körperliche Reaktion – und so war es bei uns bei dem Wein von Markus Molitor. Es war ein absolutes Erlebnis!“ Er sei bald danach extra persönlich zum Weingut gefahren, um mehr darüber zu erfahren.

„Herr Molitor hat uns damals geöffnet. Er hatte keine Ahnung, wer wir sind und warum da plötzlich zwei begeisterte Menschen vor seiner Tür stehen und unbedingt mehr über seinen Wein erfahren wollen.“ Aber er habe sie hineingelassen und seitdem seien er, Rafiqpoor, und seine Frau sogar noch größere Fans des Weinguts. „Wir bestellen hier regelmäßig – man schmeckt einfach, dass Herr Molitor sein Handwerk von Grund auf versteht.“

Während dieser Lobeshymne auf ihn und seine Weine steht Molitor daneben. Er lächelt, freut sich sichtbar über die schönen Worte über seine Arbeit, „es freut mich, wenn jemandem meine Arbeit gut gefällt“ – und dann erzählt er weiter seine Geschichte: Nachdem er – neben Parwäz Rafiqpoor – immer weitere Weinkennerinnen und Weinkenner aus ganz Deutschland für seine Flaschen begeistern kann, wächst sein Ruf als Winzer immer weiter.

100 von 100 möglichen Parker-Punkten

Molitor gewinnt weitere Auszeichnungen – unter anderem erhält er 23-mal 100 von 100 Punkten in der Wertung von Robert Parker. Parker, der den Newsletter „The Wine Advocate“ herausgibt, ist so mächtig, dass nach seinen Bewertungen die Preise von Weinen festgelegt werden;

Markus Molitor zeigt Parwäz Rafiqpoor das Weingut.

Foto: © offenblende.de

in den USA ist es gang und gäbe, dass auf den Preisschildern für Weine jeweils auch die „Parker-Punkte“ (PP) für die jeweilige Flasche angegeben werden.

23-mal 100 von 100 Punkten auf der Liste von Robert Parker … das ist also ungefähr so, als würde ein Fußballverein gleich mehrere Male hintereinander die Champions League für sich entscheiden. Andere Winzer würden diese Auszeichnung auf ihre Visitenkarten drucken lassen und ununterbrochen erwähnen. Und Molitor? „Es ist schön, wenn die eigene Arbeit gewürdigt wird“, sagt er, zu mehr Eigenlob lässt er sich nicht hinreißen.

Braucht er auch nicht, die Zahlen sprechen für sich: Mittlerweile liefert er in 65 Länder, unter anderem nach Frankreich, Italien, Spanien, in die USA, die Vereinigten Arabischen Emirate. Überall auf der Welt stehen seine Weine auf der Karte. Mit seinem Ruf ist auch sein Weingut immer weiter angewachsen. Rund 120 Hektar beträgt es aktuell, auf dieser wirklich großen Fläche arbeiten rund 130 Mitarbeiterinnen und Mitarbeiter.

„Wir holen nur ein Drittel des Möglichen heraus“

Doch trotz dieses großen und schnellen Wachstums („Früher ist so etwas über Generationen hinweg gewachsen, das war jetzt alles innerhalb weniger Jahrzehnte, das ist sehr schnell“) arbeitet Molitor immer noch genauso wie immer. Er lässt sich nicht dazu hinreißen, sich an die große Nachfrage anzupassen und mit effektiveren Arbeitsprozessen zu produzieren – obwohl es möglich wäre.

„Wir produzieren etwa 4.000 Liter Wein pro Hektar“, sagt Molitor. Das klinge zwar nach viel, sei aber deutlich weniger als das, was man aus so einer großen Fläche eigentlich herausholen könne. „Vom Staat erlaubt sind 12.000 Liter pro Hektar, wir holen also nur etwa ein Drittel von dem heraus, was wir offiziell eigentlich dürften.“ Das sei aber eine bewusste Entscheidung. „Natürlich könnten wir jeden nur möglichen Tropfen aus den Weinbergen herauspressen.“

