IT-SICHERHEIT 2021
Resilienz ist der Schlüsselfaktor

CYBER-ANGRIFFE
Wie können Unternehmen sich schützen?

DATENSCHUTZ
Vertrauensanker für die Digitalisierung

Handelsblatt Journal

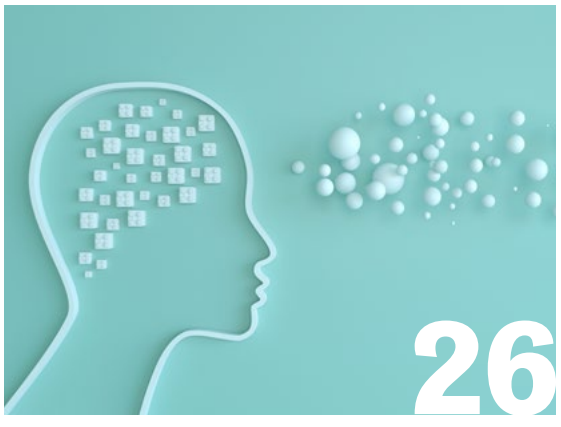
Eine Sonderveröffentlichung von Euroforum Deutschland

NOVEMBER 2021 | WWW.HANDELSBLATT-JOURNAL.DE

euroforum

Medienpartner
Handelsblatt
Substanz entscheidet.

DIE THEMEN DIESER AUSGABE



IMPRESSUM

Herausgeber
Euroforum Deutschland GmbH
Toulouser Allee 27
40211 Düsseldorf
Tel.: +49(0)211.88743-3829
handelsblatt-journal.de

Projektleitung (V.i.S.d.P.)
Christiane Daners,
Handelsblatt GmbH
c.daners@handelsblattgroup.com

Redaktionsleitung
Nicola Csepella,
Handelsblatt GmbH
n.csepella@handelsblattgroup.com

Art Direction & Layout
Solutions by Handelsblatt
Media Group GmbH
Toulouser Allee 27 | 40211 Düsseldorf
solutions-hmg.com

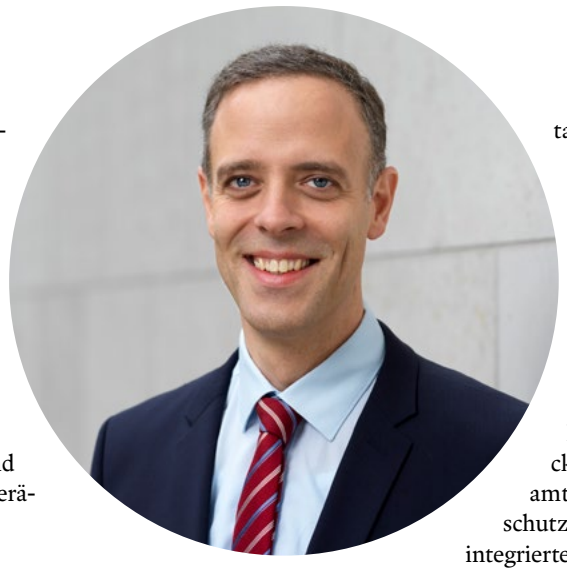
Titelbild
Getty

Medienpartner
Handelsblatt
Substanz entscheidet.

Fotos: Getty (2), Adobe Stock

EINE VERNETZTE CYBERSICHERHEITS-ARCHITEKTUR FÜR EINE VERNETZTE WELT

von Dr. Markus Richter



Dr. Markus Richter,
Staatssekretär und Beauftragter der Bundesregierung für Informationstechnik, Bundesministerium des Innern

Der digitale Raum kennt keine Grenzen. Egal ob wir in Berlin, Brüssel oder Washington sitzen – mit unserem Smartphone können wir auf eine unüberschaubare Menge von Informationen zugreifen und diese nahezu in Echtzeit an fast jeden Ort der Welt versenden. Dieser technologische Quantensprung hat unsere Welt grundlegend verändert. Neue Wirtschaftsmodelle sind entstanden, der Zugriff auf Wissen ist so einfach wie nie und aus unserem Privatleben sind vernetzte Geräte nicht mehr wegzudenken.

Neue Herausforderungen

Eine Welt, die sich immer mehr vernetzt, bringt aber auch neue Herausforderungen mit sich. Angriffe, die Sicherheitslücken in global verbreiteten Produkten ausnutzen, können weltweit Systemausfälle auslösen – mit zum Teil gravierenden Auswirkungen auf die Wirtschaft und die Versorgungssicherheit der Bevölkerung. Durch Cybercrime-as-a-Service (Cyberstraftat als Dienstleistung), das auf einer globalen und arbeitsteilig agierenden kriminellen Gemeinschaft der sog. Underground Economy basiert, können auch weniger cyberaffine Straftäter technisch komplexe Straftaten begehen. Und mit länderübergreifend verteilten Botnetzen ist es möglich, erhebliche Überlastungsangriffe auf Internetdienste durchzuführen – der Ausfall einer gesamten Plattform kann die Folge sein.

Gemeinsame Antworten

Auf diese Herausforderungen müssen wir Antworten finden. Der Staat steht dabei in besonderer Verantwortung, denn bei ihm liegt das Gewaltmonopol. Er ist daher gefordert, seine Behörden so aufzustellen, dass sie den Bedrohungen effektiv entgegentreten können. Dabei ist entscheidend: Bei solchen Bedrohungen darf es kein behördliches Silodenken geben. Dies gilt für die Behörden des Bundes genauso wie für die Zusammenarbeit zwischen Bund und Ländern. Darüber hinaus ist die internationale Dimension in den Blick zu nehmen. Ohne eine intensive europäische sowie bi- und multilaterale Zusammenarbeit können wir beim Thema Cybersicherheit nicht nachhaltig erfolgreich sein.

Daraus folgt, dass wir eine vernetzte Cybersicherheitsarchitektur benötigen. In Deutschland sind wir dabei auf einem guten Weg. Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) sorgt dafür, dass sich alle zuständigen Bundesbehörden im Cyberraum eng miteinander austauschen. Auch in den Ländern entstehen immer mehr Plattformen zur Abstimmung bei Cybervorfällen. Mit der Aufnahme von Ländervertretern in das Cyber-AZ haben wir in diesem Jahr beide Ebenen miteinander verzahnt. Um künftig noch enger mit den Ländern kooperieren zu können, soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu einer Zentralstelle im Bund-Länder-Verhältnis ausgebaut werden. Damit entwickeln wir es – neben dem Bundeskriminalamt und dem Bundesamt für Verfassungsschutz – zur dritten tragenden Säule einer föderal integrierten Cybersicherheitsarchitektur fort.

Wie wichtig die enge Zusammenarbeit mit unseren europäischen und internationalen Partnern ist und wie erfolgreich wir gemeinsam sein können, zeigt der Fall Emotet eindrücklich. Emotet galt weltweit als eine der schädlichsten Malware-Varianten, die alleine in Deutschland einen Schaden in Höhe von mindestens 14,5 Millionen Euro verursacht hat. In enger Abstimmung mit unseren Partnerbehörden wurde die Emotet-Infrastruktur Anfang des Jahres zerschlagen, ein Beschuldigter in der Ukraine vorläufig festgenommen und den Tätern gleichzeitig jede Möglichkeit genommen, die Kontrolle über ihre Infrastruktur zurückzuerlangen. An solche Erfolge wollen wir anknüpfen und die Kooperation mit unseren Partnern noch weiter vertiefen.

Auf Augenhöhe mit Wirtschaft, Wissenschaft und Gesellschaft

Die Herausforderung, Cybersicherheit zu gewährleisten, kann der Staat nicht alleine bewältigen. Er ist vielmehr auf eine Zusammenarbeit mit Akteuren aus der Wirtschaft, der Wissenschaft und der Gesellschaft angewiesen. Diese Zusammenarbeit muss auf Augenhöhe stattfinden. Hierfür bestehen bereits erfolgreiche Formate. Allein im Rahmen der Allianz für Cybersicherheit tauschen sich rund 5.400 Unternehmen und Institutionen mit dem Staat zu Sicherheitsfragen im digitalen Raum aus. Aber ich bin davon überzeugt, dass wir noch besser werden können. Wir müssen das vielfältige Wissen, das in unserer Gesellschaft vorhanden ist, bei zentralen Vorhaben umfassend einbinden. Dabei dürfen wir auch kritische Auseinandersetzungen in der Sache nicht scheuen. Wenn alle Seiten gemeinsam an konstruktiven Lösungen arbeiten, ist dies ein großer Gewinn für die Cybersicherheit. ■

Foto: Henning Schacht

OHNE CYBERSICHERHEIT KEIN DATENSCHUTZ

Cybersicherheit und Datenschutz endlich als Erfolgsfaktor verstehen

von Prof. Ulrich Kelber

Cybersicherheit und Datenschutz sind wie Geschwister: Oft ziehen sie an einem Strang, manchmal sind ihre Interessen unterschiedlich, aber am Ende sind sie doch aus einem Holz geschnitzt. Selbst ihr Image ist ähnlich und oft zu Unrecht negativ besetzt. Es wird in Kategorien wie Aufwand, Kosten und Risiken gedacht – und dabei völlig vergessen, dass Cybersicherheit wie Datenschutz darüber hinaus essenzielle Vertrauensanker für die Digitalisierung sind. Höchste Zeit für einen Perspektivwechsel.

Cybersicherheit und Datenschutz – wir streiten fast nie

Die Schutzziele von Cybersicherheit und Datenschutz zahlen aufeinander ein und sind oftmals sogar gleich. Denn der Schutz personenbezogener Daten setzt auch die Sicherheit der Datenverarbeitung voraus. Datensicherheit ist damit integraler Bestandteil des Datenschutzes. Sie schützt zum Beispiel IT-Systeme, insbesondere Hardware, Software und – auch sonstige nicht-personenbezogene Daten vor der Gefahr des Verlustes, der Zerstörung oder des Missbrauchs durch Unbefugte. Mit dieser Zielrichtung erfasst die Datensicherheit auch ganz analoge Aspekte, etwa den Zutrittsschutz von Server-Räumen oder papierbasierter Aktenräumen. Verantwortliche und Auftragsverarbeiter müssen geeignete technische und organisatorische Maßnahmen treffen, um diese Ziele zu erreichen. Geeignetheit bedeutet, dass der Schutzaufwand und das Risiko bei der Auswahl der technischen und organisatorischen Maßnahmen in einem angemessenen Verhältnis stehen müssen. So sieht es die Datenschutzgrundverordnung explizit vor. Bestimmte Maßnahmen wie die Pseudonymisierung oder Verschlüsselung werden sogar namentlich im Gesetz als Schutzmechanismen genannt. Insgesamt geht es also darum, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherzustellen beziehungsweise nach einem Zwischenfall wieder herzustellen.

In seltenen Fällen können die Interessen von Datensicherheit und Datenschutz auch gegeneinander stehen. Etwa, wenn personenbezogene Daten für eine Analyse von Cyberangriffen länger aufbewahrt werden sollen, als es aus Sicht des Datenschutzes angebracht wäre. Hier kann es – wie in jeder Familie – schon einmal zu Spannungsverhältnissen kommen, die einen sachgerechten Ausgleich erfordern.

Cybersicherheit – von Anfang an und immer wieder

Wie gesagt: Datensicherheit ist eine Voraussetzung für effektiven Datenschutz. Es gilt eine einfache Gleichung: Ohne IT-Sicherheit (und übrigens auch ohne Datenschutz) kein Vertrauen. Und ohne Vertrauen keine Nutzung von digitalen Diensten. IT-Sicherheit ist damit, wie der Datenschutz auch, ein wichtiger Erfolgsfaktor für die Digitalisierung. Wer „Security-by-design“ von Anfang an bei der Entwicklung von Produkten und Services mitberücksichtigt, ist gut beraten. Denn nachträglich wird es oftmals schwierig und (dann tatsächlich) aufwändig, grobe Defizite oder Fehler in der IT-Sicherheitsarchitektur wieder zu korrigieren. Dies ist vor allem der Fall, wenn hierdurch grundlegende Anpassungen am Systemdesign erforderlich würden.

Im Datenschutz ist diese proaktive, aus meiner Sicht sehr kluge Technikgestaltung konzeptionell bereits lange etabliert. Daher ist es kein Wunder, dass die DSGVO auch hierzu Aussagen trifft: Es geht darum, bereits in der Entwicklungsphase die datenschutzrechtlichen Implikationen mitzudenken und zu überlegen, wie datenschutzrechtliche Risiken bereits in diesem frühen Entwicklungsstadium bestmöglich reduziert werden können. Cybersicherheit ist aber wie der Datenschutz sicher keine einmalige Angelegenheit, die man zu Beginn abschließend klärt und dann zu den Akten legen kann. Es ist vielmehr eine fortwährende Aufgabe für den gesamten Lebenszyklus von Produkten und Dienstleistungen in der digitalen Welt.

Cybersicherheit und Datenschutz müssen Chefsache und Erfolgsfaktor werden

Ohne starken Datenschutz und ein hohes Maß an Cybersicherheit steigen die Risiken massiv an. Denn nicht ausreichend geschützte IT-Systeme sind lohnende Ziele für Missbrauch und Kriminalität. Es ist deshalb kurzsichtig und brandgefährlich, Cybersicherheit allein als lästigen Kostenfaktor zu betrachten. Um es anschaulich zu machen: Wenn Produktionsabläufe digitalisiert werden, ist man gut beraten, die genutzten IT-Systeme vorbildlich zu schützen. Sonst stehen die Fabrikbänder im Falle von digitaler Sabotage schlicht still. Für Unternehmungen ist das – neben den finanziellen Folgen – meistens auch mit erheblichen Reputationsschäden verbunden. Gleiches gilt für Datenpannen, die außerdem eine Reihe rechtlicher Sanktionsmöglichkeiten nach sich ziehen können. Cybersicherheit und Datenschutz sind deshalb auch aus dieser Perspektive wichtige Erfolgsfaktoren für die Digitalisierung. Denn erleidet ein Produkt oder eine Dienstleistung erst einmal einen solchen Imageschaden, dann wird es schwierig, hier wieder Boden gut zu machen.

IT-Sicherheit und Datenschutz müssen auch wegen dieser substanziellen Bedeutung Chefsache werden. Wir sollten die Chancen einer sicheren, datenschutzkonformen Digitalisierung für die deutsche und europäische Digitalwirtschaft nutzen. Hiervon sind wir leider noch zu weit entfernt. Cybersicherheit und Datenschutz werden leider oft negativ kommentiert. Die offenkundigen Vorteile werden nur selten in den Blick genommen.

Gerade der Datenschutz wird in steter Regelmäßigkeit als angebliche „Bremse“ für Innovationen gebrandmarkt. Es hält sich hartnäckig das Märchen, der er sei maßgeblich schuld daran, dass Deutschland keine funktionierenden digitalen Antworten auf die Pandemie gefunden habe. Das ist schlicht Unsinn und zeugt wahlweise von völliger Unkenntnis oder gefährlichen Hintergedanken. Mir ist kein Fall, keine seitens Gesundheitsministerium oder Robert Koch Institut geplante Funktionalität bekannt, bei der der Datenschutz dazu geführt hat, dass eine sinnvolle Technologie nicht realisiert werden konnte oder nur zeitlich verzögert wurde.

Vor allem mit Blick auf den gewaltigen Digitalisierungsschub, der sich vor unseren Augen abspielt, ergeben sich vielmehr enorme Wachstumspotenziale für unsere Digitalwirtschaft: Lassen Sie uns ein Höchstmaß an Cybersicherheit und Datenschutz zu unserem globalen Wettbewerbsvorteil ausbauen. Die Welt wartet auf solche Alternativen aus Europa. Wie sollte eine verantwortungsbewusste und sinnvolle technologische Weiterentwicklung denn auch sonst aussehen? Als Europäerinnen und Europäer muss es unser Anspruch sein, nicht nur die Geschwister Datenschutz und Cybersicherheit zusammen zu bringen, sondern die gesamte Familie, zu der auch die Aspekte Innovation und Wettbewerbsfähigkeit gehören.

