Redaktion: Helmut Reimer

Report

EU-Kommission schlägt Maßnahmen für eine faire und innovative Datenwirtschaft vor

Am 23. Februar 2022 legte die Kommission einen Vorschlag für neue Vorschriften darüber vor, wer die in den Wirtschaftssektoren in der EU erzeugten Daten nutzen darf und Zugriff darauf hat. Das Datengesetz wird für Fairness im digitalen Umfeld sorgen, einen wettbewerbsfähigen Datenmarkt fördern, Chancen für datengesteuerte Innovationen eröffnen und Daten für alle zugänglicher machen. Es wird zu neuen innovativen Diensten und zu Wettbewerbspreisen für anschließende Dienste und Reparaturen vernetzter Objekte führen. Dieser letzte horizontale Baustein der Datenstrategie der Kommission wird eine Schlüsselrolle beim digitalen Wandel und der Verwirklichung der digitalen Ziele für 2030 spielen.

Margrethe Vestager, die für das Ressort „Ein Europa für das digitale Zeitalter" zuständige ExekutivVizepräsidentin, erklärte: „Wir wollen Verbrauchern und Unternehmen noch mehr Mitspracherecht darüber einräumen, was mit ihren Daten geschehen darf, indem klargestellt wird, wer zu welchen Bedingungen Zugang zu den Daten hat. Dies ist ein zentraler Digitalgrundsatz, der zur Schaffung einer robusten und fairen datengesteuerten Wirtschaft beitragen und Leitsatz für den digitalen Wandel bis 2030 sein wird."

Der für den Binnenmarkt zuständige Kommissar Thierry Breton fügte hinzu: „Heute machen wir einen wichtigen Schritt auf dem Weg zur Erschließung einer Vielfalt an Industriedaten in Europa zum Wohle von Unternehmen, Verbrauchern, Behörden und der Gesellschaft insgesamt. Bisher wird nur ein geringer Teil der Industriedaten genutzt, und das Wachstums- und Innovationspotenzial ist enorm. Das Datengesetz gewährleistet, dass Industriedaten unter voller Einhaltung der europäischen Vorschriften weitergegeben, gespeichert und verarbeitet werden. Das Gesetz ist ein Eckpfeiler einer starken, innovativen und souveränen europäischen Digitalwirtschaft."

Daten zeichnen sich ebenso wie Musikaufnahmen, Straßenbeleuchtung oder eine malerische Aussicht durch Nicht-Rivalität aus, was bedeutet, dass viele Menschen gleichzeitig Zugang dazu haben und sie immer wieder „konsumiert" werden können, ohne dass ihre Qualität darunter leidet oder sie zur Neige gehen. Die Datenmenge nimmt kontinuierlich zu: 2018 wurden 33 Zettabyte erzeugt und 2025 werden es voraussichtlich schon 175 Zettabyte sein. Ihr Potenzial wird nicht ausgeschöpft, denn 80 % der Industriedaten werden nie genutzt. Das Datengesetz geht die rechtlichen, wirtschaftlichen und technischen Hindernisse an, die der Datennutzung im Wege stehen. Mit den neuen Vorschriften stehen mehr Daten zur Weiterverwendung zur Verfügung und das BIP dürfte bis 2028 voraussichtlich um zusätzliche 270 Mrd. Euro gesteigert werden.

Der Vorschlag für das Datengesetz beinhaltet Maßnahmen, damit Nutzer Zugang zu den von ihren vernetzten Geräten erzeugten Daten haben, die häufig ausschließlich von Herstellern gesammelt werden, und diese Daten an Dritte weitergeben können, die anschließende Dienste oder andere datengesteuerte innovative Dienste anbieten. Es bietet nach wie vor Anreize für Hersteller, in eine hochwertige Datenerzeugung zu investieren, weil es ihnen ermöglicht, die durch die Datenweitergabe entstehenden Kosten zu decken, und gleichzeitig ausschließt, dass die von ihnen bereitgestellten Daten verwendet werden, um damit in direkten Wettbewerb zu ihrem Produkt zu treten.

Maßnahmen zur Wiederherstellung einer ausgewogenen Verhandlungsmacht für KMU durch Verhinderung von Ungleichgewichten in Verträgen über die gemeinsame Datennutzung. Das Datengesetz schützt KMU vor missbräuchlichen Vertragsklauseln, die von einer Vertragspartei mit einer deutlich stärkeren Verhandlungsposition vorgegeben werden. Die Kommission wird auch Mustervertragsbedingungen entwickeln, um KMU dabei zu helfen, faire Verträge über die gemeinsame Datennutzung abzufassen und auszuhandeln.