Aber darunter würde die Qualität der einzelnen Trauben – und damit auch der entstehenden Weine – leiden. „Auch Rebstöcke können gestresst sein und bei zu viel Stress schlechtere Früchte tragen. Daher produzieren wir lieber weniger Wein, der dafür aber wirklich qualitativ hochwertig ist“, erklärt Molitor, „und gehen bei der Produktion so vor, wie wir das immer schon getan haben. Respektvoll, mit all unseren Traditionen und unserem Winzer-Handwerk.“

Große Lust am Wein

Und auch in Zukunft wird er genauso weiterarbeiten – ganz egal, wie viele Großbestellungen bei ihm noch eingehen oder welche Auszeichnungen er noch erhalten mag. Diese Einstellung gibt Molitor übrigens auch an die nächste Generation weiter: „Ich habe drei Söhne und mein ältester Sohn hat den Winzer-Beruf ebenfalls gelernt – er kann sich gut vorstellen, das Weingut später zu übernehmen. Er hat viel Lust dazu.“

Und er, Markus Molitor, würde sich darüber freuen. „Natürlich würde es mir gefallen, wenn mein Sohn das Gut irgendwann übernehmen würde.“ Auch deshalb, weil er sich dann sicher sein kann, dass das Weingut Molitor weitergeführt wird wie bisher. Mit Disziplin, Fachverstand und vor allem: mit einer großen Lust am Wein. ■

> „ES IST SCHÖN, WENN DIE EIGENE ARBEIT GEWÜRDIGT WIRD

Beim Wein kommt es auf die Anbauflächen an. Foto: © offenblende.de

Lesenswert

Empfehlungen zum Lesen, Hören und Streamen

Der Einsatz moderner Technologien bietet nicht nur Chancen, sondern beinhaltet auch viele Risiken für Unternehmen. Wir haben Medientipps für Sie zusammengestellt, die die Inhalte dieses Magazins vertiefen. Die empfohlenen Bücher, Podcasts und Serien zeigen unter anderem auf, welche Dimensionen Cyber-Angriffe einnehmen können, und enthalten viele weiterführende Informationen zum Thema Cyber-Security.

Gier, Macht, Scham? Motive krimineller Manager psychologisch erklärt

Buch von Benjamin Knull, geb. Schorn

Warum gibt es eigentlich Wirtschaftskriminalität? Was bringt Wirtschaftsbosse und Manager dazu, kriminell zu werden? Und gibt es typische Wirtschaftskriminelle? Mit diesen und weiteren spannenden Fragen beschäftigt sich Benjamin Knull. Er ist Forensic-Investigation-Spezialist und Gründer des Instituts für Governance & Psychologie – und er schreibt klug und dabei sehr interessant über sein Thema. Unbedingt lesenswert!

Upload

Serie von Amazon

Was passiert eigentlich nach dem Tod? Da lebt man weiter – als digitale Version des eigenen Selbst. Und in dieser neuen virtuellen Existenz kann man dann alles anders und besser machen, als man es auf Erden getan hat. Aber ist hier wirklich alles so schön und bunt und harmonisch, wie es den Anschein hat? Die Antwort gibt es in dieser Sci-Fi-Serie.

The Age of Data: Embracing Algorithms in Art & Design

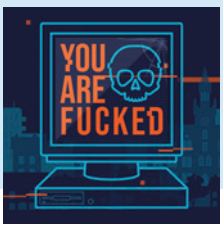
Buch von Christoph Grünberger

Künstliche Intelligenz ist heute überall – auch in der Kunst! Das Buch thematisiert eine neue Generation von Künstlerinnen und Künstlern, die Daten intensiv nutzen und sich mit algorithmusgestützter Gestaltung in der Vertikalen beschäftigen. Der Herausgeber konnte die relevantesten zeitgenössischen Protagonistinnen und Protagonisten gewinnen, die hier ihre wichtigsten Arbeiten vorstellen und Einblicke in ihre kreativen Prozesse geben.

You are fucked – Deutschlands erste Cyberkatastrophe

Podcast vom MDR

In der Landkreisverwaltung von Anhalt-Bitterfeld geht nichts mehr. Hacker haben Daten verschlüsselt und erpressen den Landkreis. „You are fucked" ist ihre erste Nachricht – und der Landkreis muss tatsächlich für 210 Tage den Katastrophenfall ausrufen. Dieser Podcast rekonstruiert die Geschehnisse von damals und fragt auch: Was haben Verwaltungen und Behörden aus Deutschlands erster Cyber-Katastrophe gelernt?