Für diese gemeinsame Aufgabe wünsche ich uns allen – sei es in der Cybersicherheit, sei es im Datenschutz – bestmöglichen Erfolg. ■

Prof. Ulrich Kelber,
Bundesbeauftragter für den Datenschutz und die Informationssicherheit

> Die Welt wartet auf europäische Alternativen mit einem Höchstmaß an Cybersicherheit und Datenschutz. ”

Fotos: Getty, Bundesregierung/Kugler

Aufklärung, Auswertung, Prävention –

NACHRICHTENDIENSTE ALS INSTRUMENT DER RESILIENTEN DEMOKRATIE

von Thomas Haldenwang

Resilienz ist das Modewort der Stunde – und als neues Kriterium für die Widerstandsfähigkeit von Gesellschaften in aller Munde. Die steile Karriere des Begriffes ist plausibel, denn in den vergangenen 20 Jahren mussten Politik und Gesellschaft reaktiv mehreren großen Krisen trotzen. Internationaler Terrorismus, eine Finanzkrise, der Klimawandel und die aktuelle Pandemie haben die Verwundbarkeit interdependenter Gesellschaften schmerzhaft offengelegt. Es verbreitet sich ein Bedürfnis nach vorausschauenden Strategien zur Krisenbewältigung – und ein neues Bewusstsein für die Notwendigkeit robuster Sicherheitsarchitekturen.

Aus dem Blickwinkel der Resilienz wird „robust" dabei zunehmend als Fähigkeit verstanden, Risiken zu antizipieren und die eigenen Ressourcen flexibel auf erkannte Bedrohungen auszurichten. Es gilt, Schäden frühzeitig zu verhindern oder auf ein kontrollierbares Maß einzugrenzen.

In diesem Sinne ist das Bundesamt für Verfassungsschutz bereits durch seinen gesetzlichen Auftrag ein effizienter Dienstleister für die Widerstandskraft einer offenen, aber wehrhaften Demokratie. Für den Schutz aller in Deutschland lebenden Menschen und die Verteidigung der freiheitlichen demokratischen Grundordnung ist es unabdingbar, dass Extremismus und Terrorismus sowie Spionage, Sabotage und illegitime Einflussnahme fremder Mächte frühzeitig aufgeklärt werden. Dafür arbeiten wir als Inlandsnachrichtendienst im Bedarfsfall auch mit verdeckten Mitteln – sei es in der sogenannten Realwelt oder im Cyberraum.

Unsere Auswertungserkenntnisse bleiben jedoch nicht im Verborgenen, sondern informieren und sensibilisieren in vielfältigen Produkten politische Entscheidungsträger, zuständige staatliche Stellen und die Öffentlichkeit. Denn wir verstehen uns als dienender Akteur der wehrhaften Demokratie – und den informierten Bürger als Grundbaustein einer resilienten, demokratischen Sicherheitsarchitektur. Nur wenn ein ausreichend valides Bild der Sicherheitslage zur Verfügung steht, können entsprechende Entscheidungen getroffen, Maßnahmen verabschiedet und Ressourcen mobilisiert werden.

Thomas Haldenwang,
Präsident, Bundesamt für Verfassungsschutz

> Wir verstehen uns als dienender Akteur der wehrhaften Demokratie – und den informierten Bürger als Grundbaustein einer resilienten, demokratischen Sicherheitsarchitektur.

Bekanntlich mobilisiert das Bundesamt für Verfassungsschutz seit vielen Jahren enorme Ressourcen im Bereich der Cyberabwehr. Die hohe Attraktion potenzieller Spionageziele im Vorfeld der Bundestagswahl oder im Bereich der Impfstoffentwicklung rechtfertigten an dieser Stelle jede weitere Anstrengung. Infolge der Pandemie hat sich durch die intensivierte Nutzung von Fernzugriffstools im Homeoffice eine ohnehin uferlose Angriffsfläche nochmals sprunghaft ausgedehnt. Und so bleibt das Niveau der Bedrohung hoch. Ungebrochen sind Politik und Verwaltung, Wirtschaft und Wissenschaft, Forschung und Kritische Infrastrukturen begehrte Hochwertziele von Cyberangriffen.

Eine Trendumkehr ist nicht in Sicht. Vielmehr beunruhigt die hohe Komplexität und Raffinesse zahlreicher Kampagnen. Beispielhaft dafür ist der im Dezember 2020 medienwirksam gewordene, großangelegte Supply-Chain-Angriff auf einen US-amerikanischen IT-Dienstleister. Nachdem der Schadcode in eine Netzwerk-Monitoring-Software eingeschleust worden war, erfolgte über legitime Updates die Auslieferung manipulierter Software an Firmenkunden. Betroffen war auch deutsche Kundschaft aus der Wirtschaft, Verwaltung sowie Bundesbehörden. Während hinter diesem Vorfall ein staatlicher Akteur vermutet wird, beobachten wir grundsätzlich mit Sorge, dass sowohl in der analogen als auch in der digitalen Sphäre Grenzen zwischen staatlichen und privaten Protagonisten verschwimmen – und damit eine quantitative wie qualitative Entgrenzung einhergeht.

Um in einer solchen Lage Spionage-, Sabotage- oder auch illegitime Einflussnahmeaktivitäten wirksam abwehren zu können, ist sowohl die internationale Kooperation mit anderen Diensten als auch der intensive Informationsaustausch im Nationalen Cyberabwehrzentrum unverzichtbar. Darüber hinaus umfasst die ganzheitliche Agenda des Bundesamtes für Verfassungsschutz neben der nachrichtendienstlichen Fallbearbeitung auch eine

Vielzahl von Sensibilisierungsmaßnahmen. Denn um die Resilienz aller gefährdeten Stellen zu stärken, detektieren wir nicht nur staatliche Cyberangriffe und bemühen uns um eine Zuordnung, sondern ermöglichen durch gezielte Präventionsarbeit auch die Teilhabe an unseren Erkenntnissen zu den Modi Operandi der Angriffskampagnen.

So brachten wir etwa in die Erstellung eines bundesweiten Lagebildes zur möglichen Gefährdung der Bundestagswahl unsere langjährige Expertise ein. Zahlreich erkannte Phishing-Angriffe der Cybergruppierung GHOSTWRITER mit Fokus auf private E-Mail-Adressen von Abgeordneten des Deutschen Bundestages und der Landesparlamente veranlassten uns, gemeinsam mit anderen Behörden auch kurzfristig intensive Sensibilisierungen im politischen Raum durchzuführen. Obwohl die Gefahr einer Desinformations- oder Einflussnahmekampagne abstrakt blieb, gaben wir unsere Erkenntnisse an die relevanten Zielgruppen weiter. Denn im Hinblick auf eine erfolgreiche Prävention gilt für Nachrichtendienste die Ausnahme: Schweigen ist Silber, Reden ist Gold.

> Als Inlandsnachrichtendienst arbeiten wir im Bedarfsfall auch mit verdeckten Mitteln – sei es in der sogenannten Realwelt oder im Cyberraum.

Damit alle Potenziale zugunsten einer Demokratie mit hoher Resilienz abgerufen werden, bedarf es jedoch auch der strengen Selbstprüfung aller beteiligten Kräfte. Auf die anhaltend dynamische Sicherheitslage reagiert das Bundesamt für Verfassungsschutz ebenfalls mit anhaltender, innerer Dynamik. Nur in Bewegung und in konsequenter Fortentwicklung können die mannigfaltigen Herausforderungen gemeistert werden. Angesichts stetig steigender Datenmengen investieren wir in zukunftsfähige Technologie – etwa in Big Data-Infrastrukturen und den Einsatz Künstlicher Intelligenz. Um technisch hoch versierten Angreifergruppierungen auf Augenhöhe begegnen und Forensik- oder Malwareanalysen durchführen zu können, ist für unsere Cyberabwehr eine adäquate technische Ausstattung essenziell.

Diese Schritte sind notwendig und rentabel, denn es gilt der Grundsatz, dass nur durch Technik und harte Arbeit aus Daten valide Erkenntnisse werden – und aus Erkenntnissen eine gewinnbringende Information für Entscheidungsträger. Deshalb ist unser Anspruch ein reaktionsschneller Nachrichtendienst, der volatilen Lageentwicklungen agil entgegentritt – und die Resilienz unserer Demokratie stärkt. ■

Advertorial

Cybersicherheit entlang der gesamten Lieferketten

Angriffe gegen Unternehmen und ihre Zulieferer häufen sich – 2021 legten Cyberkriminelle allein mit dem Sunburst- und dem Kaseya-Hack über 1.000 Unternehmen lahm und brachten in den USA eine Gas-Pipeline zum Erliegen. Unternehmen und Betreiber von kritischen Infrastrukturen müssen sich künftig besser auf derartige Bedrohungen vorbereiten – und dies auch von ihrer Lieferkette fordern.

von Sudhir Ethiraj

Der wichtigste Schritt, um besser gewappnet zu sein, ist das Einflechten des Sicherheitsgedanken in die Unternehmenskultur. Auch der Nachweis von Cybersicherheit durch Zertifizierungen wird immer wichtiger. „Security by Default" ist dabei für die gesamte Lieferkette relevant. Dazu ist es notwendig, über Branchen hinweg einheitliche Richtlinien und Standards zu etablieren, um die Sicherheit von Produkten oder Infrastruktur bereits in der Konzeptionsphase zu berücksichtigen. Außerdem muss die Lieferkette vollständig erfasst werden, um auch schwächere Glieder zu stärken.

Vorreiter Automobilbranche

Ein aktuelles Beispiel ist die neue UNECE-Regularie R155 sowie die ISO/SAE 21434 für Automotive Cybersecurity. Die UNECE-Cybersicherheitsregularie verpflichtet Automobilhersteller, ein zertifiziertes Cybersicherheitsmanagementsystem (CSMS) zu unterhalten, welches mindestens alle drei Jahre bewertet und erneuert werden muss. Ab Mitte 2022 dürfen keine neuen Fahrzeugtypen in Europa mehr zugelassen werden, wenn Hersteller diese Standards nicht erfüllen und nachweisen können. Das hat Auswirkungen auf die gesamte Lieferkette in der Automobilindustrie.

Standards stärken das Vertrauen

Die beschriebenen Entwicklungen bei der Standardisierung von Cybersicherheit in der Automobilindustrie zeigen, dass sich die Standardisierung sowohl auf die Hersteller als auch auf deren globale Wertschöpfungsketten auswirken kann. Die Zertifizierung dazu ist der formale Nachweis, dass Anforderungen erfüllt sind. Ein strukturiertes Risikomanagement und Zertifizierung basierend auf Standards sind Grundvoraussetzungen, um die Absicherung gegen Cyberangriffe und das Vertrauen von Kunden in das jeweilige Unternehmen und seine Produkte zu stärken. Cybersicherheit wird damit auch zum Wettbewerbsvorteil. ■

www.tuvsud.com/cybersecurity

Sudhir Ethiraj,
Global Head of Cybersecurity Office (CSO),
TÜV SÜD AG

> Es ist notwendig, einheitliche Richtlinien und Standards über Branchen hinweg zu etablieren.

Foto: TÜV SÜD

CYBERSICHERHEIT BRAUCHT FORSCHUNG

von Dr. Haya Shulman

Unternehmen, Behörden, Vereine, Parteien, Forschungseinrichtungen, selbst Privatpersonen – sie alle stehen im Fokus von Cyberangreifern. Nahezu wöchentlich gibt es Berichte zu neuen Angriffsmethoden und zu erfolgreichen Cyberangriffen auf wichtige Einrichtungen. Die Angriffe nehmen zu, die Angriffstaktiken werden immer ausgefeilter, und die Cyberkriminellen organisieren sich immer besser. Ihre Ziele sind vielfältig: meist finanzieller Gewinn mit Ransomware und Erpressung, aber auch Spionage, Identitätsdiebstahl, Desinformation und Sabotage.

> Die weitaus größte Zahl der Verwundbarkeiten und Angriffe kann man beheben und abwehren. Man muss dazu Cybersicherheit zur Chefsache machen.

Cyberangriffe gefährden die digitale Gesellschaft und Demokratie, sie legen kritische Infrastrukturen lahm, sind verheerend für die Wirtschaft und können sogar Menschenleben kosten.

Wie funktioniert die Attribution von Cyberangriffen?

Die Cyberangriffe kommen dabei aus vielen Ländern, die meisten gehen aber zurück auf Angreifer-Gruppen aus Russland, China und Iran. Für die Zuordnung eines Angriffs zu einem Land oder einer Gruppe – also zur Attribution – werden eine Vielzahl von Faktoren ausgewertet, z.B. ob ein ähnliches Vorgehen oder ähnliche Schadsoftware schon einmal beobachtet wurde, welche Spracheinstellungen der Compiler hatte, welche Server der Angreifer verwendet. Die Uhrzeiten, zu denen Schadsoftware mit einem Server des Angreifers kommuniziert, können zudem Hinweise auf die Zeitzone der Angreifer geben.

Allerdings sind all dies nur Indizien, und wenn es ein Angreifer darauf anlegt, kann er diese Indizien vortäuschen und „unter falscher Flagge" handeln. Beispielsweise übernahm 2019 die Gruppe „Turla", die im Auftrag des russischen Auslandsgeheimdienstes FSB operiert, die Infrastruktur einer vom Iran unterstützten Gruppe und nutzte sie für Angriffe auf Ziele in mehr als 35 Ländern. Für all diese Angriffe wurde zunächst aber nicht Russland, sondern der Iran verantwortlich gemacht. Solche Operationen unter falscher Flagge sind häufig und werden von verschiedenen Angreifer-Gruppen und Ländern durchgeführt.

Hackbacks im Sinne eines Gegenangriffs auf den vermeintlichen Täter sind daher hoch riskant. Attribution ist schwierig und fehlerbehaftet und man kann nie sicher sein, wer wirklich der Täter war. Abgesehen von völkerrechtlichen Aspekten wäre deshalb das Risiko, den Falschen anzugreifen oder unkalkulierbar hohe Schäden anzurichten, viel zu groß. Die Attribution zu Staaten ist dennoch wichtig, aber nicht für die tägliche Cybersicherheit, sondern z.B. für politische Diskussionen und das Aushandeln internationaler Abkommen.

Man muss schneller sein als die Cyberangreifer

Aus der Attribution kann man aber Erkenntnisse ableiten, wie Angreifer typischerweise vorgehen, wenn sie bestimmte Sektoren angreifen, welche Art von Schwachstellen sie ausnutzen, welche Werkzeuge sie verwenden, welche Ziele sie verfolgen.

Das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE hat aus diesen Erkenntnissen einen Werkzeugkasten zur Analyse der Verwundbarkeit von Organisationen entwickelt. Unsere Analysen sind sehr effizient und leichtgewichtig, d. h., wir dringen nicht in IT-Systeme ein, sondern wir beobachten beispielsweise, welche Schwachstellen es in den Infrastrukturen gibt und welche Benutzerpasswörter im Darknet gehandelt werden, wie Sicherheitsmechanismen von einer Organisation eingesetzt werden und gegen welche Angriffe die IT-Systeme empfänglich wären.

Diese Analysen haben wir in den vergangenen 12 Monaten für eine Vielzahl von IT-Infrastrukturen durchgeführt, z.B. für Unternehmen, Universitäten, Behörden und Parteien. Die Ergebnisse waren über alle Sektoren hinweg sehr ähnlich: So gut wie jede IT-Infrastruktur ist verwundbar.

Schutz vor Cyberangriffen

Die Lage ist also dramatisch. Schaut man sich unsere Analysen und die Erfahrungen aus den Cyberangriffen der letzten Monate an, sieht man aber auch, dass sie keinesfalls hoffnungslos ist. Die weitaus größte Zahl der Verwundbarkeiten und Angriffe, die wir beobachten, kann man mit bekannten Vorgehensweisen beheben und abwehren. Man muss dazu aber Cybersicherheit zur Chefsache machen: Verantwortliche benennen und Standards und Regeln einführen; die eigene IT so strukturieren, dass Angriffe sich nicht so einfach ausbreiten können; Daten sichern.