Mittel für Behörden für den Zugang zu und die Nutzung von Daten im Besitz des Privatsektors, die unter besonderen Umständen und vor allem bei öffentlichen Notständen wie Überschwemmungen und Waldbränden benötigt werden oder aber zur Wahrnehmung eines rechtlichen Mandats, sofern Daten nicht anderweitig verfügbar sind. Der Datenzugang ist erforderlich, damit rasch und sicher reagiert werden kann und Unternehmen dabei möglichst wenig belastet werden.

Neue Vorschriften, damit Kunden effektiv wechseln können zwischen Anbietern von CloudDatenverarbeitungsdiensten, und führt Schutzmaßnahmen gegen unrechtmäßige Datenübermittlungen ein.

Zudem werden im Datengesetz bestimmte Aspekte der 1990 erlassenen Datenbankrichtlinie überarbeitet, um Investitionen in die strukturierte Darstellung von Daten zu schützen. So wird präzisiert, dass Datenbanken, die Daten von Geräten und Objekten des Internets der Dinge enthalten, keinem gesonderten Rechtsschutz unterliegen sollten. Dies garantiert, dass sie zugänglich sind und genutzt werden können.

Verbraucher und Unternehmen haben Zugang zu den von ihren Geräten erzeugten Daten und können sie für anschließende Dienste und Dienste mit Zusatznutzen wie vorausschauende Wartung verwenden. Dank zusätzlicher Informationen können Verbraucher und Nutzer wie landwirtschaftliche Betriebe, Fluggesellschaften und Bauunternehmen bessere Entscheidungen treffen und z. B. hochwertigere oder nachhaltigere Produkte und Dienste erwerben und damit zu den Zielen des Grünen Deals beitragen.

Unternehmen und Industrieakteure haben Zugang zu mehr Daten und profitieren von einem Wettbewerbsmarkt für Daten. Anbieter von anschließenden Diensten können ihre Dienste besser auf den jeweiligen Bedarf ihrer Kunden zuschneiden und so mit Herstellern konkurrieren, die vergleichbare Dienste anbieten. Außerdem können Daten zusammengeführt werden, um vollkommen neue digitale Dienste zu entwickeln.

Zur Unterstützung der europäischen Datenstrategie hat die Kommission heute auch einen Überblick über die gemeinsamen europäischen Datenräume vorgelegt, die gegenwärtig in verschiedenen Sektoren und Bereichen entwickelt werden.

Hintergrund

Das Datengesetz ist nach dem Daten-Governance-Gesetz die zweite große Gesetzgebungsinitiative, die als Folgemaßnahme zur europäischen Datenstrategie vom Februar 2020 ergriffen wird, um die EU an die Spitze der datengesteuerten Wirtschaft zu bringen.

Zusammen werden diese Initiativen das wirtschaftliche und gesellschaftliche Potenzial von Daten und Technologien im Einklang mit den Vorschriften und Werten der EU freisetzen. Sie werden einen Binnenmarkt schaffen, der einen ungehinderten Datenfluss in der EU und zwischen den Wirtschaftszweigen ermöglicht – zum Wohle von Unternehmen, Forschenden, Behörden und der Gesellschaft insgesamt.

Mit dem im November 2020 vorgelegten Daten-Governance-Gesetz, über das Rat und Europäisches Parlament im November 2021 Einigung erzielt haben, werden Verfahren und Strukturen geschaffen, die die gemeinsame Datennutzung von Unternehmen, Einzelpersonen und der öffentlichen Hand vereinfachen. Mit dem Datengesetz wird hingegen klargestellt, wer unter welchen Bedingungen aus Daten Wert schöpfen kann.

Im Rahmen einer öffentlichen Konsultation vom 3. Juni bis zum 3. September 2021 wurden Stellungnahmen zu den Maßnahmen für eine faire gemeinsame Datennutzung zugunsten von Verbrauchern und Unternehmen eingeholt. Die Ergebnisse wurden am 6. Dezember 2021 veröffentlicht.

IT-Planungsratssitzung in Saarbrücken

Am 9. März 2022 tagte der IT-Planungsrat (IT-PLR) in Saarbrücken. Die Mitglieder beschlossen weitere Schritte für die Verwaltungsdigitalisierung über 2022 hinaus und reagierten auf den völkerrechtswidrigen Angriffskrieg der Russischen Föderation auf die Ukraine.