CYBERSNACS

Podcast der Allianz für Cyber-Sicherheit

Cyber-Sicherheit hat viele verschiedene Aspekte. Im Podcast der Allianz für Cyber-Sicherheit werden sie alle besprochen. Regelmäßig sind Expertinnen und Experten aus der Wirtschaft und dem IT-Bereich zu Gast und berichten von ihren ganz individuellen Erfahrungen und geben Tipps. Sie erklären dabei auch die technischen Grundlagen – für alle verständlich. Außerdem gibts im CYBERSNACS-Radar einen Ausblick auf aktuelle Entwicklungen bei der Cyber-Sicherheit. Unsere Empfehlung ist Folge 24, in der die Cyber-Sicherheitsaspekte von ChatGPT und Co. diskutiert werden.

Alles gesagt?

Podcast von der ZEIT

Christian Lindner, Joachim Gauck oder Alice Schwarzer – sie alle waren schon zu Gast im Interview-Podcast „Alles gesagt?" von der ZEIT. Kein Wunder, dass sie hier alle dabei sein wollten, denn das Konzept des Podcasts ist tatsächlich außergewöhnlich: Die beiden Interviewer Christoph Amend und Jochen Wegner – beide Journalisten bei der ZEIT – unterhalten sich so lange mit ihren Gästen, bis die selbst erklären, dass nun „alles gesagt" sei. Ein Gespräch kann also ein paar Minuten oder fünf Stunden dauern. Sehr spannend und wirklich unterhaltsam!

Cyberbunker: Darknet in Deutschland

Dokumentation von Netflix

Diese Doku enthüllt, wie eine Hacker-Gruppe von einem Bunker des Kalten Krieges aus in einem ruhigen deutschen Städtchen über das Internet die kriminelle Unterwelt eroberte. Sehr spannend und unterhaltsam!

Fotonachweise siehe S. 79

Agenda

Unsere Kalender füllen sich ständig, Termine müssen anderen weichen. Die Agenda wächst Stunde um Stunde. Mit unseren Vorschlägen wollen wir Sie auf Events aufmerksam machen, die rund um das Thema Sicherheit für Unternehmen relevant sein können. Diese thematisch vielfältigen Veranstaltungen helfen, sich zu Cyber-Security zu informieren und mit Expertinnen und Experten auszutauschen. Vielleicht findet das ein oder andere Event noch einen Platz in Ihren Planungen …

Foto: Adobe Stock

Barcelona Cybersecurity Congress

Das wichtigste Cybersecurity Treffen Europas

21.-23.05.2024

Der Barcelona Cybersecurity Congress ist ein wichtiger Treffpunkt für Interessenvertreterinnen und -vertreter, Branchenakteurinnen und -akteure sowie Dienstleisterinnen und Dienstleister, um Lösungen für aktuelle Herausforderungen zu finden. Technologieexpertinnen und -experten, Führungskräfte sowie Visionärinnen und Visionäre der Branche teilen ihre Erfahrungen und ihr Know-How zu neuen Technologien und Möglichkeiten der Cyber-Sicherheit.

Barcelona, Spanien
www.barcelonacybersecuritycongress.com

European Economic Conference

Kluge Köpfe bewegen Europa

04.-05.06.2024

Die dritte F.A.Z. European Economic Conference bietet eine Plattform für Vertreterinnen und Vertreter der europäischen Wirtschaft, Politik und Wissenschaft, für die Diskussion über die Rolle der EU bei der Förderung von Wirtschaftswachstum, sozialem Zusammenhalt und nachhaltiger Entwicklung. Die Konferenz fördert relevante Debatten und Lösungsansätze für ein starkes Europa.

Berlin, Deutschland
https://www.european-economic.eu/

Cybersecurity Summit

Die neue Cyber-Security-Messe

19.06.2024

Auf der neuen Messe und Konferenz für IT-Security im Unternehmen treffen sich die führenden Köpfe der Branche - vom Mittelstand bis zum Konzern. Gemeinsam tauschen sie ihre Erfahrungen aus, diskutieren Best Practices und Herausforderungen und lernen die neuesten Lösungen kennen.