Und vor allem müssen Organisationen „Cyber-Brandschutzübungen" durchführen und den Ernstfall üben. Also lernen, sich auf Angriffe vorzubereiten und den Schutz aktuell zu halten, Angriffe zu erkennen, sie abzuwehren und nach einem Angriff die IT wieder hochzufahren. In diesen Punkten gibt es oft massive Defizite, weshalb wir in ATHENE eine „Cyberrange" aufgebaut haben: Eine Lernumgebung, in der Organisation genau solche Übungen unter sehr realitätsnahen Bedingungen durchführen können: https://cyberrange.sit.fraunhofer.de/

Zur Cyberabwehr gehört auch die technische Attribution

Hier geht es aber nicht nur darum, welcher Staat oder welche Gruppe für einen Angriff verantwortlich ist, sondern z.B. von welchem Server und über welchen Kanal der Angriff durchgeführt wurde. Diese Fragen kann man oft präzise beantworten und zur Grundlage für eine aktive Cyberabwehr machen – also z.B. die Quelle eines Angriffs aktiv blockieren oder gezielt abschalten. Hier sind allerdings noch viele rechtliche Fragen zu klären.

Offensive Forschung ist wichtig

Grundlage unserer Analysen in ATHENE ist die offensive Cybersicherheitsforschung. Das bedeutet nicht, dass wir für unsere Forschung selbst angreifen, sondern dass wir analysieren, wie Angreifer vorgehen, welche Werkzeuge sie verwenden, wie Angreifer z.B. im Darknet kommunizieren und welche Informationen sie dort zum Verkauf anbieten. Wir interessieren uns dabei vor allem auch dafür, wie weit verbreitet Sicherheitsprobleme sind, und führen dazu beispielsweise Messungen des gesamten Internets durch. Wir untersuchen also nicht nur, wie verwundbar eine bestimmte Organisation ist, sondern wie verwundbar z.B. ein bestimmter Wirtschaftssektor, ein bestimmtes Land oder auch wie verwundbar das gesamte Internet ist. Dafür suchen wir selbst nach Schwachstellen genau wie es Angreifer täten. Zum Beispiel untersuchen wir Schwachstellen, die Angreifer ausnutzen können, um die Kommunikation z.B. zwischen Banken und ihren Kunden umzuleiten. Durch solche Umleitungen erreichen die Angreifer, dass die Nachrichten die Netze der Angreifer durchlaufen. So können die Kriminellen die Kommunikation abhören und manipulieren. Tatsächlich gibt es viele solcher Schwachstellen, oft auch in genau den Systemen, die solche Umleitungsangriffe eigentlich verhindern sollten. Wenn wir solche Schwachstellen finden, evaluieren wir die Umleitungsangriffe und geben Empfehlungen, wie die Betroffene die Lücken beheben können. Um Schwachstellen im gesamten Internet zu untersuchen, entwickeln wir Methoden, die unsere Suche automatisieren. Denn nur durch Automatisierung können solche Analysen für Wirtschaft und Gesellschaft zugänglich werden.

Dr. Haya Shulman,
Head of Cybersecurity Analytics and Defences, Fraunhofer SIT

> Vor allem müssen Organisationen „Cyber-Brandschutzübungen" durchführen. „

Wir entwickeln Werkzeuge und Methoden, wie man Schwachstellen, Fehler und Fehlkonfigurationen vermeiden kann. Angefangen von der Software, der automatisierten Konfiguration von Sicherheitsmechanismen bis hin zur Entwicklung neuer, robuster und ökonomisch einführbarer Sicherheitsmechanismen z.B. für das Routing im Internet und die Verschlüsselung.

Fazit

Cyberangriffe sind eine ernsthafte Bedrohung für Wirtschaft, Staat und Gesellschaft. Als Organisation kann man sich aber schützen: Die Mehrzahl der heutigen Angriffe kann mit bekannten Methoden abgewehrt werden. Damit das gelingt, muss man Cybersicherheit zur Chefsache machen, in jeder einzelnen Organisation wie auch in der Politik. Man muss in Cybersicherheit aber nicht nur heute, sondern dauerhaft investieren und sie damit aktuell und wirksam halten. Man muss permanent verstehen, wo die Schwachstellen liegen, wie verwundbar man ist, was man konkret zur Aufrechterhaltung und Verbesserung der Cybersicherheit tun kann. Schwachstellen entstehen fast immer durch mangelndes Wissen, mangelnden Überblick über die eigene IT und Organisation und durch schlichte menschliche Fehler in Programmierung und Konfiguration von IT.

Um diese Probleme zu meistern, müssen wir den Grad der Automatisierung in der IT dramatisch erhöhen. Sowohl in den Sicherheitsanalysen als auch in der Entwicklung und Konfiguration von Sicherheitslösungen. Forschung wie die, die wir in ATHENE leisten, spielt dabei die entscheidende Rolle. ■

Fotos: Getty, Fraunhofer SIT/ Farideh Diehl

Advertorial

Effektive Absicherung gegen Ransomware-Angriffe

Mit technologischem Vorsprung den Angreifern die Stirn bieten

von Dominik Bredel

Ransomware-Angriffe sind auch im Jahr 2021 eine der größten Bedrohungen im IT-Umfeld für Unternehmen. Beispielsweise ordnet das US-Justizministerium in diesem Jahr Ermittlungen im Kontext von Ransomware-Angriffen die gleiche Priorität zu wie herkömmlichem Terrorismus. Aber auch lokale Institutionen, wie das BSI schätzen in ihrer Bedrohungslage 2021 Ransomware-Angriffe als eines der Hauptangriffsszenarien von Cyberkriminellen, da es sich in den vergangenen Jahren als lukratives Geschäftsmodell entwickelt hat.

Was ist Ransomware?

Bei einer Ransomware-Attacke handelt es sich um einen Cyber-Angriff, der weitflächig den Zugriff auf Dateien und IT-Systeme eines Unternehmens verhindert. Im Regelfall wird dies durch die Verwendung von Verschlüsselungsmechanismen erreicht. Anschließend fordern die Angreifer das Opfer auf ein Lösegeld zu zahlen, um ihre Dateien und Systeme wieder zu entschlüsseln.

Bedrohungslage 2021

Dabei zeigt die Erfahrung der vergangenen Jahre, dass potenziell jedes Unternehmen von einem Ransomware-Angriff betroffen sein kann. Aktuell genutzte Angriffsvektoren, wie die zunehmende Nutzung von Einfallstoren über Lieferanten oder Partneranbindungen im Netzwerk, oder bewusst nicht auf einzelne Unternehmen ausgerichtete Ransomware-Varianten, ergeben eine Bedrohungslage, die jedes Unternehmen unabhängig von Größe und Branche treffen kann.

Darüber hinaus ist in der jüngsten Vergangenheit eine weitere Professionalisierung von Ransomware-Angriffen zu beobachten. Angreifer bieten mittlerweile sogenannte Ransomware-as-a-Service Lösungen an, die wie in herkömmlichen Onlineshops erworben werden können.

War es vor wenigen Jahren also nur technisch versierten Personen möglich eine Ransomware-Attacke durchzuführen, ist dies heute einem breiten Personenkreis möglich. Es reicht kriminelle Energie, um einen Cyber-Angriff in die Wege zu leiten.

Effektive Absicherung

Die Auswirkungen eines erfolgreichen Ransomware-Angriffs sind weitreichend. Unternehmen sollten daher effektive technologische Maßnahmen ergreifen, um finanzielle und weitere Schäden so gering wie möglich zu halten.

Fakt ist aber auch: Unabhängig davon welche Abwehrmaßnahmen implementiert werden, kann eine Ransomware-Attacke nicht zu 100% ausgeschlossen werden. Daher sollte der Fokus von Unternehmen nicht nur darauf liegen den Angriff selbst zu verhindern, sondern dessen Auswirkungen so gering wie möglich zu halten. Die Verbindung der nachfolgenden technischen Maßnahmen ermöglicht es genau dieses Ziel zu erreichen:

> Die Auswirkungen eines erfolgreichen Ransomware-Angriffs sind weitreichend.

Dominik Bredel,
Associate Partner Security and Resilience, kyndryl

1. Einsatz von „Air Gaps“

Unter einem „Air Gap“ versteht man eine durch Segmentierung implementierte Trennung zwischen Produktions-Umgebungen und der Backupinfrastruktur. Dabei existiert eine Verbindung zwischen beiden Infrastrukturen nur dann, wenn Backups geschrieben werden.

2. Nutzung von unveränderbarem Speicher

Die Einsatzbereiche von unveränderbaren Speichern waren in der Vergangenheit durch langsame Zugriffszeiten limitiert. Moderne Speichersysteme ermöglichen mittlerweile eine software-basierte Realisierung eines „write-once-read-many“ Ansatzes, sowie schnelle Wiederherstellungszeiten.

3. Kontinuierliche Verifikation von Backup-Daten

Der Einsatz einer Datenvalidierungs-Engine stellt sicher, dass gesicherte Daten und Konfigurationen von Systemen „sauber“ und „brauchbar“ sind, indem ein kontinuierlicher Abgleich mit aktueller Malware vorgenommen wird.

4. Automatisierung von Disaster Recovery

Die ersten drei Maßnahmen sollten es ermöglichen, dass das Backup unbeschadet und unverschlüsselt ist. Um das „Golden-Master“ Backup dann wiederherstellen zu können empfiehlt sich der Einsatz von Automatisierungslösungen im Kontext von Disaster Recovery.

Durch die intelligente Kombination dieser vier Technologien und Mechanismen ist es möglich, zu jedem Zeitpunkt sicher zu stellen, dass selbst, wenn ein Ransomware-Angriff erfolgreich war, man als Unternehmen in der Lage ist, in einem kurzen Zeitraum von einem unverschlüsselten Backup eine Wiederherstellung der kritischen Applikationen vorzunehmen. Dieser technologische Vorsprung ermöglicht es Unternehmen, Angreifern die Stirn zu bieten und etabliert eine effektive Absicherung gegen Ransomware-Angriffe sowie die Verringerung der damit zusammenhängenden Folgen.

Als unabhängiger Technologie-Partner unterstützt Kyndryl Sie in allen Schritten der Beratung, Implementierung und des Betriebs solcher ganzheitlichen Lösungen gegen Cyber-Angriffe. Bei weiterem Interesse können Sie jederzeit gerne Kontakt mit uns aufnehmen. ■

www.kyndryl.com

kyndryl

Foto: iStock Photo

Advertorial

Wie IT-Sicherheit der nächsten Generation aussieht

Cyberkriminelle agieren cleverer als je zuvor. Standard-Antiviren-Software ist deshalb immer öfter machtlos gegen digitale Bedrohungen. Künstliche Intelligenz sorgt nun für besseren Schutz gegen Malware, Zero Day und Co.

von Frank Ziarno

Im Dezember 2020 erwischte es die Funke Mediengruppe, Anfang April 2021 den Medienkonzern Madsack: Hackerangriffe störten weite Teile der Computersysteme, Zeitungen konnten nicht gedruckt werden. Anfang Mai infizierte Schadsoftware die IT-Netzwerke der Technischen Universität Berlin. Und kurz darauf sorgte ein Fall in den USA für Aufsehen: Mitte Mai 2021 legte Erpressungssoftware (Ransomware) eine der größten Pipelines des Landes lahm. Es drohten sogar Versorgungsengpässe bei Öl, Benzin und Kerosin. Nur eine Lösegeldzahlung in Höhe von rund fünf Millionen US-Dollar ermöglichte dem Pipelinebetreiber die Wiederaufnahme seines Betriebs.

Ein Cyberangriff ist für Unternehmen und Institutionen im besten Fall ein großes Ärgernis, schlimmstenfalls aber ruinös. Obwohl Cyberattacken immer ausgefeilter werden, haben mehr als 70 Prozent der deutschen Unternehmen im Jahr 2020 ihre Ausgaben für IT-Sicherheit nicht erhöht. Das ergab eine repräsentative Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Weiter heißt es dort, dass viele Firmen gerade einmal zehn Prozent des IT-Budgets für Sicherheitsmaßnahmen ausgeben – zu wenig.

Mit Machine-Learning zu größerer IT-Sicherheit

Vor allem im pandemiegeprägten Jahr 2020, in dem viele Menschen im Homeoffice gearbeitet haben, hätten die Security-Ausgaben steigen müssen. Der Grund ist simpel: Mit der Nutzung privater Netzwerke und Endgeräte im Homeoffice hat sich die Zahl potenzieller Einfallstore für Schadsoftware deutlich erhöht.

Dennoch wird das Thema Cybersicherheit weiter vernachlässigt, hat das IT-Beratungsunternehmen IDC herausgefunden. „Vorrangig in kleinen und mittleren Unternehmen vertrauen noch deutlich zu viele Verantwortliche auf Bordlösungen und Standardeinstellungen“, schreiben die Analysten in ihrer aktuellen Umfrage zur Cybersecurity in Deutschland. Angesichts des Umstandes, dass drei von vier befragten Unternehmen in jüngster Vergangenheit Ziel einer erfolgreiche Cyberattacke wurden, sei solch eine Strategie „hochriskant“.

Gründe für mehr Schutz gibt es also reichlich. Deshalb haben wir in Kooperation mit Malwarebytes eine Echtzeit-Endpunkt-Sicherheitslösung in die eigene Software integriert. Mit dieser Lösung lassen sich Endgeräte und Server vor Cyberbedrohungen schützen. Künstliche Intelligenz (KI) erhöht den Schutz.

Der zusätzliche Schutz durch KI macht in der Praxis einen großen Unterschied zu konventionellen, ausschließlich signaturbasierten Sicherheitslösungen. Beim signaturbasierten Ansatz wird nur nach bekannter Schadsoftware gesucht. Welche Software gut und welche schlecht ist, definieren regelmäßige Updates. Selbstlernende Sicherheitsalgorithmen hingegen erkennen Schadsoftware anhand ihres Verhaltens, beispielsweise durch eine höhere Prozessorauslastung auf einem Endgerät, Aktivitäten zu ungewöhnlichen Uhrzeiten oder andere Anomalien beim Ausführen eines Programms.

Frank Ziarno,
Director Product Management, TeamViewer

NextGen-Lösung inklusive „Rollback-Versicherung“

Dieser von den Fachleuten „NextGen“ – kurz für: Next Generation – genannte Ansatz entdeckt auch, was Madsack, Funke und die TU Berlin beschäftigte: die sogenannten Zero-Day-Exploits. Mit dieser Art Angriff nutzen Cyberkriminelle noch unbekannte Sicherheitslücken – und zwar sofort (gefährlich ab Tag Null: Day Zero). Unser Anwendung bewahrt Netzwerke außerdem zugleich vor weiteren Gefahren wie Viren, Trojanern, Ransomware oder Bruteforce-Attacken – sie vereint insgesamt sieben verschiedene Erkennungstechniken.

> Zusätzliche Cybersecurity durch KI macht einen großen Unterschied zu ausschließlich signaturbasierten Lösungen.

Doch was passiert, wenn diese Vorkehrungen nicht ausreichen? Dieses Szenario deckt TeamViewer ebenfalls mit ab: Mit der Lösung „Endpoint Detection & Response“ (EDR) lassen sich infizierte Endgeräte vom restlichen Netzwerk isolieren und trotzdem noch mit unserer Software ansteuern, um das Sicherheitsproblem eingehender zu untersuchen. Die Funktion „Ransomware Rollback“ macht es möglich, verschlüsselte Dateien bis zu 72 Stunden nach Manipulation wieder in den Ursprungszustand zu versetzen. Das ist wie eine Versicherungspolice.