Als zentrales Steuerungsgremium zur Digitalisierung der Verwaltung stimmt sich der IT-Planungsrat in seinen regelmäßigen Sitzungen über organisatorische, rechtliche und finanziellen Fragestellungen zur Verwaltungsdigitalisierung ab. Am 9. März tagte das Gremium unter der Leitung des diesjährigen Vorsitzenden Dr. Markus Richter, Staatssekretär im Bundesministerium des Innern und für Heimat (BMI) und Bundes-CIO in Saarbrücken.

Angesichts des Kriegs in der Ukraine waren sich alle Mitglieder einig, in ihrer Sitzung nicht einfach zur Tagesordnung überzugehen. Der IT-Planungsrat ordnete daher seine Aktivitäten in den Kontext ein. Die Mitglieder verständigten sich darauf, die für die Unterstützung der betroffenen Menschen relevanten Anstrengungen zur Digitalisierung der Verwaltung zu priorisieren und zu intensivieren.

Weitere Beschlüsse für die Verwaltungsdigitalisierung über 2022 hinaus

Das Jahr 2022 läutet den Endspurt der laufenden Umsetzung des Onlinezugangsgesetzes (OZG) ein: Bis Ende 2022 sollen alle Verwaltungsdienstleistungen auch online angeboten werden. Bund, Länder und Kommunen arbeiten daher weiterhin daran, verwaltungsinterne Arbeitsabläufe und digitale Serviceleistungen für Bürger:innen und Unternehmen einfach und nutzerfreundlich zu gestalten. Auch wenn schon viel geschafft wurde, gibt es noch viel zu tun; insbesondere was die nachhaltige Weiterentwicklung der Verwaltungsdigitalisierung über die Umsetzungsfrist des OZG hinaus betrifft.

Dr. Annette Schmidt, Präsidentin der FITKO (Föderale IT-Kooperation) kommentiert: „Die Verwaltungsdigitalisierung endet nicht mit der Umsetzungsfrist des Onlinezugangsgesetzes (OZG). Dies zeigen auch die heutigen Beschlüsse des IT-Planungsrats, bei deren Umsetzung die FITKO umfassend unterstützt."

Dr. Markus Richter, Staatssekretär im Bundesministerium des Innern und für Heimat und Bundes-CIO

„Mit vereinten Kräften müssen wir alles daransetzen, die OZG-Umsetzung voranzubringen. Durch die heutigen Beschlüsse gehen wir weiter in die richtige Richtung. Wir sprechen uns zum Beispiel für ein zentrales Bürgerpostfach aus. Die Länder können nachnutzen. So steigern wir die Interoperabilität der Nutzerkonten."

Modernisierung der Register schreitet voran

Bürgerinnen und Bürger sowie und Unternehmen sollen künftig digitale Verwaltungsleistungen nutzerfreundlich nach dem Once-Only-Prinzip in Anspruch nehmen können. Bürger:innen oder Unternehmen sollen damit Informationen, die einmal bei der Verwaltung hinterlegt sind, nicht erneut als Nachweis einbringen müssen. Hierfür ist eine verknüpfte Registerlandschaft notwendig Der IT-Planungsrat hat in seiner heutigen Sitzung die Programmplanung der Gesamtsteuerung Registermodernisierung samt Meilensteinen bis 2025 beschlossen. Diese sieht u.a. vor, dass die notwendigen technischen Komponenten für eine verknüpfte Registerlandschaft bis 2024 umgesetzt sind und der laufende Betrieb mit Anschluss priorisierter Register bis 2025 realisiert wird.

Fortschritte auch beim Organisationskonto

Des Weiteren hat der IT Planungsrat die Weichen für den Betrieb des einheitlichen Organisationskontos gestellt. Es soll Firmen bundesweit ermöglichen, sich mithilfe ihrer Elster-Zertifikate bei Online-Diensten anzumelden, Anträge authentifiziert auszufüllen und abzusenden sowie Bescheide über ein zentrales Postfach zu empfangen. Pilotpartner, die im vergangenen Jahr schon am Organisationskonto angebunden wurden, sind Bremen, Nordrhein-Westfalen, Bayern, Hamburg und der Bund; weitere Länder sollen zeitnah folgen. Meilensteine für 2022 sind die Bereitstellung der Postfächer, die eine Kommunikation zwischen Behörden und Unternehmen ermöglichen, sowie der Autorisierungstechnologie. In seinen Beratungen stimmte der IT-Planungsrat einer Übernahme des einheitlichen Organisationskontos in sein Produktportfolio zu. Das Produktmanagement soll ab 01.01.2023 von der FITKO übernommen werden.