Hamburg, Deutschland
www.cybersecuritysumm.it

Cloud & Cyber Security Expo

Tech Show Frankfurt

22.-23.05.2024

Die Veranstaltung ist Teil der Tech Show Frankfurt und begrüßt Führungskräfte, wichtige Entscheidungsträgerinnen und Entscheidungsträger sowie Sicherheitsstrateginnen und -strategen aus Unternehmen aller Größen und Branchen. Dort entdecken Sie neueste Trends, Cyber-Sicherheitslösungen und Best-Practice-Tipps und treffen einflussreiche Branchengrößen.

Frankfurt, Deutschland
www.cloudsecurityexpo.de

Handelsblatt Summit Zukunft IT 2024

Transforming IT in the Age of AI

10.-12.06.2024

Im Zeitalter von KI und digitaler Disruption müssen IT-Leaderrinnen und IT-Leader dafür sorgen, dass ihr Unternehmen an der Spitze des Wettbewerbs bleibt. Künstliche Intelligenz hat das Potenzial, das strategische IT-Management zu revolutionieren – mit dem Ziel, Innovationen voranzutreiben, Effektivität zu steigern und Kosten zu senken. Diskutieren Sie beim Handelsblatt Summit Zukunft IT, wie die Digitalisierung die Wirtschaft umkrempelt und welche zentrale Rolle IT-Leaderrinnen und IT-Leader dabei spielen.

München, Deutschland
live.handelsblatt.com/event/handelsblatt-summit-zukunft-it/

IFA

Consumer Electronics unlimited

06.-10.09.2024

2024 wird die weltgrößte Messe für Unterhaltungselektronik und Haushaltsgeräte 100 Jahre alt. Auch in diesem Jahr präsentiert die IFA eine Vielzahl aktueller Entwicklungen, Innovationen und Trends. Ein Besuch ermöglicht einen Einblick in wegweisende Technologien und Geräte sowie ihre fortschreitende Digitalisierung und Vernetzung.

Berlin, Deutschland
www.ifa-berlin.com

Wer es genauer wissen will

S. 6
Staat of the Art?

[1] dpa (2024): Kanzleramt verschickt geheime Dokumente weiter per Rohrpost. In: Süddeutsche Zei-tung. URL: https://www.sueddeutsche.de/politik/bundesregierung-kanzleramt-verschickt-geheime-dokumente-weiter-per-rohrpost-dpa.urn-newsml-dpa-com-20090101-240111-99-570182 [Stand 31.01.2024]

[2] Melanie Staudacher (2021): Reaktion auf Cyberangriffe dauert 21 Stunden. In: Security Insider. https://www.security-insider.de/reaktion-auf-cyberangriffe-a-1071216/ [Stand 31.01.2024]

[3] Tagessschau (2023): 136.865 Fälle von Cybercrime. URL: https://www.tagesschau.de/inland/cyberangriffe-deutschland-bka-100.html [Stand 31.01.2024]

[4] Tagessschau (2023): 136.865 Fälle von Cybercrime. URL: https://www.tagesschau.de/inland/cyberangriffe-deutschland-bka-100.html [Stand 31.01.2024]

[5] Tagesspiegel (2022): Immer mehr KMU betroffen. URL: https://background.tagesspiegel.de/cybersecurity/immer-mehr-kmu-betroffen [Stand 31.01.2024]

[6] bitkom (2023): Bitkom zum BSI-Jahresbericht. URL: https://www.bitkom.org/Presse/Presseinformation/Bitkom-BSI-Jahresbericht [Stand 31.01.2024]

[7] Security Insider (2023): Angriffe durch organisierte Kriminalität nehmen zu: 206 Milliarden Euro Schaden pro Jahr für die deutsche Wirtschaft. URL: https://www.security-insider.de/206-milliarden-euroschaden-pro-jahr-fuer-die-deutsche-wirtschaft-a-9cb41fbcc2273ca60de1ce13488ab757/?cflt=rel [Stand 31.01.2024]