Die Frage ist nicht, ob ein Angriff kommt, sondern nur, wann er erfolgt. Unternehmen sollten deshalb gewappnet sein. Dank NextGen-Technologie war Cybersicherheit noch nie so leistungsstark und einfach zugleich. ■

www.teamviewer.com

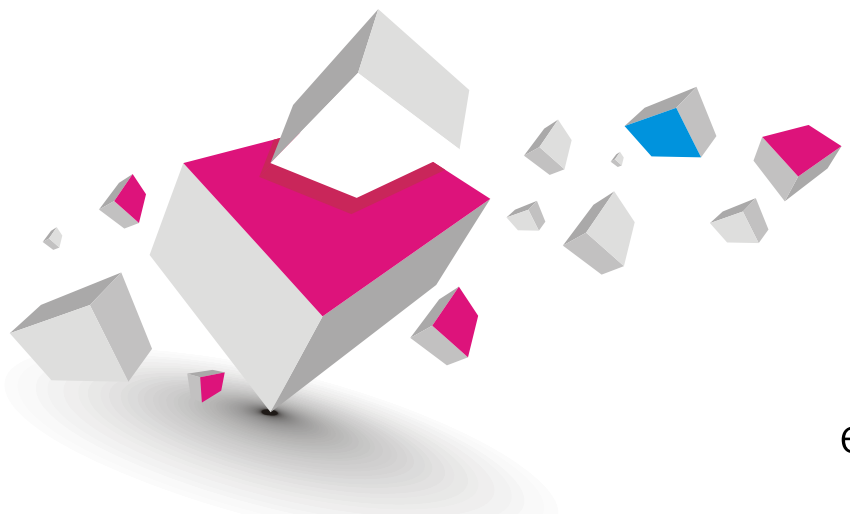
Lesen Sie mehr über Digitalisierung „Made in Germany“ im TeamViewer-Themenhub auf Handelsblatt Online:

TeamViewer

Advertorial

NACH DER RANSOMWARE-INFEKTION:

Neugestalten oder wiederaufbauen?



Noch immer wird die Gefahr unterschätzt, ins Visier von Ransomware-Akteuren zu geraten. Erst wenn die Lösegeldforderung für verschlüsselte Daten eingeht, werden Hebel in Bewegung gesetzt. Doch in welche Richtung sollten Unternehmen im Falle eines Cyber-Angriffs denken?

von Kevin Schwarz

Das exponentielle Wachstum der mit dem Internet verbundenen IT-Infrastrukturen vergrößert die Angriffsfläche für eine Malware-Infektion. Viele Unternehmen exponieren Informationen ihrer IT-Systeme, ohne sich dieser Gefahr bewusst zu sein. Homeoffice, Multicloud-Umgebungen oder Web-Server: IT-Abteilungen fehlt häufig der Überblick, welche dieser Systeme dem Internet ausgesetzt sind, und bieten dadurch Angriffsflächen.

Angriffsfläche wird genutzt

Auch wenn die Sicherheitsmodernisierung im Zuge der allgemeinen Transformation in die Cloud berücksichtigt werden sollte, reagieren viele Unternehmen zu spät. Mal sind es mangelnde Ressourcen oder Budgets für eine Security Transformation, mal gibt man sich mit der Anhäufung von Bitcoins oder Cyber-Versicherungen zufrieden.

Unternehmen tun jedoch gut daran, sich mit strategischen Überlegungen in Form von Incident-Response-Plänen zu befassen, um auch auf diese Weise vorbereitet zu sein. Backup- und Disaster Recovery-Strategien sind notwendig, um im Ernstfall eines Angriffs die befallenen Systeme wieder herzustellen. Wichtig ist auch, die Kontrolle über die gekaperten Systeme schnell zurückzugewinnen. Da eine komplette Bereinigung und Wiederherstellung von Daten Zeit in Anspruch nehmen, sollte parallel der Zugriff auf wichtige Anwendungen in einem vertrauenswürdigen Modus aufgebaut werden. Hier kann ein Zero-Trust-Ansatz helfen, der einen sicheren und getunnelten Zugang zu einzelnen Anwendungen aufbaut.

Hochfahren oder Neuaufbau?

Nach einer Ransomware-Infektion gilt es außerdem zu überlegen, ob es sinnvoll ist, zur ursprünglichen Security-Architektur zurückzukehren. Kann einer Sicherheitsinfrastruktur weiterhin vertraut werden, wenn sie sich als überwindbar herausgestellt hat? Wenn die forensische Untersuchung zeigt, welche Einfallstore die Angreifer nutzen konnten, sollten diese geschlossen und stärker gesichert werden. Vor allem aber sollte die Sicherheit der gesamten IT-Infrastruktur auf den Prüfstand und alle bisherigen Sicherheitskonzepte hinterfragt und die Chance für eine Neuausrichtung im Zusammenspiel mit der Cloud-Transformation genutzt werden.

www.zscaler.de

Kevin Schwarz,
Director Transformation Strategy, Zscaler EMEA

> Kann einer Sicherheitsinfrastruktur weiterhin vertraut werden, wenn sie sich als überwindbar herausgestellt hat?

Foto: iStock Photo

Advertorial

Mittelstand im Fadenkreuz von Cyberkriminellen

Cybercrime ist eines der größten Risiken des 21. Jahrhunderts. Neue technologische Entwicklungen, Digitalisierung und Videostreaming führen im Privatbereich und bei Unternehmen zu weitreichenden Gefahren.

Digitalisierung bietet nicht nur der Wirtschaft Chancen, sondern leider auch Kriminellen. Und diese nehmen nicht nur Großkonzerne ins Visier: In einer Umfrage bei mittelständischen Unternehmen erklärten 55 Prozent der Befragten, dass ihre Firma bereits einen Hackerangriff erlitten hätte. 70 Prozent sagten, dass sie mit einem Angriff in der nahen Zukunft rechnen würden. Für die Erhebung befragte das Marktforschungsinstitut Appinio im Frühjahr 2021 im Auftrag der Württembergischen Versicherung 200 Entscheiderinnen und Entscheider im deutschen Mittelstand.

Da mittelständische Betriebe häufig schlechter vor Cyberrisiken geschützt sind als Großunternehmen, sind sie attraktive Angriffsziele. Hackerinnen und Hacker können vertrauliche Firmen- und Kundendaten stehlen, das Unternehmen erpressen oder den Betriebsablauf lahmlegen. Neben Ertragsausfällen und Kosten für die Datenrettung droht oft ein Verlust von Reputation und Kundenvertrauen.

Als Partner des Mittelstands, der auf die Absicherung von Betriebsabläufen spezialisiert ist, empfiehlt die Württembergische den doppelten Schutz: Firmen sollten das Risiko eines erfolgreichen Angriffs über Prävention senken und sich gegen finanzielle Folgen im Ernstfall absichern.

Vorbeugend gilt, Schwachstellen in der eigenen IT zu identifizieren und diese sowohl durch technische Maßnahmen als auch interne Schulungen abzudichten. Denn die Gefahren sind vielseitig, je nach Betrieb unterschiedlich und nicht nur durch Technik, sondern auch durch das Verhalten der Nutzerinnen und Nutzer bedingt. So erfolgen die meisten Cyberattacken auf den Mittelstand per E-Mail: 40 Prozent der Befragten berichteten von solchen Angriffen. Angestellte werden darin verleitet, schädliche Links oder Anhänge anzuklicken, oder es werden Zahlungsaufträge der Geschäftsleitung vorgegaukelt. Eine Sensibilisierung der Belegschaft reduziert dieses Kern-Risiko erheblich.

Gelingt ein Cyber-Angriff, helfen regelmäßige Daten-Backups und eine Cyber-Versicherung, den Schaden einzugrenzen. Die Württembergische verbindet in ihrem Angebot beide Ansätze: Die Cyber-Police schließt neben Schadensbehebung, Übernahme des Ertragsausfalls und Krisenkommunikation auch Beratungsleistungen wie Präventionstrainings mit ein.

www.wuerttembergische.de

württembergische

Foto: Adobe Stock/Song_about_summer

Foto: Getty

CYBER-RESILIENZ

FÜR UNTERNEHMEN DER KRITISCHEN INFRASTRUKTUR

Cyber-Security muss auf einer neuen Ebene stattfinden

von Dr. Michael Ebner

Präsident Joe Biden musste am 9. Mai 2021 den nationalen Notstand für die USA erklären. Und das wegen eines kompromittierten Passwortes für ein altes Mitarbeiterkonto für den Fernzugang auf das IT-System der größten Kraftstoff-Pipeline der USA, Colonial Pipeline. Da nicht klar war, wie groß der Schaden durch die Ransomware-Attacke war, hatte das Unternehmen seine Anlagen vorsorglich selbst heruntergefahren. Es kam zu Kraftstoffengpässen an Tankstellen der Ostküste der USA, ein Flughafen machte dicht, Flüge fielen aus und die Panik führte zu Hamsterkäufen. Nach ein paar Tagen war der Spuk vorbei. Doch dieser Fall hat deutlich gemacht, wie verheerend Cyber-Angriffe auf unsere kritische Infrastruktur (KRITIS) sein können und was sie für eine Kette auslösen (können).

Mit Digitalisierung und Vernetzung nimmt die Gefahr zu

Ein weiteres Beispiel: 2020 wurde der sogenannte Solarwinds Hack bekannt. Weltweit waren mehr als 18.000 Unternehmen und Behörden betroffen, sogar Teile des

Foto: Getty

Pentagon sowie Unternehmen der kritischen Infrastruktur. Einfallstor war ein verseuchtes Update der Solarwinds-Software Orion. Versicherer nennen das einen „Cyber-Hurricane“, einen Angriff auf zahlreiche Unternehmen durch gemeinsam genutzte Infrastruktur.

Die Beispiele zeigen: Cyberkriminelle werden immer professioneller und laut Bundesamt für Sicherheit in der Informationstechnik (BSI) werden vermehrt Techniken und Methoden verwendet, die zuvor nur bei strategisch ausgerichteten Spionage-Angriffen bekannt waren.

Auch für Systeme der kritischen Infrastruktur gilt: Mit zunehmender Digitalisierung und Vernetzung nimmt die Gefahr zu, dass ein Cyberangriff Auswirkungen hat, die jede und jeder spürt. Autor Marc Elsberg mit seinen Blackout-Szenarien in seinem Bestseller lässt grüßen.

Homeoffice als Schwarzer Schwan für IT-Security

Letztes Beispiel: Die pandemiebedingte Homeoffice Situation für Unternehmen war für viele IT-Abteilungen wie ein Schwarzer Schwan. Plötzlich arbeiteten tausende Mitarbeiter:innen von zuhause und mussten über das öffentliche Internet auf die internen Systeme zugreifen.

In einer unbeständigen, unsicheren, komplexen und mehrdeutigen (VUCA-)Welt und angesichts der aktuellen Bedrohungslage sind Krisen, Großschadenslagen oder Katastrophen ausgelöst durch Cyberangriffe noch mehr zu erwarten als in der Vergangenheit. Erfolgreiche Angriffe, aber auch technische oder menschliche Fehler (wie bei Facebook im Oktober 2021 passiert) werden sich nicht verhindern lassen. Solche „schwarzen Schwäne“ bzw. Worst Worst Case Szenarien sind heutzutage wahrscheinlicher geworden.

Die Antwort: Cyber-Resilienz

Unsere Antwort als Verantwortliche für die Cyber-Security auf die aktuellen Entwicklungen: Die Entwicklung einer Cyber-Resilienz. Für das World Economic Forum bezieht sich Cyber-Resilienz auf die Fähigkeit von Organisationen, eine „Langzeitstrategie zur Widerstandsfähigkeit von technischen Systemen in Bezug auf Cyber-Ereignisse“ zu entwickeln.

Auf EU-Ebene sind schon entsprechende Verordnungen und Gesetze für kritische Infrastrukturen in Vorbereitung bzw. verabschiedet. Cyber-Resilienz in kritischen Infrastrukturen wird eine entscheidende Voraussetzung für die Aufrechterhaltung der Versorgungssicherheit sein.

Stärkere Integration als Weg zur Cyber-Resilienz

Was kann nun pragmatisch die Basis sein für solch eine Langzeitstrategie? Wie können Sicherheitsverantwortliche vorgehen?

Bei der EnBW haben wir uns mit der Cyber-Resilienz ein neues langfristiges Zielbild gegeben und dabei berücksichtigt, wohin sich das EnBW Geschäft entwickeln will. Agilität, Integration, Ganzheitlichkeit, Out-of-the-Box-Denken und Handlungsfähigkeit sind für unseren Ansatz nur einige Stichworte.

Dabei ist eines gesetzt: Die Fortführung der Absicherung der Industrieanlagen und kritischen Infrastrukturen. Dazu zählen insbesondere das Management von Risiken zur Informationssicherheit (ISMS) und eine Cyber-Abwehr durch Systeme zur Angriffserkennung, die per IT-Sicherheitsgesetz festgelegt sind.

Die nächste Stufe der Verbesserung ist das Management von Cyber-Risiken und den Erhalt der Handlungsfähigkeit durch eine ganzheitlichere Sicht und einen flexibleren Ansatz. Der Weg dazu ist eine noch stärkere Integration mit Business Continuity Prozessen und dem

Dr. Michael Ebner,
CISO, EnBW Energie Baden-Württemberg AG

Krisenmanagement für den Bereich der digitalen Systeme, sprich Cyber. Resiliente Enterprise Architekturen flankieren diesen Ansatz in der technischen Umsetzung. Die ganzheitliche, gemeinsame Risikosicht und die Steigerung der Handlungsfähigkeit entwickeln sich während der Reise und zeigen den weiteren Weg.

Cyber-Resilienz Governance

Im ersten Schritt ist der Rahmen im Unternehmen festzulegen, müssen die Verantwortlichkeiten geklärt und insbesondere die Steuerung für eine Cyber-Resilienz Governance definiert werden.

Die ganzheitliche Betrachtung der Cyber-Risiken erfolgt durch eine enge Verzahnung bzw. der Integration von Informationssicherheit (ISMS) und Cyber Business Continuity. Die EnBW hat daher kürzlich die Governance für beide Themen beim Chief Information Security Officer (CISO) angesiedelt.

Die Handlungsfähigkeit kann noch erhöht werden, wenn die Cyber-Abwehr ein Teil der Notfall- und Krisenorganisation des Konzerns wird. Bei der EnBW ist der CISO deshalb Teil des Konzern-Krisenstabs und damit direkte Schnittstelle zur Cyber-Abwehr Organisation.

Cyber Business Continuity

Zweiter Schritt ist die risikobasierte Ausrichtung zur Cyber-Resilienz über das Cyber Business Continuity Management. Dieser Blick ist umfassender als beim ISMS, weil der Blickwinkel erweitert wird auf notwendige Maßnahmen, um bei großen Cyberangriffen widerstandsfähiger und handlungsfähiger zu sein. Hierbei wird über den Kern der reinen Leistungserbringung kritischer Infrastrukturen noch stärker hinausgeschaut bzw. Beteiligte stärker eingebunden. Gerade die Abhängigkeit bzw. Verfügbarkeit von externen Dienstleistern oder Behörden in einer Cyber-Großschadenslage ist eine generelle Herausforderung.

Ein wichtiger Faktor, um Cyber-Resilienz zu erreichen, ist die Einbindung der Mitarbeitenden im Unternehmen. Die Durchführung von Awareness-Aktionen und Übungen sind ein gutes Mittel, um die Aufmerksamkeit zu erhalten und die Belegschaft mit den Prozessen vertraut zu machen.

Cyber-Abwehr und Krisenmanagement

Im nächsten Schritt sollte die Cyber-Abwehr stärker in die üblichen Notfall- und Krisenprozesse integriert werden. Das erfolgt über den konzernweiten Cyber-Sicherheitsvorfallsprozess, der vom EnBW Cyber Emergency Response Team (EnBW CERT) gesteuert wird. Damit arbeiten im Krisenfall die Mitarbeiter:innen der kritischen Infrastruktur und der Cyber-Abwehr noch enger Hand in Hand und können ihr Wissen schneller austauschen, um größeren Schaden abzuwenden und schnell Gegenmaßnahmen einzuleiten.

Frühzeitige Erkennung von Angriffen, Fehlern etc. sowie Informationen über die Lage und Mittel zur Reaktion darauf sind weiterhin die Basis für die Handlungsfähigkeit. Über den EnBW Full Kritis Service werden auch externen Kunden Dienstleistungen zur Cyber-Abwehr bereitgestellt.

Cyber-Resilienz by Design – Resiliente Enterprise Architekturen

Im vierten und letzten Schritt – Cyber-Resilienz by Design – ist es notwendig, sichere, integrative und agile technische Architekturen aufzubauen, um Erkennungs-, Widerstands- und Wiederherstellungsfähigkeiten zu verbessern. Die ganzheitliche Sicht und Transparenz ist eine Herausforderung in Anbetracht des Zusammenwachsens digitaler Systeme aus IT, IoT und kritischer Infrastruktur sowie Cloud-Services.