Gemeinsam abgestimmtes Vorgehen beim Thema Cybersicherheit

Außerdem befasste sich das Gremium auch mit dem Thema Cybersicherheit. In den vergangenen Monaten hat die Länderarbeitsgruppe Cybersicherheit der IMK (LAG CS) eine „Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien" erarbeitet, die dem IT-PLR in der heutigen Sitzung vorgelegt wurden. Die Mitglieder begrüßten eine länderübergreifende und gemeinsam abgestimmte Leitlinie und betonten erneut die hohe Bedeutung einer gesamtstaatlichen Cybersicherheitsarchitektur.

Bitkom: Mustervertrag zur Beschaffung von Cloudleistungen

Nach intensiven Verhandlungen mit der IT-Wirtschaft, vertreten durch den Bundesverband Informationswirtschaft, Telekommu-

nikation und neue Medien e.V. (Bitkom), hat die öffentliche Hand sich mit dem Bitkom auf vertragliche Regelungen zur Beschaffung von Cloudleistungen geeinigt und am 01. März 2022 veröffentlicht. Die von Bitkom vertretene IT-Wirtschaft kündigte an, diese Regelungen zukünftig bei öffentlichen Beschaffungen grundsätzlich zu akzeptieren.

Mit den ergänzenden Vertragsbedingungen für die Beschaffung von Cloudleistungen (EVB-IT Cloud) können die hohen Anforderungen der öffentlichen Hand an Leistungsqualität, Daten- und IT-Sicherheit sowie Kontrollrechte bei der Nutzung von Cloudleistung berücksichtigt werden. Mit den EVB-IT Cloud steht nun ein weiteres und von den öffentlichen Auftraggebern lang erwartetes Werkzeug für die öffentlichen Beschaffungsstellen in Bund, Ländern und Kommunen zur Verfügung.

Die EVB-IT Cloud bestehen aus einem Vertragsmuster, den Einkaufsbedingungen (AGB), einem fachlichen Kriterienkatalog und einer Anlage zur partiellen Einbeziehung von Anbieter-AGB. Sie setzen die vertraglichen Mindeststandards des Bundesamts für Sicherheit in der Informationstechnik und die Basisanforderungen des C5-Kataloges (Cloud Computing Compliance Criteria Catalogue) um. Die Hinweise zur Nutzung unterstützen bei der Anwendung und beim Ausfüllen der EVB-IT Cloud.

18 Monate nach ihrer Veröffentlichung werden die EVB-IT Cloud einer erneuten Prüfung unterzogen und ggf. angepasst. Hierzu ist die Arbeitsgruppe EVB-IT insbesondere auf das Feedback der Anwender angewiesen. Bitte teilen Sie Ihre Erfahrungen und Anregungen unter DGI5@bmi.bund.de mit.

Die EVB-IT Cloud erweitern die bestehenden und mit der IT-Wirtschaft abgestimmten zehn EVB-IT Vertragsmuster für die Durchführungen von IT-Beschaffungen öffentlicher Auftraggeber. Diese Vertragsmuster werden seit Mitte der 90er Jahre von einer Arbeitsgruppe unter Federführung des Bundesministeriums des Innern und für Heimat und mit Teilnehmern aus Bund, Ländern und Kommunen erstellt. In ständiger Übung werden die EVB-IT vor ihrer Einführung mit dem Bitkom mit dem Ziel abgestimmt, Einvernehmen herzustellen und eine breite Akzeptanz bei den potenziellen Vertragspartnern zu erreichen.

Bosch bündelt Automotive Softwareentwicklung bei ETAS

Gemäß einer Mitteilung vom 08. Dezember 2022 bündelt Bosch unter dem Dach der ETAS GmbH künftig die Entwicklung von anwendungsunabhängiger Software für Fahrzeuge und Cloud. Die ESCRYPT-Automotive-Security-Lösungen werden dabei zum Bestandteil des Angebots einer domänenübergreifenden Plattform für Software-definierte Fahrzeuge der Zukunft.