[8] BMF (2024): Ausgaben und Einnahmen des Bundeshaushalts in Deutschland im Jahr 2023. In: Statis-ta. URL: https://de.statista.com/statistik/daten/studie/164669/umfrage/soll-und-ist-entwicklung-des-bundeshaushalts/ [Stand 31.01.2024]

[9] bitkom (2023): Bitkom zum BSI-Jahresbericht. URL: https://www.bitkom.org/Presse/Presseinformation/Bitkom-BSI-Jahresbericht [Stand 31.01.2024]

[10] Bundesamt für Sicherheit in der Informationstechnik (2021): IT-Sicherheit im HOME-OFFICE. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Umfrage-Home-Office/umfrage_home-office-2020.pdf?__blob=publicationFile&v=3 [Stand 31.01.2024]

[11] HDI (2022): Cyberangriffe und Schäden bei KMU - Ergebnisse der HDI Cyber-Studie. URL: https://www.hdi.de/konzern/presse/cyberangriffe-und-schaeden-bei-kmu/ [Stand 31.01.2024]

[12] Andreas Schulte (2023): Vorsicht vor der zweiten Welle. In: Tagesspiegel Background. URL: https://background.tagesspiegel.de/cybersecurity/vorsicht-vor-der-zweiten-welle [Stand 31.01.2024]

[13] bitkom (2023): Bitkom zum BSI-Jahresbericht. URL: https://www.bitkom.org/Presse/Presseinformation/Bitkom-BSI-Jahresbericht [Stand 31.01.2024]

[14] Statistisches Bundesamt (2023): Unternehmen in Deutschland: Anzahl der rechtlichen Einheiten in Deutschland nach Beschäftigtengrößenklassen im Jahr 2022. In: Statista. URL: https://de.statista.com/statistik/daten/studie/1929/umfrage/unternehmen-nach-beschaeftigtengroessenklassen/ [Stand 31.01.2024]

[15] Bastian Benrath (2022): Hacker erbeuten 211.529 Dollar Lösegeld – im Durchschnitt. In: FAZ. URL: https://www.faz.net/aktuell/wirtschaft/schneller-schlau/4000-hackerangriffe-am-tag-allein-in-deutschland-18126679.html [Stand 31.01.2024]

[16] Mittelstand Heute (2023): Cybersicherheit in Deutschland weiterhin kritisch (2023/24)! URL: https://www.mittelstand-heute.com/cybersicherheit-in-deutschland-weiterhin-kritisch-2023/24 [Stand 31.01.2024]

[17] Tagessschau (2023): 136.865 Fälle von Cybercrime. URL: https://www.tagesschau.de/inland/cyberangriffe-deutschland-bka-100.html [Stand 31.01.2024]

S. 38
Lücken im System

[1] BDO, DKI (2024): Personalnotstand im Krankenhaus – Quo vadis? URL: https://www.bdo.de/de-de/insights/weitere-veroffentlichungen/studien/fachkraftemangel-gekommen,-um-zu-bleiben-krankenhausstudie [Stand 15.01.2024]

S. 44
Cyber-Security aus Accounting-Sicht

[1] Europäische Kommission: Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheits-niveau in der gesamten Union (NIS2-Richtlinie). URL: https://digital-strategy.ec.europa.eu/de/policies/nis2-directive [Stand 15.01.2024]

[2] Federal Register (2023): Cybersecurity Risk Management, Strategy, Governance, and Incident Dis-closure. URL: https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure [Stand 15.01.2024]

S. 54
Metaversum: transformative Chance oder temporärer Hype?

[1] Nele Höfler, Hannah Krolle (2023): Was hinter dem Metaverse-Hype steckt. In: Handelsblatt. URL: https://www.handelsblatt.com/technik/metaverse-was-hinter-dem-metaverse-hype-steckt/28073180.html [Stand 15.01.2024]

S. 58
Auch Hacker nutzen ChatGPT

[1] bitkom (2023): Deutsche Wirtschaft drückt bei Künstlicher Intelligenz aufs Tempo. URL: https://www.bitkom.org/Presse/Presseinformation/Deutsche-Wirtschaft-drueckt-bei-Kuenstlicher-Intelligenz-aufs-Tempo#_ [Stand 31.01.2024]