Zusammenfassend lässt sich festhalten: Die vom BSI im Lagebericht 2021 als „angespannt bis kritisch“ eingeschätzte Lage bestätigt den Trend der vergangenen Jahre, in denen die Gefahr von Cyberangriffen kontinuierlich zugenommen hat. Machen wir uns nichts vor: Die Bedrohungen und Unwägbarkeiten werden weiter zunehmen. Deshalb mein Appell, insbesondere in Unternehmen der kritischen Infrastruktur dem Thema Cyber-Security einen größeren Stellenwert einzuräumen und zur Chefsache zu machen. Das umfassende Konzept der Cyber-Resilienz bietet die Chance, Unternehmen besser zu schützen, früher zu reagieren und im Krisenfall schneller Lösungen zu finden. ■

> Das umfassende Konzept der Cyber-Resilienz bietet die Chance, Unternehmen besser zu schützen, früher zu reagieren und im Krisenfall schneller Lösungen zu finden.

Advertorial

Die digitale Achillesferse schützen

Wie Unternehmen ihre Cyberabwehr optimieren

von Moritz Anders und Dr. Alexander Köppen

Immer raffiniertere Angreifende durchforsten die dunklen Ecken von Systemen und Netzwerken, suchen – und finden – Schwachstellen. Wo auch immer die digitale Achillesferse einer Organisation liegt, Cyberkriminelle setzen alles daran, diese zu finden und geschickt auszunutzen. Egal, ob Ransomware-Angriffe, Malware über Software-Updates oder Attacken auf Cloud-Dienste: Cyberkriminalität wird in den kommenden Jahren weiter zunehmen. Davon sind knapp 60 Prozent der Führungskräfte überzeugt, die für die Studie „Digital Trust Insights 2022“ der Wirtschaftsprüfungs- und Beratungsgesellschaft PwC befragt wurden.

Viele dieser Vorfälle ließen sich mit soliden Cyberpraktiken und starken Kontrollen verhindern. Das Problem: Die Prävention von Cyberangriffen erfolgt in vielen Organisationen noch nicht systematisch und datenbasiert. Laut PwC-Studie, an der sich 3.600 Führungskräfte weltweit – davon 258 in Deutschland, beteiligt haben, setzt nur jedes fünfte Unternehmen hierzulande auf eine Quantifizierung von Cyberrisiken oder relevante Technologien wie Real-Time-Threat-Intelligence und KI-basierte Netzwerküberwachung.

Das ist ein zentrales Versäumnis, denn Cyberrisiken sind Unternehmensrisiken. Umso wichtiger ist es, dass Organisationen ihre Sicherheitslage immer ganzheitlich betrachten. Die reine Risikobewertung als Momentaufnahme wird der aktuellen Bedrohungslage nicht gerecht. Was Unternehmen jetzt brauchen, ist ein Risiko-Reporting in Echtzeit.

Dr. Alexander Köppen
Partner Cyber Security & Privacy, PwC Deutschland

Moritz Anders
Partner Cyber Security & Privacy, PwC Deutschland

Hohe Komplexität lähmt die Cybersicherheit

Eine Schwachstelle vieler Unternehmen ist dabei ihre hohe Komplexität: Mehr als 80 Prozent der IT-Führungskräfte in Deutschland halten die Technologien, Daten und Betriebsumgebungen in ihren Unternehmen für unnötig komplex – und schätzen, dass sie daher nicht optimal gegen Cyberangriffe geschützt sind.

Dabei bringt die Vereinfachung des Betriebs, der Prozesse und der zugehörigen Systeme handfeste Vorteile: Sie hilft einer Organisation dabei, ihre Cyberrisiken schneller zu erfassen und die IT-Sicherheit zu verbessern. Diese Erkenntnis setzt sich jedoch nur langsam durch: Noch nutzen zu wenige Unternehmen Daten und Automatisierung, um ihre Prozesse effizienter und schlanker zu gestalten.

> Was Unternehmen jetzt brauchen, ist ein Risiko-Reporting in Echtzeit.

Foto: iStock Photo

Auch in der Lieferkette lauern Cyberrisiken
Eine weitere große Schwachstelle in vielen Organisationen ist zudem das Risiko, das in der Lieferkette lauert: Die PwC-Studie zeigt, dass Unternehmen die Sicherheitsrisiken, die durch ihre Geschäftspartner und Zulieferer entstehen, häufig nicht vollständig überblicken. Rund ein Drittel der Führungskräfte in Deutschland gesteht ein, die IT- und Software-Risiken in ihrer Lieferkette wenig oder gar nicht zu kennen. Rund 60 Prozent haben keinerlei Maßnahmen umgesetzt, die eine nachhaltige Wirkung auf ihr Risikomanagement für Dritte versprechen.

CEOs spielen Schlüsselrolle
Das zu ändern, ist in erster Linie die Aufgabe des CEOs. Ihm oder ihr fällt bei der Optimierung der Cybersicherheit eine Schlüsselrolle zu: Die Geschäftsführung gibt in Sachen IT-Sicherheit und Datenschutz die Richtung für die gesamte Organisation vor. Sie kann Cybersicherheit als wichtigen Faktor für das Unternehmenswachstum und das Vertrauen der Kunden etablieren und unternehmensweit ein Sicherheitsbewusstsein schaffen. Diese Chance gilt es nun zu nutzen – mit Blick auf die aktuelle Bedrohungslage besser heute als morgen. ■

www.pwc.de/dti2022

WIE CYBERSICHERHEIT GELINGT – EIN LEITFADEN FÜR FÜHRUNGSKRÄFTE

- Begreifen Sie das Thema Cybersicherheit als zentral für Unternehmenswachstum und Kundenvertrauen.
- Verknüpfen Sie die Cyberrisken mit den übergreifenden Unternehmensrisiken.
- Leiten Sie das Target Operating Model für Informationssicherheit strategisch sauber her und verankern Sie es in der Organisation.
- Stellen Sie bei jedem Transformationsprojekt oder jeder neuen Geschäftsinitiative die Frage: Wie sorgen wir in diesem Bereich für Cybersicherheit?
- Managen Sie die Cyberrisiken effektiv, indem Sie diese quantifizieren und genau an den Stellen investieren, an denen die größten Effekte zu erwarten sind.
- Fühlen Sie Ihren wichtigsten Geschäftsbeziehungen auf den Zahn und nutzen Sie einen Third-Party-Tracker, um die Schwachstellen in Ihrer Wertschöpfungskette aufzuspüren.
- Erweitern Sie Ihre technologischen Fähigkeiten, um Cyberangriffe über Software aufzudecken, zu verhindern und angemessen darauf zu reagieren.
- Sensibilisieren Sie Ihre Führungskräfte für Cyber- und Geschäftsrisiken, die von Drittparteien und der Lieferkette ausgehen.

Advertorial

IT-Sicherheit ist essenziell für die Digitalisierung

Kaum ein Unternehmen kann im Jahre 2021 darauf verzichten, Digitalisierung und ihre Möglichkeiten zu nutzen. Dabei haben viele Firmen eines gemeinsam: Sie haben ein großes IT-Sicherheitsproblem!

von Jochen Meyer

Cyberangriffe in Unternehmen
Schaffen es Angreifer in das Netzwerk eines Unternehmens einzudringen und dort Schadsoftware zu platzieren, die auf Servern und Clients alles verschlüsselt und unbrauchbar macht, ist es oft zu spät. Erst wenn Produktionsbänder stillstehen, medizinische Versorgungsgeräte nicht mehr funktionieren und alle Beschäftigten nach Hause geschickt werden müssen, weil sie nicht mehr arbeiten können, geben sich die Kriminellen scheinbar zufrieden.

Die Nutzer sehen zu diesem Zeitpunkt alle Daten nur noch mit einer kryptischen Endung. Wir aus der IT-Forensik schauen deutlich genauer hin. So findet sich in jedem Verzeichnis noch ein Fußabdruck des Angreifers. Die Ransom Note ist meist eine Text- oder HTML-Datei, in der auch das Erpresserschreiben zu finden ist. Meist wird mit der Veröffentlichung oder der Weitergabe der gestohlenen Daten gedroht, wenn das Lösegeld nicht gezahlt wird.

Cybercrime als Geschäftsmodell
Die Höhe des Lösegelds liegt nicht selten in Millionenhöhe. Und selbst bei Zahlung des Lösegelds gibt es nie die Garantie, dass Sie alle Daten zurückbekommen oder diese bereits im Darknet gehandelt werden.

Organisierte Banden bieten ihre Dienste im Darknet oft „as a Service“ an. Neben politisch motivierten Angriffen gibt es auch diejenigen, die ihre Backdoors über unzählige E-Mail-Adressen streuen, mit der Hoffnung, dass irgendjemand aus dem Unternehmensnetzwerk diese Mail öffnet, den Datei-Anhang aktiviert und somit den Angreifern den Weg ins Netzwerk ermöglicht. Nachdem die Daten abgetragen wurden, räumt der Angreifer auf, löscht sämtliche wichtige Eventlogs und startet die Verschlüsselung von Hand, um weitere Spuren zu verwischen.

Prävention statt Frustration
Eine 100%ige Absicherung vor einem Cyber-Angriff gibt es nicht. Jedoch können durch präventive Maßnahmen, hochwertige Sicherheitslösungen und gutes Monitoring Sicherheitsvorfälle schneller entdeckt und der Schaden minimiert werden. Brennt ein Gebäude, ist es immer sinnvoll vorher zu wissen, wo der Feuerlöscher hängt. Die Aufgabe der IT-Sicherheit ist also: Vorbereitung auf das Unbekannte. ■

Jochen Meyer,
Senior SOC Analyst, suresecure GmbH

> Eine 100%ige Absicherung vor einem Cyberangriff gibt es nicht.

www.suresecure.de

sure[secure]

Advertorial

Haftungsfalle Hackerangriff

Digitalisierung und Cybersecurity: Doppelherausforderung für die Unternehmensleitung

von Dino Huber, Ferdinand Grieger und Andreas Pankow

Cyberangriffe stellen eine substanzielle Bedrohung für Unternehmen jeder Art und Größe dar. Die Schäden erreichten in den letzten Jahren kontinuierlich neue Höchstwerte. Allein der Angriff mit dem Erpressungstrojaner NotPetya im Jahr 2017 kostete die weltweit tätige Rederei Møller-Mærsk knapp 300 Mio. US-Dollar. Im Fall von erfolgreichen Hackerattacken drohen den Unternehmen die Inanspruchnahme durch Kunden, Lieferanten, Kooperationspartner usw. auf Basis vertraglicher und gesetzlicher Anspruchsgrundlagen. Da Cyberangriffe zumeist auch datenschutzrechtliche Implikationen aufweisen, sind ebenfalls empfindliche Bußgelder oder zumindest Opportunitätskosten durch behördliche Ermittlungen zu befürchten. Vorstände und Aufsichtsräte haften der Aktiengesellschaft gegenüber für Schäden durch erfolgreiche Hackerangriffe nach dem Aktiengesetz persönlich (§ 93 Abs. 1 Satz 1 AktG, bzw. §§ 116 Satz 1 i.V.m. § 93 AktG). Die Haftung des GmbH-Geschäftsführers ergibt sich aus dem GmbHG (§ 43 Abs. 2 GmbHG).

> Die Rechtslage ist eindeutig: Ist ein Unternehmen nicht hinreichend abgesichert, haften Führungsorgane bei Hackerangriffen mit ihrem Privatvermögen.

Cybersecurity ist nicht delegierbare Chefsache

Für Führungsorgane stellt diese Sachlage eine schwierige Doppelherausforderung dar. Einerseits müssen sie die Unternehmen durch die Fokussierung auf fortschreitende Technologien und Digitalisierung zukunftsfähig machen. Tun sie dies nicht, ist der Verlust von Marktanteilen, die Unternehmensexistenz und die Bedrohung des eigenen Arbeitsplatzes zu befürchten. Andererseits müssen sie die mit der zunehmenden Digitalisierung einhergehenden Risiken für die Unternehmen mit gleicher Aufmerksamkeit in den Blick nehmen. Diese Doppelherausforderung und die daraus resultierenden Gefahren sind vielen Führungsorganen nicht bewusst.

Vielfach besteht der Irrglaube, sich durch einen Verweis auf die mangelnde Ressortzuständigkeit in Kollektivorganen, auf Versicherungslösungen oder die Auslagerung der IT an externe Dienstleister von der Haftung exkulpieren zu können. Cybersicherheit ist jedoch nicht delegierbare Chefsache. Eine haftungsrechtlich relevante Übertragung auf ein Mitglied eines Kollektivorgans oder externe Dienstleister ist kaum möglich. Versicherungslösungen weisen oft umfängliche Haftungsausschlüsse und damit im Schadensfall Deckungslücken auf. Die Rechtslage ist eindeutig: Ist ein Unternehmen nicht hinreichend abgesichert und kommt es zu einem erfolgreichen Hackerangriff, haften Führungsorgane mit ihrem Privatvermögen.

Dino Huber,
CEO, Deutsche Gesellschaft für Cybersicherheit

Ferdinand Grieger,
CLO, Deutsche Gesellschaft für Cybersicherheit Switzerland

Andreas Pankow,
CEO, Deutsche Gesellschaft für Cybersicherheit Switzerland

Neben Standards müssen Unternehmen auf leistungsstarke und anerkannte Cybersecurity-tools setzen

Um dieser Haftungsfalle zu entgehen, ist ein abwehrfähiges Information Security Management System notwendig. Mittlerweile existieren hierfür anerkannte Standards. Es ist jedoch unabdingbar, hierüber hinaus marktübliche und leistungsfähige Tools und Prozesse einzusetzen, um der Gefahr von Cyberattacken entgegenzutreten. Neben regelmäßigen Penetrationstests (simulierte Hackerangriffe) sollte die eigene IT-Infrastruktur auch einer ständigen Überwachung durch einen Schwachstellenscanner unterliegen. Der Einsatz von Schwachstellenscannern stellt eine erste Maßnahme zur Prävention von Hackerattacken dar.

Der Markt spiegelt den Bedarf an diesem Cybersecuritytool mittlerweile gut wider. Erfreulicherweise gibt es auch Lösungen „Made in Germany“, was aus Gründen der Rechtssicherheit im Hinblick auf die durch die Scans gewonnenen Erkenntnisse von Relevanz sein kann. Mit Hilfe eines solchen Scanners sollte eine kontinuierliche Analyse der Cybersicherheit durch dauerhafte und wiederkehrende Scans in unternehmensgerechten Intervallen erfolgen. Die Scans sollten eine gewisse „Tiefe“ nicht unterschreiten und auch eine Darknet-Analyse umfassen. Ein nachvollziehbares Scoring kann dem Nutzer dann wichtige Anhaltspunkte zum Status Quo seiner Cybersicherheit liefern. Die Nutzung möglichst vieler Datenquellen und einer eigenen Schwachstellendatenbank sind zudem qualitätsbestimmende Parameter. Von entscheidender Bedeutung ist schließlich die professionelle Begleitung des Schwachstellenscanners zur qualifizierten Ergebnisanalyse und kompetenten Maßnahmenbegleitung. Eine qualifizierte und konstante Schwachstellenanalyse kann zudem dazu beitragen, die Versicherbarkeit bestimmter Risiken sowohl für die Unternehmen als auch die Assekuranz verbindlicher und sicherer einschätzen zu können.

Werden diese Aspekte hinreichend berücksichtigt, können Schäden durch Hackerangriffe und somit die Inanspruchnahme der für Cybersicherheit verantwortlichen Führungsorgane vermieden werden. ■

www.dgc.org

DEUTSCHE GESELLSCHAFT FÜR CYBERSICHERHEIT

Fotos: Jörg Östreich, Nadja Langenbach (2)

Advertorial

IT-Security – Die Zukunft ist Software

Agilität und flexibles Handeln als Erfolgsfaktoren für Business Continuity

von Benjamin Isak

Der schnelle Übergang zum Homeoffice im Jahr 2020 und der weiter anhaltende Wechsel auf hybride Arbeitsmodelle stellen nicht nur Unternehmen branchenübergreifend vor komplexe Herausforderungen bezüglich ihrer IT-Sicherheit. Auch der gesamte öffentliche Sektor wie Behörden und Ministerien, die zu jeder Zeit essenzielle Services für Land und Bevölkerung unterbrechungsfrei erfüllen müssen, stehen unter Zugzwang.