Für eine führende Rolle in der softwaredominierten Zukunft der Mobilität nimmt Bosch weitere Weichenstellungen vor. Übergreifend einsetzbare Fahrzeug-Basissoftware, Middleware, Cloud-Services sowie Entwicklungswerkzeuge werden künftig unter dem Dach der ETAS GmbH entwickelt und vertrieben. Ab Mitte 2022 sollen insgesamt 2.300 Fachleute aus unterschiedlichen Entwicklungsbereichen von Bosch und ETAS in der ETAS GmbH zusammengeführt werden.

Mit der Bündelung des Angebots von anwendungsunabhängiger Software für Fahrzeuge und Cloud bei ETAS entsteht eine zentrale Plattform, mit der Software künftig schneller, effizienter und gemeinsam mit Partnern entwickelt werden kann. „Unser universelles Softwarefundament ist eine zentrale Voraussetzung für die Digitalisierung moderner, softwaredefinierter Fahrzeuge“, sagt Dr. Stefan Hartung, Vorsitzender des Unternehmensbereichs Mobility Solutions der Robert Bosch GmbH. Bosch kombiniert künftig seine übergreifend einsetzbare Softwareplattform mit der Kompetenz in der Entwicklung innovativer Softwarefunktionen. „Damit schafft Bosch ein am Markt einzigartiges Angebot und erzielt einen signifikanten Wettbewerbsvorteil“, sagt Dr. Markus Heyn, Geschäftsführer der Robert Bosch GmbH. ETAS bietet die übergreifend einsetzbare Plattform sowie die passende Entwicklungsumgebung künftig sowohl Automobilherstellern als auch anderen Zulieferern an.

„Für die Entwicklung von Fahrzeug-Betriebssystemen wollen wir uns künftig weltweit noch besser am Markt aufstellen“, sagt Heyn „Mit diesem Schritt bieten wir für bestehende und neue Kunden ein ganzheitliches Angebot einer horizontalen, domänenübergreifenden Plattform, um Software-definierte Fahrzeuge zu realisieren“, ergänzt Christoph Hartung, Vorsitzender der Geschäftsführung der ETAS GmbH.

ESCRYPT, als eine Marke der ETAS GmbH, bringt dabei die geeigneten Cybersecurity-Lösungen für die Absicherung der Software-definierter Fahrzeuge, intelligenten Verkehrssysteme und vernetzten Fahrzeugflotten der Zukunft mit ein.

Industrielle Cybersicherheit: Zunahme der gemeldeten Schwachstellen auch bei IoT-, IT- und medizinische Geräten

Die Offenlegung von Schwachstellen in industriellen Kontrollsystemen (ICS) hat sich in den letzten vier Jahren mehr als verdoppelt (plus 110 %), allein in der zweiten Jahreshälfte 2021 stieg im Vergleich zu den vorangegangenen sechs Monaten die Anzahl um 25 Prozent. Dies geht aus dem vierten halbjährlichen ICS Risk & Vulnerability Report hervor, der am 02. März 2022 von Claroty, Spezialist für die Sicherheit von cyber-physischen Systemen (CPS) in Industrie-, Healthcare- und Unternehmensumgebungen, veröffentlicht wurde. Die Studie zeigt zudem, dass sich ICS-Schwachstellen über die Betriebstechnik (OT) hinaus auf das erweiterte Internet der Dinge (XIoT) ausweiten: 34 Prozent der aufgedeckten Sicherheitslücken betrafen demnach IoT-, Medizin (Internet of Medical Things/IoMT)- und IT-Systeme.

Der Bericht bietet eine umfassende Analyse der im zweiten Halbjahr 2021 veröffentlichten ICS-Schwachstellen, einschließlich der von Clarotys preisgekröntem Forschungsteam Team82 aufgedeckten sowie solcher, die aus vertrauenswürdigen offenen Quellen stammen. Hierzu zählen die National Vulnerability Database (NVD), das Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), CERT@VDE, MITRE und die Anbieter von Industrieautomatisierung Schneider Electric und Siemens.