[2] Cisco (2024): Cisco 2024 Data Privacy Benchmark Study. URL: https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html [Stand 31.01.2024]

[3] E.ON (2023): Helferin mit Energieexpertise: E.ON schaltet eigene Generative Künstliche Intelligenz live. URL: https://www.eon.com/de/ueber-uns/presse/pressemitteilungen/2023/eon-schaltet-eigene-generative-kuenstliche-intelligenz-live.html [Stand 31.01.2024]

S. 62
Anruf vom Fake President

[1] Herbert Fromme (2019): Betrüger erbeutet 220 000 Euro mit gefälschter Stimme. In: Süddeutsche Zeitung. URL: www.sueddeutsche.de/digital/ki-deepfake-versicherung-betrug-1.4493902 [Stand 31.01.2024]

[2] Fraunhofer-Institut für Intelligente Analyse und Informationssysteme IAIS (2021): Effiziente Be-trugserkennung durch Maschinelles Lernen. URL: www.iais.fraunhofer.de/content/dam/iais/gf/bda/Downloads/Fraunhofer_IAIS_Whitepaper_Fraud.pdf [Stand 31.01.2024]

[3] Bundeskriminalamt (2023): Wirtschaftskriminalität. Bundeslagebild 2022. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Wirtschaftskriminalitaet/wirtschaftskriminalitaetBundeslagebild2022.html [Stand 31.01.2024]

[4] Allianz Trade (2023): Allianz Trade Statistik: Fake-President-Betrug kommt wieder in Mode, Zah-lungsbetrug steigt um fast ein Drittel. URL: www.allianz-trade.de/presse/pressemitteilungen/allianz-trade-statistik-fake-president-betrug-kommt-wieder-in-mode.html [Stand 31.01.2024]

[5] manager magazin (2016): 40 Millionen Euro weg - dieser MDax-Konzern fällt auf Betrüger rein. URL: www.manager-magazin.de/unternehmen/autoindustrie/autozulieferer-leoni-um-40-millionen-betrogen-a-1107998.html [Stand 31.01.2024]

IMPRESSUM

Herausgeber
BDO AG Wirtschaftsprüfungsgesellschaft
Fuhlentwiete 12
20355 Hamburg
Tel.: +49 40 30293-0
hamburg@bdo.de
Internet: www.bdo.de
vertreten durch Parwäz Rafiqpoor

Chefredaktion
Parwäz Rafiqpoor (V. i. S. d. P.)
BDO AG Wirtschaftsprüfungsgesellschaft
Fuhlentwiete 12, 20355 Hamburg

Konzeption: BDO AG Wirtschaftsprüfungsgesellschaft, Hamburg
Art-Direktion: BDO AG Wirtschaftsprüfungsgesellschaft, Hamburg
Lektorat: Text first GbR, Hamburg

Autorinnen und Autoren dieser Ausgabe
Mitarbeiterinnen und Mitarbeiter der BDO AG Wirtschaftsprüfungsgesellschaft, Hamburg, BDO Cyber Security GmbH, Hamburg und BDO Legal Rechtsanwaltsgesellschaft mbH, Hamburg, sowie Malte Brenneisen (MB), Hamburg, und Laslo Seyda (LS), Hamburg

Bildquellen
Fotos: Adobe Stock, Fraunhofer AISEC, HRS, Körber, offenblende.de

Titelfoto: Adobe Stock
Lesenswert S. 74-75: Blanvalet, Frankfurter Allgemeine Buch, niggli, Amazon Studios, MDR, Lea Dohle für ZEIT ONLINE, Bundesamt für Sicherheit in der Informationstechnik, btf.

Redaktionsschluss: 31.01.2024
Druck: BDO AG Wirtschaftsprüfungsgesellschaft Print Center
Neumann-Reichardt-Straße 27-33, Haus 8, 1. OG, 22041 Hamburg

Ein Magazin der BDO AG Wirtschaftsprüfungsgesellschaft | Fuhlentwiete 12 | 20355 Hamburg
BDO foresight | www.bdo.de/foresight