Dabei steigt naturgemäß der Druck auf die IT- und Security-Teams. Die Business Continuity muss zu jeder Zeit gewährleistet sein und gleichzeitig sollen Mitarbeiter im Homeoffice oder unterwegs sicher, flexibel und komfortabel arbeiten können.

Um dies zu erreichen, sollte man in Sachen IT-Sicherheit auf skalierbare Software-Lösungen setzen und dies sowohl im Enterprise-Bereich, als auch bei der Kommunikation von Verschlusssachen (VS-NfD) bei Behörden und geheimschutzbetreuten Unternehmen.

Schnelligkeit gewinnt!

Eine wesentliche Herausforderung stellt die Reaktionsgeschwindigkeit im Handeln dar: Wie zügig und robust kann ein Unternehmen reagieren, wenn von heute auf morgen die Anzahl der Mitarbeiter im Homeoffice stark erhöht werden muss? Was bedeutet dies für eine vorhandene Remote-Access-/Enterprise-VPN-Infrastruktur? Hierbei unterscheidet man, wo und wie die Umgebung konzipiert ist und betrieben wird:

- **OnPremise**
  Das Unternehmen betreibt alle Netzwerk-Lösungen und Anwendungen selbst in den eigenen Räumlichkeiten oder dem eigenen Rechenzentrum.

- **In der Cloud**
  Jegliche Netzwerk-Infrastrukturen und Anwendungen laufen in der Cloud und werden dort gehostet, gegebenenfalls werden sie sogar von Dritt-Anbietern betrieben.

- **Hybrid**
  Hierbei handelt es sich um einen Mischbetrieb aus Cloud und OnPremise.

Arbeiten Sie schon oder warten Sie noch?

Egal welches Betriebsmodell man wählt: Software schafft den entscheidenden Vorteil. Besonders bei Fragen der Skalierbarkeit und Lieferzeiten hat eine Software-Lösung für Enterprise-VPN die Nase vorn. In den aktuell schwierigen Zeiten mit globalem Chipmangel sowie massiv gestörten Lieferketten kann Hardware, wie beispielsweise ein Gateway für Remote-Access, im Zweifel gar nicht oder erst nach Monaten geliefert werden.

Zeit, die gerade dann nicht vorhanden ist, wenn eine Infrastruktur für gestiegenen Homeoffice-Bedarf unvorhergesehen schnell erweitert werden muss. Wie es sich hierbei mit der Aufrechterhaltung der Geschäftskontinuität und der Flexibilität in den Handlungsmöglichkeiten als Unternehmen verhält, liegt auf der Hand.

Betrachtet man den gleichen Fall unter Einsatz einer rein softwarebasierten Enterprise-VPN-Lösung, stellt sich das Szenario völlig anders dar. Und dabei ist es nicht von Belang, wo oder in welchem Betriebsmodell die Lösung läuft.

Zur Erweiterung einer Remote-Access-Infrastruktur ist der Prozess teils aufwendig, wenn Hardware zugekauft und konfiguriert werden muss. Wer hingegen softwarebasiert aufgestellt ist, kann seinen Anbieter direkt kontaktieren und innerhalb von Minuten durch Software- und Lizenzbereitstellung die Infrastruktur erweitern, wenn nicht sogar die Userzahl verdoppeln. Hierdurch kann Mitarbeitern in kürzester Zeit ein sicherer und performanter Zugang zum unterbrechungsfreien Arbeiten von überall ermöglicht werden.

Echte Virtualisierbarkeit und Skalierbarkeit machen den Unterschied

Zentralkomponenten wie Gateways und VPN-Management sind für alle Anwender vollumfänglich virtualisierbar und können hochverfügbar zugeschaltet werden. Die Geschäftstätigkeit ist somit zu jeder Zeit sichergestellt und unternehmerische Flexibilität bleibt bestehen. Eine Software-Lösung stellt also die Voraussetzung für nachhaltiges Handeln und echte Cyber-Resilienz dar!

Benjamin Isak,
Director Sales Public & Defence, NCP engineering GmbH

An dieser Stelle bieten etablierte deutsche Hersteller wie NCP engineering aus Nürnberg als Experten für IT-Security und Secure Communications passende und teils vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bis zur Geheimhaltungsstufe VS-NfD zugelassene Lösungen an. Unternehmen, Behörden und Ministerien sind mit diesen Produkten sicher und zukunftsfähig in Bezug auf digitale Souveränität und Cyber-Resilienz aufgestellt.

www.ncp-e.com

VIELFÄLTIG UND WERTVERBUNDEN

Erfolgreiche Cybersicherheit-Teams müssen nicht nur so unterschiedlich und vielseitig wie die Angreifer sein, gegen die sie sich täglich behaupten müssen. Sie sollten auch eine Wertegemeinschaft bilden. Nur so können sie mit Erfolg der stetig wachsenden Cyberbedrohung gerecht werden.

von Natalia Oropeza

Cyberattacken kommen von überall her – und oft aus unerwarteter Richtung. Die Angreifer reichen von jugendlichen Hackern über kriminelle Organisationen bis hin zu staatlichen Akteuren mit unbegrenzten Ressourcen. Ihre Methoden sind vielgestaltig: Denial-of-Service-Angriffe, in Lieferketten eingeschmuggelte Schadsoftware oder Phishing-Mails, die Benutzer verführen, auf scheinbar harmlose Links oder Dokumente zu klicken. Vielfältig sind auch ihre Ziele: Sabotage, Spionage oder Gelderpressung. Und die Schäden gehen in die Abermilliarden.

Um sich dagegen zu verteidigen, braucht es Teams von Cybersicherheitsexpert:innen, die nicht aus einem Holz allein geschnitzt sind. Sie müssen unterschiedliche Erfahrungen, Talente, Perspektiven, Denkweisen und Lebensläufe mitbringen, denn erst aus einer Vielfalt von Ideen und Vorschlägen erwachsen Lösungen, die den heutigen Bedrohungen gewachsen sind.

Mehrere Studien haben bestätigt, dass kognitiv diverse Teams erfolgreicher sind. Ein McKinsey-Report von 2020 etwa stellte anhand der Daten von 1.000 Unternehmen fest, dass Firmen mit größerer ethnischer und Geschlechtervielfalt wirtschaftlich deutlich besser abschneiden. Allerdings laufen zufällig bunt zusammen gewürfelte Teams Gefahr, sich nicht einig zu werden. Deshalb ist neben Diversität ebenso wichtig, dass Mitarbeitende auf der Grundlage gemeinsamer Werte stehen. Das mag in der Altenpflege der Dienst am Menschen sein, in einem Technologieunternehmen Innovation oder überall Leitprinzipien wie jene, neben Diversität auch für Chancengleichheit und Inklusion zu sorgen. Ein gutes Team ist daher immer auch eine Wertegemeinschaft.

Natalia Oropeza, Chief Cybersecurity Officer und Chief Diversity Officer, Siemens AG

> Siemens registriert monatlich rund 1.000 Cyberangriffe weltweit.

Harter Wettbewerb um die besten Talente

Beides verwirklicht Siemens in seiner Cybersecurity-Abteilung. Diversität bedeutet in unserem Unternehmen nicht nur Geschlechtervielfalt – es geht auch um Alter, ethnische Zugehörigkeit, sexuelle Orientierung, soziale Herkunft oder zum Beispiel Nationalität. So betreibt Siemens weltweit fünf große Cybersecurity-Standorte, deren Mitarbeitende mehr als 25 Nationen angehören. Auf diesem Wege verfügt mein Team über eine Vielfalt von Denkweisen, die Innovation, kreatives Denken und schnelle Problemlösungen fördern.

Die Folge: Ein starkes, weltweit aufgestelltes Team. Und das ist in der Tat nötig: Siemens registriert mit seinen rund 300.000 Mitarbeitenden und hunderten Fabriken monatlich rund 1.000 Cyberangriffe – Tendenz steigend –, die innerhalb kürzester Zeit erfolgreich ab-

Foto: Bernhard Huber

gewehrt werden müssen. Das Team entwickelt außerdem innovative Sicherheitslösungen, um den Angreifern einen Schritt voraus zu sein, und sorgt dafür, dass alle Mitarbeitende des Konzerns verstehen, wie wichtig Cybersicherheit auch in ihrem Arbeitsalltag ist.

Grundsätzlich hilft die Vielfalt eines Teams auch, dass sich mehr Jobkandidaten für ein Unternehmen interessieren. So ergab eine Umfrage unter Nutzern von Glassdoor – einer Webseite, auf der Arbeitgeber bewertet werden –, dass Diversität für 76 Prozent ein wichtiges Kriterium für die Wahl eines Arbeitsplatzes ist. Das fällt umso mehr für Cybersecurity ins Gewicht, denn hier gibt es weltweit einen stets größer werdenden Mangel an Expert:innen und folglich einen harten Wettbewerb um die besten Talente.

Um attraktiv zu wirken, muss sich die gesamte Kultur der Branche verändern. In der Informatik wird beispielsweise das Begriffspaar „Master/Slave“, um Hierarchien für Datenübertragung in Netzwerken zu charakterisieren, heute immer weniger eingesetzt. Auch sind Zweifel angebracht, wie gut KI-Programme sind, die mit Datensets trainiert werden, die allein eine homogene Gruppe ausgewählt hat. Lange herrschte in männlich dominierenden Cybersecurity-Kreisen etwa auch die Haltung vor, dass es für alles eine technologische Lösung gibt. Aber auch das stimmt nicht. Das sind nur wenige Beispiele, die zeigen, warum dieser Wandel Richtung Vielfalt so wichtig ist. Und wir als Firmen müssen alles daran setzen, ihn voranzutreiben.

> Ein gutes Team ist immer auch eine Wertegemeinschaft.

Mehr Engagement der Mitarbeitenden

Wer sich bei einem Unternehmen bewirbt, will aber nicht nur eine diverse Kultur, sondern eine Art Zuhause finden, schließlich verbringen Menschen einen großen Teil ihres Lebens bei und mit der Arbeit. Das bedeutet, dass Mitarbeitende sich mit den Werten einer Organisation identifizieren können müssen. Werte, die von außen weniger sichtbar sein mögen, die aber Mitarbeitende alltäglich erleben und die letztlich dazu führen, dass sie sich mit einem Unternehmen identifizieren.

Chancengleichheit etwa bedeutet flexible Arbeitsbedingungen für Menschen, die Kinder zu Hause haben oder einen alten Menschen pflegen müssen. Auch, dass alle Zugang zu denselben Informationen haben und es für die gleiche Arbeit den gleichen Lohn geben muss. Inklusion wiederum zielt darauf ab, dass jede Stimme in einem Unternehmen gehört wird, selbst, wenn das für manchen unbequem sein mag.

Denn inklusive Arbeitskultur und Diversität führen zu einem höheren Engagement der Mitarbeitenden. Beides hilft ihnen, Sinn in ihrer Arbeit zu sehen – und sich entsprechend einzubringen. Eine Situation, von der Firmen wie Mitarbeitende gleichermaßen profitieren.

Daher setzt Siemens in seinen Cybersecurity-Teams vieles daran, sie nicht nur divers zu gestalten, sondern dass unsere Mitarbeitenden dort eine Art Heimat finden. Das ist gut, aber es gibt zweifelsohne auch noch viel zu tun. ■

Advertorial

ZERO TRUST:

Sicherheit für die IT in Zeiten hybrider Arbeitsmodelle

New Work und Remote Offices haben zu einer Fülle neuer Angriffsvektoren für Cyberkriminelle geführt – und gefährden damit die IT-Infrastruktur von Unternehmen akut. Ob sensible Daten, das gesamte Rechenzentrum oder die Reputation: Die Schäden können in vielen Bereichen gravierend sein. Je mehr Menschen remote arbeiten, desto wichtiger werden sichere Unternehmensnetzwerke. Es ist Zeit für Zero Trust.

Was ist Zero-Trust-Sicherheit?

Bis heute basiert der primäre Schutz vieler Unternehmen auf einer eher klassischen Netzwerkarchitektur und aus Authentifizierungsbarrieren. Wer sie passiert, dem stehen alle Anwendungen zur Bearbeitung offen. Das bedeutet: Jeder Mitarbeiter hat zumindest theoretisch Zugang zu allen Systemen und Anwendungen, auch wenn er die Anwendung überhaupt nicht benötigt. Das Zero-Trust-Modell geht einen anderen Weg. Es sorgt durch dynamische Sicherheits- und Zugriffsentscheidungen auf Basis von Identität, Gerät und Nutzerkontext für einen deutlich erweiterten Schutz. So können nur authentifizierte und autorisierte Mitarbeiter auf bestimmte Anwendungen und Daten zugreifen. Gleichzeitig werden Anwendungen und Nutzer besser vor Bedrohung aus dem Internet geschützt.

Warum lohnt sich die Einführung eines Zero-Trust-Modells?

Bei der von Akamai angebotenen Zero-Trust-Lösung werden Sichtbarkeit und Nutzung von Anwendungen nur genau dann gewährt, wenn es erforderlich ist. Dies bringt deutlich mehr Sicherheit mit sich. Der Mitarbeiter erhält so ausschließlich Zugang zu jenen Anwendungen, die er für seine aktuelle Aufgabe braucht. In einer Zeit täglich ansteigender Phishing- und Malware-Angriffen auf Unternehmen ist eine derartige Sicherheitslösung, insbesondere aufgrund des deutlich zunehmenden Anteils von Remote-Arbeit BYOD („bring your own device“), nicht mehr wegzudenken. Zero-Trust-Lösungen sorgen insbesondere in heterogenen und durch externe Zugriffe geprägten Umgebungen für einen wirksamen Schutz, auch indem zusätzlich Phishing- oder Malware-Seiten automatisch für User gesperrt werden, so dass Infektionen vermieden und laterale Ausbreitung von Schadsoftware verhindert werden kann.

Sollte Zero Trust der neue Standard werden?

Die Antwort ist eindeutig: ja. Für die Arbeit im Homeoffice sowie andere Remote-Varianten erfüllt das Zero-Trust-Modell alle Sicherheitsvoraussetzungen. Als neuer globaler Sicherheitsstandard kann der Ansatz Unternehmensdaten wirksam schützen und Cyber-Angriffe abwehren. ■

www.akamai.de

Illustration: flaticon.com

CYBERMOBBING,

DIE UNTERSCHÄTZTE GEFAHR IM UNTERNEHMEN

von Dipl. Math. Matthias Goebel und Dipl. Ing. Uwe Leest

In den letzten Jahren häufen sich die Angriffe auf Unternehmen durch Hacker. Mit dem Ziel Unternehmen zu erpressen, werden Daten gestohlen, Maschinen lahmgelegt und Datenbanken blockiert. Unternehmen investieren daher verstärkt in ihre Informationssicherheit, um frühzeitig Schaden abwenden zu können.

Wie sieht es dabei mit der Prävention, dem Schutz vor Angriffen auf eigene Mitarbeiter aus? Mit einer guten Unternehmenskultur und HR-Prozessen, die Mitarbeiter schützen und in Problemfällen Unterstützung und Rückhalt bieten, kann man Angriffe auf die eigenen Mitarbeiter vermeiden und Schäden mindern. Wir reden über Cybermobbing.

Aktuelle Studien zeigen, dass der deutschen Wirtschaft durch Produktionsausfallkosten im Krankheitsfall ein direkter Schaden von knapp 8 Mrd. Euro durch Mobbing/Cybermobbing entsteht.

Die indirekten Schäden, welche z.B. in Form von Humankapitalverlusten durch Versetzungen und verminderte Arbeitsleistung, Kompetenzverlust oder Frühverrentungen, durch Personalsuche und Einarbeitung neuer Mitarbeiter nach Kündigungen, Gerichtsverfahren, Entschädigungszahlungen, Reputationsverluste etc. entstehen, dürften aber um ein Vielfaches höher liegen.

Was ist Cybermobbing?

Unter Cybermobbing versteht man verschiedene Formen der Diffamierung, Beleidigung, Belästigung, Bedrängung, Bloßstellung oder Nötigung von Personen mit Hilfe elektronischer Kommunikationsmedien über das Internet wie z.B. Mails, Chatrooms, Videos, soziale Netzwerke, Instant Messaging etc. oder auch mittels Mobiltelefone, die sich über einen längeren Zeitraum erstrecken.

Hierbei spielt die Anonymität im Internet eine besondere Rolle. Sie enthemmt die Täterinnen und Täter, da häufig keine negativen Reaktionen oder Konsequenzen zu befürchten sind. Die strafrechtliche Verfolgung ist durch die Anonymität im Internet fast unmöglich. Das Opfer kann sich nicht wehren, da es häufig nicht weiß, von wem die Angriffe stammen. Es fühlt sich in besonderem Maße hilflos.

Aktuelle Situation in Deutschland

Der herrschende Trend zur Digitalisierung in fast allen Lebensbereichen, der durch die besonderen Umstände der Covid19-Pandemie noch beschleunigt wurde, begünstigt dabei das Auftreten von Cybermobbing. Wie der WDR kürzlich berichtete, hat die zentrale Anlaufstelle Cyberkriminalität der Staatsanwaltschaft in Nordrhein-Westfahlen gerade in diesem Jahr einen starken Anstieg

Foto: Adobe Stock

der Fälle von Cybercrime und Cybermobbing festgestellt.

Unsere aktuelle „Mobbingstudie“, durchgeführt unter 4.000 Personen in Deutschland, Österreich und der deutschsprechenden Schweiz zeigt: Oft wird Cybermobbing im Unternehmen unterschätzt, sowohl im Umfang als auch in den Auswirkungen.

In der gesamten Stichprobe geben 11,5% der Befragten in Deutschland an, Opfer von Cybermobbing zu sein, das sind 2,3 absolute Prozentpunkte mehr als 2018 und entspricht einer relativen Steigerung um 25,0%. Dabei hat sich die Zunahme von Cybermobbing seit 2018 im Vergleich zur Erststudie von 2014 sogar noch beschleunigt.

Frauen und jüngere Menschen sind besonders häufig von Cybermobbing betroffen. Der größte Anstieg der Prävalenzrate bei Cybermobbing im Vergleich zu 2018 ist in der Alterskohorte der 18 bis 24jährigen feststellbar.

Strukturen und Ursachen für Cybermobbing im Unternehmen

Das höchste Cybermobbingrisiko in Deutschland haben mit 16% Personen in Serviceberufen, das geringste in Büroberufen (8%). Die sozialen Berufe liegen hier mit 11% etwa im Mittelfeld. In Österreich haben Personen in Handel und Verkauf (17%) und in Serviceberufen (15%) das höchste, Befragte in Produktion und Handwerk (8%) und in den sozialen Berufen (9%) das geringste Risiko.

Häufig werden Lügen und Gerüchte verbreitet (39%) und die Opfer unter Druck gesetzt, erpresst oder bedroht (28%). 20% der Befragten gaben an, im Internet oder den sozialen Medien absichtlich ausgegrenzt worden zu sein und etwa 14% der Cybermobbingopfer mussten erleben, wie unangenehme oder peinliche Fotos oder Videofilme im Internet lanciert wurden. Diese Methode ist insofern besonders perfide, da Fotos oder Videos, die erst einmal im Internet eingestellt sind, fast unmöglich wieder von dort entfernt werden können. Von dieser Art des Cybermobbings sind Frauen (18%) stärker betroffen als Männer (10%).

Cybermobbing erfolgt in 72% der Fälle aus der gleichen Hierarchieebene, in 44% der Fälle aus einer übergeordneten Hierarchieebene und in 15% der Fälle aus einer tieferen Hierarchieebene. Dabei erfolgen 9% der Angriffe anonym.

Unerwünschtes Verhalten ist aus Sicht der Opfer die häufigste Ursache, danach folgen die Äußerung unerwünschter Kritik und das Vertreten der eigenen Werte und Überzeugungen.

Im Arbeitsumfeld werden vor allem ein konkurrenzorientiertes Umfeld und starre Hierarchien, aber auch die Wahrnehmung der eigenen Mehrleistung als Ursachen der Vorkommnisse identifiziert.

Beschäftigte, die während Covid19-Pandemie nicht im Homeoffice waren, sondern im Betrieb gearbeitet haben, sind deutlich stärker von Cybermobbing betroffen, wenn sie in ihrer Wahrnehmung mehr als ihre Kolleginnen und Kollegen leisten. Die Gruppendynamik spielt hier eine entscheidende Rolle.

Auswirkungen auf Unternehmen und Mitarbeiter

Durch Cybermobbing können den Unternehmen erheblich finanzielle Schäden entstehen. Aber auch die Kündigungsbereitschaft ist bei Opfern von Cybermobbing ca. 40% höher als bei Nichtbetroffenen. Und Opfer von Cybermobbing weisen jährlich fast doppelt so viele Krankheitstage auf wie nicht betroffene Beschäftigte.

Cybermobbing erhöht auch die Suchtgefahr signifikant: Zwischen ca. 15-20% der Opfer haben deswegen zu Alkohol, Medikamenten oder Drogen gegriffen. Oft

Dipl. Math. Matthias Goebel,
Referent, Bündnis gegen Cybermobbing e.V.

> Aktuelle Studien zeigen, dass der deutschen Wirtschaft ein direkter Schaden von knapp 8 Mrd. Euro durch Mobbing/ Cybermobbing entsteht.

erkennen Vorgesetzte nicht die wahren Ursachen für das Verhalten der Mitarbeiter.

Obwohl es in Deutschland (noch) kein Gesetz gegen Cybermobbing gibt, ergeben sich für Unternehmen eine Anzahl anderer, auch rechtlicher Risiken: Zum einen kann eine Fürsorgepflichtverletzung durch nicht erkanntes und geduldetes Mobbing vorgeworfen werden, was zu hohen Abfindungszahlungen führen kann. Des Weiteren sind Unternehmen bei unerkanntem oder geduldetem Cybermobbing dem Risiko verschiedener Straftatbestände ausgesetzt: Üble Nachrede, Verleumdung, Körperverletzung, Nötigung, Bedrohung, Verletzung des höchstpersönlichen Lebensbereiches durch unerlaubte Bildaufnahmen.

Auch darf der Imageschaden nicht unterschätzt werden, den Unternehmen haben können.

Dipl. Ing. Uwe Leest,
Vorstandsvorsitzender, Bündnis gegen Cybermobbing e.V.

Maßnahmen zur Eindämmung der Gefahren

Unternehmen und Führungskräfte sind nicht nur gesetzlich verpflichtet gegen Cybermobbing vorzugehen, sondern es ist auch anzuraten, entsprechende Maßnahmen einzuleiten, um Schaden vom Unternehmen fernzuhalten.

Leider haben Unternehmen die Cybermobbingproblematik bisher nicht ausreichend realisiert. In weniger als einem Drittel der Unternehmen sind Strukturen etabliert oder werden spezifische Maßnahmen ergriffen, um diesem Risiko wirkungsvoll und präventiv entgegenzuwirken.

Zu den ersten und wichtigsten Maßnahmen gehört zunächst zu akzeptieren, dass Cybermobbing in jedem Unternehmen vorkommen kann. Die Augen vor der Realität zu schließen ist keine Lösung und stoppt Cybermobbing nicht.

Als konkrete Maßnahmen zur Prävention, sowie zur Unterstützung von Führungskräften und Betroffenen haben sich folgende Maßnehmen bewährt:

- Ordnen Sie die Verantwortung für Cybermobbing im Unternehmen einer bestehenden (oder auch neuen) Organisation zu. Das kann z.B. die Personalabteilung oder die Sozialberatung sein. In diesem Verantwortungsbereich liegen dann alle Maßnahmen zur Prävention und Abwehr von Vorfällen.
- Schaffen Sie klare Leitlinien zum Umgang mit Konflikten ggfs. mit dem Betriebsrat.
- Weiterbildung und das Üben im Umgang mit Mobbingvorfällen ist ein kritischer Erfolgsfaktor in der Abwehr von Vorfällen und der Minderung von Auswirkungen. Insbesondere gilt es die Führungskräfte, Personalreferenten und Mitbestimmungsgremien entsprechend zu schulen.
- Sehr hilfreich sind Aufklärungsaktionen (Informationen und Schulungen) für Mitarbeiter.
- Insbesondere bei größeren Unternehmen sollten auch Mitarbeiter als Berater oder Coaches ausgebildet werden, gut dafür eignen sich z. B. die Vertrauensleute. In kleineren Unternehmen kann diese Leistung auch durch Externe erbracht werden.
- Ergänzen Sie bestehende Veranstaltungen mit dem Thema Cybermobbing oder führen Sie eigene Veranstaltungen zu diesem Thema durch.
- Nutzung von modernen KI basierten Tools zum Erkennen von Mobbing Inhalten in Messages etc. Solche Lösungen werden z.B. von Instagram und anderen Messaging Medien angeboten und können vom jeweiligen Nutzer aktiviert werden.

Die Digitalisierung unserer Gesellschaft wird weitergehen, unser Kommunikationsverhalten ist ein Teil des Problems, daher ist Prävention und Aufklärung ein wichtiger Baustein für jedes Unternehmen im Kampf gegen Cybermobbing.

Das Bündnis gegen Cybermobbing bietet ein umfassendes Servicepaket (CyMoS) für Unternehmen an. Von der Beratung über Schulungen für Mitarbeiter und Führungskräfte, bis hin zu einer Hotline, wenn es mal brennt!

Die aktuelle Studie zum Download finden Sie unter:
www.buendnis-gegen-cybermobbing.de/mobbingstudie2021

„PRIVACY – ACCELERATING DREAMS & INNOVATION!“

Porsche richtet Datenschutz strategisch für Geschäftserfolg und besseres Kundenerlebnis aus.

von Christian Völkel

Porsche erachtet die digitale Selbstbestimmung seiner Kunden als sehr wichtig für den Erfolg des Unternehmens im digitalen Zeitalter. Die gesamte Automobilbranche befindet sich mitten in einem tiefgreifenden Change Prozess auf der Datenautobahn. Dieser hat auch die bisherige Ausprägung des Datenschutzes im unternehmerischen Umfeld nicht unberührt gelassen. Um den neuen Ansprüchen gerecht zu werden, haben wir die strategische Ausrichtung des Datenschutzes mit Fokus auf Produkte und Kunden als eigenes Strategiefeld in der Unternehmensstrategie 2030 verankert. Die Eckpfeiler der neuen Porsche Datenschutzstrategie „Privacy – Accelerating Dreams & Innovation“ wurden kürzlich vom Vorstand verabschiedet, so dass die Strategie bei der künftigen Entwicklung von Produkten und Services berücksichtigt werden wird.

Warum gibt sich Porsche eine neue Datenschutzstrategie?

Das Selbstverständnis der Marke Porsche ist von einem hohen Maß an Freiheit und Souveränität in Bezug auf das Produkt Porsche geprägt: ‚The car that nobody needs but everybody wants‘. Diesen Anspruch an unsere Produkte gilt es, in das digitale Zeitalter zu überführen. Unsere Kunden messen ihre Freiheit und Souveränität künftig nicht nur an der Exklusivität unserer Fahrzeuge, der Beschleunigung und dem Abtrieb bei Kurvenfahrten. Sondern auch daran, wie groß ihre Selbstbestimmung bei der Nutzung unserer digitalen Produkte und Verwendung der Kundendaten ist. Die Wahrung der digitalen Selbstbestimmung unserer Kunden ist wichtig für den Erfolg des Unternehmens im digitalen Zeitalter. Ziel ist es, das hohe Vertrauen in die Marke auch in der digitalen Welt zu erhalten.

Christian Völkel,
Chief Privacy Officer, Porsche AG

> Digitale Sicherheit und Privatsphäre können durchaus als USP begriffen werden.

Datenschutz hatte bei Porsche bereits in der Vergangenheit stets einen hohen Stellenwert. Der Grad des Datenschutzes in den Produkten und Services hing aber immer stark von individuellen Produktentscheidungen ab. Einerseits haben wir Produkte und Dienstleistungen mit einem sehr hohen Datenschutzniveau auf den Markt gebracht. Andererseits wurden auch Initiativen gestartet, die – in voller Übereinstimmung mit den gesetzlichen Anforderungen – den Datenschutz erfüllten, ihn aber hinsichtlich des Kundeninteresses eher im Hintergrund haben wirken lassen. Das soll sich jetzt ändern und über die Einhaltung von Compliance-Standards hinausgehen. Digitale Sicherheit und Privatsphäre können durchaus als USP begriffen werden: Schaut man auf den einen oder anderen Tech-Giganten, wird man feststellen, dass „Privacy“ dort sogar strategisch zur Prime-Time platziert wird.

Strategische Vision und Mission

Wesentlicher Bestandteil unserer Datenschutzstrategie ist die Definition der Vision und Mission: Das Vertrauen in die Marke Porsche soll sich in Zukunft nicht nur durch die Qualität der Produkte und Services auszeichnen, sondern auch durch das gute Gefühl der Kunden, selbstbestimmt mit ihren Daten umgehen zu können. Die Marke Porsche ist Ausdruck von Freiheit: „The brand for those who follow their dreams“ – diese Freiheit soll auch in digitalen Geschäftsmodellen zum Ausdruck kommen.

Diesem Anspruch wollen wir auch beim Datenschutz gerecht werden: „Mit Privacy made by Porsche wollen wir Träume und Innovationen durch datengetriebene Geschäftsmodelle und ein hohes Maß an Datenverfügbarkeit beschleunigen. Unsere Vision ist ‚Privacy – Accelerating Dreams & Innovation“, sagt Lutz Meschke, stell-

Fotos: Dr. Ing. h.c. F. Porsche Aktiengesellschaft (2)

vertretender Vorstandsvorsitzender der Porsche AG und Vorstand für Finanzen und IT.

Die Datenschutzstrategie soll uns in den Kernmärkten befähigen, gemeinsam Innovationen zu ermöglichen und die Träume unserer Kunden wahr werden zu lassen – in globaler Ausprägung bei Berücksichtigung von lokalen Anforderungen. Darüber hinaus ist es die Aufgabe der Porsche Privacy Strategy, datengetriebene Innovation, den ethischen Umgang mit Daten und die Einhaltung gesetzlicher Vorgaben zu verbinden. Dabei stehen die Kunden im Mittelpunkt.

Ableitung der strategischen Dimensionen für den Datenschutz

Datenschutz ist komplex, Datenschutz ist nicht eindimensional. Daher haben wir die Datenschutzstrategie multidimensional definiert und in vier Perspektiven gegliedert. Die erste Perspektive entspricht den Querschnittsfunktionen der Porsche Unternehmensstrategie 2030. Die zweite Perspektive wird durch die Unternehmenswerte definiert. Die dritte Perspektive besteht aus den bekannten Datenschutzgrundsätzen, die auf den OECD Fair Information Principles und den klassischen Datenschutz-Schutzzielen basieren. Die vierte Perspektive deckt die Datenschutzorganisation selbst ab.

Eine fundierte Datenschutzstrategie ermöglicht es, den Anforderungen von Kunden und Märkten gerecht zu werden und die Aktivitäten auf der Datenautobahn gezielt und harmonisiert zu beschleunigen. Wir sehen Datenschutz als Weg, um Digitalisierungsinitiativen zu beschleunigen.

Wie setzen wir die Datenschutzstrategie in die Praxis um?

„Porsche drives dreams!“ – Das Unternehmen wird das Privacy User Interface in seinen Autos von Generation zu Generation verbessern. Der erste vollelektrische Sportwagen Taycan war ein großer Sprung hinsichtlich des Privacy Interfaces. Das wird sich in den künftigen Modellen fortsetzen. Der Kunde erhält mit einfacher Bedienweise zu den Privacy Einstellungen volle Transparenz und Kontrolle über die Datenverarbeitung im Fahrzeug. „The customer in the driver‘s seat“!

„Porsche drives innovation!“ – Wir streben an, die Datenverfügbarkeit in verschiedenen datenrelevanten Anwendungsbereichen wie Verkehrssicherheit oder digitalen Diensten zu erhöhen. Die Datenschutzstrategie unterstützt den Ausgleich zwischen lokaler und zentraler Datenspeicherung. Die Vorteile der Digitalisierung werden erforscht und Privacy by Design als ein zentraler Innovationstreiber für mehr Kundensouveränität gesehen.

Am Ende des Tages steht bei uns der Mensch im Mittelpunkt. Deshalb bezieht das Unternehmen in seine strategischen Ziele nicht nur seine Kunden und Mitarbeiter, sondern alle Beteiligten mit ein. Die digitale Transformation mit Datenschutzgedanken wird die Organisation prägen. Es ist Porsche wichtig, dass die Ziele nicht nur kommuniziert, sondern auch erlebt und verinnerlicht werden.

Fazit

Der selbstbestimmte Umgang mit Ihren Daten spielt für unsere vielfältigen Kundengruppen bereits heute eine große Rolle, die weiter zunehmen wird. Porsche glaubt an die Zukunftsfähigkeit des Datenschutzes auch als Wettbewerbsvorteil und wird Datenschutz mutig und mit Pioniergeist an seine Kunden kommunizieren. ■

Advertorial

Das Zero-Trust-Konzept muss über die klassische IT-Sicherheit hinausgehen

Vertrauen ist nicht gut, Kontrolle ist besser

von Michael Pietsch

Cyberkriminelle haben durch den Einsatz von Ransomware in den vergangenen Monaten eine traurige Erfolgsgeschichte geschrieben. Die verdeutlicht zwei Dinge. Erstens hat sich Cyberkriminalität immer mehr zum Geschäft entwickelt, und zweitens wird deutlich, dass es Angreifern gelingt, traditionelle IT-Sicherheitsmaßnahmen zu überwinden.

Und nun?

Wenn herkömmliche Sicherheitsprodukte versagen, werden IT- und Sicherheitsteams oft sich selbst überlassen. Ein Zero-Trust-Ansatz ist die Antwort. Das National Institute of Standards (NIST) beschreibt Zero Trust als „eine sich entwickelnde Reihe von Cybersicherheitsparadigmen, welche die Abwehr von statischen, netzwerkbasierten Perimetern auf Benutzer, Assets und Ressourcen konzentrieren“.

Während Zero Trust traditionell als Netzwerksicherheitsmodell verwendet wurde, gelten die Prinzipien auch für die Datensicherheit und Sicherheitsarchitektur im Allgemeinen: Vertraue niemandem und gewähre die geringsten Privilegien, damit die Identität eines Benutzers nur noch für die ihm zugewiesene Rolle Zugriff erhält. Es ist das Gegenteil des vorherrschenden „Vertrauens, aber Verifizieren“-Modells. So weit, so gut.

Wichtig ist die Implementierung von Zero Trust nicht nur, um Eindringlinge im Netzwerk zu bremsen, sondern auch um das Backup zu schützen, das sowohl ein beliebtes Opfer der Angreifer als auch eine Lebensversicherung für die Betroffenen ist.

Zero Trust Data Security – Unveränderliche Backups und moderne Data Security

Moderne Lösungen für Data Security und Datenmanagement nutzen konsequent das Zero-Trust-Konzept, um Angreifer auch dann nirgendwo hingehen zu lassen, wenn es ihnen gelungen ist, in das Netzwerk einzudringen. Unternehmen können mit bewährten Sicherheitspraktiken und regelmäßigen Sicherheitsüberprüfungen mit Schwerpunkt auf Datenintegrität, Benutzerzugriffskontrollen, Datenverschlüsselung, Anwendungszugriff und API-Sicherheit ein Höchstmaß an Datenschutz gewährleisten, um ihre Datensicherheit zu verbessern.

Bei älteren Backup-Systemen kann auf Backups über das Netzwerk zugegriffen werden; Dadurch werden Daten verändert und gelöscht. In einer auf Zero Trust basierenden Backup-Architektur ist jedoch keine Online- oder Netzwerkspeicherung möglich. Die Backups können nicht manipuliert werden. Um zu verhindern, dass Zugangsdaten kompromittiert werden, kommen Multi-Faktor-Authentifizierung, TOTP, zertifikatbasierte Authentifizierung und TLS 1.2 zum Einsatz. Dies bedeutet, dass Unternehmen in der Lage sind, Daten nach einem Angriff wiederherzustellen.

Michael Pietsch,
GM Country Manager Germany, Rubrik

> Wichtig ist die Implementierung von Zero Trust nicht nur, um Eindringlinge im Netzwerk zu bremsen, sondern auch um das Backup zu schützen.

Die Sicherheitsprozesse sind maximal automatisiert. Die Verschlüsselung von Backups erforderte bisher einen aufwändigen manuellen Prozess. Heute können Unternehmen diese Prozesse automatisieren, um eine effektive Datensicherheit, aber auch ein effizientes Datenhandling zu gewährleisten. Ziel ist es, den reibungslosen Geschäftsbetrieb zu schützen – und nicht zu bremsen. ■

www.rubrik.com

Künstliche Intelligenz –

WAS BRINGT DIE GEPLANTE EU-VERORDNUNG UND WIE KÖNNEN SICH UNTERNEHMEN DARAUF VORBEREITEN?

von Dr. Anna Zeiter

Künstliche Intelligenz (KI) bietet ein riesiges Potenzial in verschiedenen Lebensbereichen, wie Gesundheit, Energie, Verkehr, Landwirtschaft, Reisen, Bildung, Verwaltung, Strafverfolgung und Cybersicherheit. Sie birgt aber auch eine Reihe von gesellschaftlichen Risiken. Die EU-Kommission hat vor diesem Hintergrund im April 2021 einen Verordnungsvorschlag veröffentlicht, mit welchem der Einsatz von KI in der EU einheitlich geregelt werden soll (https://ec.europa.eu/germany/news/20210421-kuenstliche-intelligenz-eu_de). Dieser Verordnungsvorschlag ist eines der ersten Gesetzgebungspakete weltweit, welches sich der Regulierung von KI widmet. Die EU will damit insbesondere auf die Risiken reagieren, die bestimmte KI-Systeme mit sich bringen. Dabei verfolgt die Kommission in erster Linie einen risikobasierten Ansatz, der auf eine mehrstufige Einteilung von KI-Systemen setzt. Während gewisse KI-Anwendungen ganz verboten werden sollen, bestehen für andere weniger riskante KI-Systeme unterschiedlich strenge Pflichten. Bei Verstößen gegen die geplante Verordnung sollen erhebliche Geldbußen drohen. Der Verordnungsvorschlag befindet sich aktuell im ordentlichen Gesetzgebungsverfahren in Brüssel – ein In-Kraft-Treten wird jedoch nicht vor 2023 erwartet. Sollte die Verordnung angenommen werden, hätte sie spürbare Auswirkungen auf Unternehmen innerhalb und außerhalb der EU.

Was ist der Regelungszweck der neuen Verordnung?

Ziel der EU-Kommission ist es, mit dem Verordnungsentwurf auf der einen Seite das gesellschaftliche Vertrauen in KI zu stärken und KI-spezifische Risiken zu

limitieren sowie auf der anderen Seite Europa als globales Zentrum für vertrauenswürdige KI zu stärken bzw. unternehmerische Tätigkeiten im Bereich KI nicht über Gebühr einzuschränken. Der Verordnungsentwurf ist damit eine Gratwanderung zwischen Grundrechtsschutz und Innovationsförderung.

Für wen sollen die Regelungen gelten?
Der geplante geografische Anwendungsbereich der EU-Verordnung ist weit und hat – genau wie auch bereits die DSGVO – extraterritorialen Effekt. Die Regelungen des Verordnungsentwurfes sollen nicht nur für öffentliche und private Akteure innerhalb der EU gelten, sondern auch für außerhalb der EU ansässige Unternehmen, sofern ein KI-System in der EU in Verkehr gebracht wird oder Menschen in der EU von seiner Verwendung betroffen sind.

Was ist ein KI-System?
Neben dem territorialen Anwendungsbereich ist auch der inhaltliche Anwendungsbereich der geplanten Verordnung relativ umfassend. Ein KI-System liegt bereits dann vor, wenn Software mit einer der folgenden Techniken entwickelt wurde: maschinelles Lernen, logik- und wissensbasierte Verfahren oder statistische Verfahren.

Welche Risiko-Einstufungen gibt es?
Die EU-Kommission verfolgt bei dem vorliegenden Verordnungsentwurf einen risikobasierten Ansatz, der auf eine vierstufige Einteilung von KI-Systemen setzt:

Unannehmbares Risiko: Hierunter fällt eine geringe Zahl besonders schädlicher KI-Anwendungen, die als Bedrohung für die Sicherheit, die Lebensgrundlagen und die Rechte der Menschen gilt. Solche KI-Systeme sollen demnach komplett verboten werden. Hierzu gehören beispielsweise Anwendungen, die menschliches Verhalten manipulieren, um den freien Willen der Nutzer zu umgehen (z.B. Spielzeug mit Sprachassistent, das Minderjährige zu gefährlichem Verhalten ermuntert), biometrische Echtzeit-Fernidentifizierungssysteme, die zu Strafverfolgungszwecken im öffentlichen Raum eingesetzt werden sowie Systeme, die den Behörden eine Bewertung des sozialen Verhaltens (Social Scoring) ermöglichen.

Hohes Risiko: Hierunter versteht man eine begrenzte Zahl von KI-Systemen, die sich nachteilig auf die Sicherheit der Menschen oder deren Grundrechte auswirken. Hierzu gehört z.B. autonomes Fahren, der Einsatz von Drohnen, roboterassistierte Medizintechnik, Software zur Auswertung von Lebensläufen, automatisierte Überprüfung von Reisedokumenten sowie die maschinelle Bewertung der Kreditwürdigkeit. Für diese KI-Systeme gelten verbindliche Anforderungen, wie beispielsweise an die Qualität der verwendeten Datensätze, die technische Dokumentation, Transparenz für die Nutzer, menschliche Aufsicht und Cybersicherheit.

Geringes Risiko: Zu solchen Anwendungen gehören KI-Systeme, von denen eine gewisse Manipulationsgefahr ausgeht, wie z.B. von Chatbots oder Deep Fakes. Solchen KI-Anwendungen werden besondere Transparenzverpflichtungen auferlegt. Beim Umgang mit KI-Systemen wie Chatbots sollte den Nutzern z.B. bewusst sein, dass sie es mit einer Maschine zu tun haben, damit sie in voller Kenntnis der Sachlage entscheiden können, ob sie die Anwendung weiter nutzen wollen oder nicht.

Minimales Risiko: Alle anderen KI-Systeme – dies soll nach Intention der EU-Kommission die große Mehrzahl der Anwendungen sein, wie z.B. KI-gestützte Videospiele oder Spam-Filter – sollen weiterhin unter Einhaltung des allgemein geltenden Rechts entwickelt und verwendet werden können. Hierzu gehören beispielsweise die datenschutzrechtlichen Vorschriften der DSGVO. Zu den datenschutzrechtlichen Anforderungen an KI-Anwendungen hat die Datenschutzkonferenz (das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder) bereits im April 2019 ein detailliertes Papier herausgegeben (https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf).

Dr. Anna Zeiter,
Chief Privacy Officer, eBay Inc.

> Der Verordnungsentwurf ist eine Gratwanderung zwischen Grundrechtsschutz und Innovationsförderung.

Wer setzt die geplante Verordnung durch?
Von der EU-Kommission geplant ist eine dezentrale Durchsetzung der neuen KI-Verordnung. Jeder Mitgliedstaat soll dafür mindestens eine nationale Behörde benennen, welche die Anwendung und Umsetzung der Vorschriften beaufsichtigt und die Marktüberwachung wahrnimmt. Eine nationale Aufsichtsbehörde wird den Mitgliedsstaat zudem im Europäischen Ausschuss für künstliche Intelligenz vertreten. Dieser setzt sich aus Vertretern der zuständigen nationalen Aufsichtsbehörden, dem Europäischen Datenschutzbeauftragten und der EU-Kommission zusammen. Unklar ist aktuell noch, welche nationalen Behörden die geplante KI-Verordnung konkret durchsetzen sollen. In Frage kommen die zuständigen Datenschutzbehörden, die Wettbewerbs- bzw. Verbraucherschutzbehörden oder auch eigens für den Bereich KI neugegründete Aufsichtsorgane. Die Tatsache, dass der Europäische Datenschutzbeauftragte bereits im Europäischen Ausschuss für künstliche Intelligenz vertreten sein wird, legt nahe, dass die KI-Aufsichtsfunktion den nationalen bzw. in Deutschland den Landesdatenschutzbehörden zukommen wird. Dies würde sogar einige Synergien mit sich bringen, da die Datenschutzbehörden bereits jetzt – unter der DSGVO – Datenverarbeitungsprozesse und diesbezügliche Risikobewertungen beaufsichtigen.

Welche Sanktionen sind bei Verstößen vorgesehen?
Bei Verstößen gegen die neuen Regelungen sieht der aktuelle Verordnungsentwurf erhebliche Bußgelder vor: von bis zu EUR 30 Mio. bzw. 6 % des weltweiten Jahresumsatzes eines Unternehmens. Für global agierende Firmen kann dies bedeuten, dass die Jahresumsätze des weltweiten Konzerns herangezogen werden, und nicht nur die Jahresumsätze der Europäischen Tochter. Die in der Verordnung aktuell vorgesehenen Geldbußen sind damit insgesamt um 50% höher als die bereits im Mai 2018 von der DSGVO eingeführten signifikanten Sanktionen. Dies sollten CEOs, CFOs und COOs bei der Entwicklung und Einführung von KI-Systemen ihres Unternehmens in der EU im Auge behalten.

Wie geht es im Gesetzgebungsverfahren weiter?
Als nächstes wird der Kommissionsentwurf der KI-Verordnung durch das Europäische Parlament und den Europäischen Rat gehen. Es ist zu erwarten, dass der Entwurf dabei noch erhebliche Änderungen erfahren wird. Erfahrungsgemäß dauert es 18 Monate bis zu zwei Jahren, bis eine Verordnung ratifiziert wird und in sämtlichen EU-Mitgliedsstaaten unmittelbar in Kraft tritt – das wäre Anfang 2023.

Was können Unternehmen bereits jetzt tun?
Die verbleibende Zeit bis Anfang 2023 können Unternehmen sinnvoll nutzen, um sich auf die geplante Verordnung vorzubereiten. Als erstes sollten Unternehmen dafür eine umfassende Übersicht von sämtlichen bereits existierenden Anwendungen erstellen, die unter den weiten KI-Begriff fallen. Als nächster Schritt ist es zu empfehlen, die identifizierten KI-Systeme grob in die oben skizzierten Risikostufen einzuteilen und Anwendungen mit unannehmbarem Risiko unmittelbar zu unterbinden und solche mit hohem Risiko genauer zu beleuchten und bereits jetzt zusätzliche Schutzmaßnahmen einzuführen. Daneben sollte schon jetzt im Unternehmen ein Gremium eingerichtet werden, das in Zukunft KI-Anwendungen nach Risikolevel bewertet und jeweilige Schutzmaßnahmen festlegt. Zu den Mitgliedern eines solchen KI-Gremiums sollten die verantwortlichen ProduktentwicklerInnen aus dem KI-Bereich, MitarbeiterInnen aus der Rechtsabteilung, der Abteilung für Ethics und Compliance sowie der oder die Datenschutzbeauftragte gehören.

Fazit
Die geplante EU-Verordnung zu KI wird – in vorliegender oder auch in abgeänderter Form –spürbare Auswirkungen auf Unternehmen haben, die innerhalb der EU KI-Anwendungen in Verkehr bringen. Aus diesem Grund sollten Unternehmen bereits jetzt damit beginnen, sich auf die kommenden Vorschriften vorzubereiten und interne Verzeichnisse, Prozesse und Entscheidungsgremien einführen. ■

Fotos: Getty

Handelsblatt Jahrestagung

24. bis 26. Januar 2022, Sofitel Munich Bayerpost | **HYBRID EDITION**

Strategisches IT-Management 2022

Digital Transformation: The Race Goes On

Jan Brecht
CIO, Daimler AG

Francesco Bonfiglio
CEO, GAIA-X, European Association for Data and Cloud

Hanna Hennig
CIO, Siemens AG

Dr. Bettina Uhlich
CIO, Evonik Industries AG

Limitierte Anzahl Vor-Ort-Tickets
Jetzt anmelden

Handelsblatt

Substanz entscheidet.