„Da immer mehr cyber-physische Systeme miteinander verbunden werden und der Zugang zu diesen Netzwerken über das Internet und die Cloud erfolgt, benötigen Sicherheitsverantwortliche zeitnahe, nützliche Schwachstelleninformationen, um ihr Risikomanagement entsprechend anpassen zu können“, erklärt Amir Preminger, Vice President of Research von Claroty. „Die zunehmende digitale Transformation in Verbindung mit der Konvergenz von ICS- und IT-Infrastruktur ermöglicht es den Forschern, ihre Arbeit über die OT hinaus auf das XIoT auszuweiten. Aufsehenerregende

Cybervorfälle im zweiten Halbjahr 2021 wie die Tardigrade-Malware, die Log4j-Schwachstelle oder der Ransomware-Angriff auf den Tankstellenzulieferer Oiltanking zeigen die Anfälligkeit dieser Netzwerke und unterstreichen die Notwendigkeit der Zusammenarbeit der Sicherheitsforscher bei der Entdeckung und Offenlegung neuer Schwachstellen."

Die wichtigsten Ergebnisse:

Die Anzahl der offengelegten ICS-Schwachstellen ist in den letzten vier Jahren um 110 Prozent gestiegen. Dies zeigt, dass das Bewusstsein für dieses Thema deutlich gestiegen ist und Sicherheitsforscher zunehmend auch OT-Umgebungen einbeziehen. 797 Schwachstellen wurden im zweiten Halbjahr 2021 gemeldet, was einem Anstieg von 25 Prozent gegenüber 637 im ersten Halbjahr 2021 entspricht.

34 Prozent der aufgedeckten Schwachstellen betreffen IoT-, IoMT- und IT-Komponenten. Deshalb müssen Unternehmen OT, IT und IoT unter einem konvergenten Sicherheitsmanagement zusammenführen. Betreiber dieser Systeme benötigen einen genauen Überblick über ihre Umgebungen, um Schwachstellen zu managen und ihre Gefährdung zu verringern.

Die Hälfte der Schwachstellen (50 %) wurde von externen Spezialisten entdeckt, die meisten davon durch Forscher von Cybersicherheitsunternehmen, die ihren Schwerpunkt neben der IT- und IoT-Sicherheitsforschung auf ICS verlagern. Außerdem meldeten 55 neue Forscher Sicherheitslücken.

Die Zahl der durch interne Experten gemeldeten Schwachstellen stieg in den letzten vier Jahren um 76 Prozent. Dies unterstreicht die wachsende Bedeutung der Disziplin sowie einen höheren Reifegrad bei der Schwachstellenforschung und zeigt, dass die Hersteller immer größere Ressourcen für die Sicherheit ihrer Produkte bereitstellen.

87 Prozent der Schwachstellen weisen eine geringe Angriffskomplexität auf, d. h. sie erfordern keine speziellen Bedingungen und Angreifer können jedes Mal mit einem wiederholbaren Erfolg rechnen. 70 Prozent erfordern keine besonderen Berechtigungen, um eine Schwachstelle erfolgreich auszunutzen, und 64 Prozent der Schwachstellen bedürfen keiner Benutzerinteraktion.

63 Prozent sind aus der Ferne ausnutzbar. Dies zeigt, dass die Sicherung von Remote-Verbindungen und Geräten von größter Wichtigkeit ist, zumal der durch die Pandemie beschleunigte Bedarf an sicheren Fernzugriffslösungen ungebrochen ist.

Clarotys Forschungsabteilung Team82 bleibt führend bei der Erforschung von ICS-Schwachstellen und hat im zweiten Halbjahr 2021 110 Schwachstellen und insgesamt über 260 Schwachstellen aufgedeckt.

Die verbreitetste potenzielle Auswirkung ist die Remote-Code-Ausführung (bei 53 % der Schwachstellen), gefolgt von Störungen (Denial-of-Service) (42 %), der Umgehung von Schutzmechanismen (37 %) und Möglichkeiten für Angreifer, Anwendungsdaten zu lesen (33 %).

Zu den wichtigsten Abhilfemaßnahmen gehören Netzwerksegmentierung (empfohlen bei 21 % der Schwachstellen), der Schutz vor Ransomware, Phishing und Spam (15 %) und Beschränkungen des Datenverkehrs (13 %).

Die vollständigen Ergebnisse, eingehende Analysen und zusätzlichen Maßnahmen zum Schutz vor unzulässigen Zugriffen und Risiken, finden sich im halbjährlichen ICS Risk & Vulnerability Report von Claroty. Dieser kann hier heruntergeladen werden: *https://security.claroty.com/1H-vulnerability-report-2021*

„Ice Phishing" – neue Art von Blockchain-Betrug auf dem Vormarsch

Microsoft warnte am 01.März 2022 vor einer neuen Art von Blockchain-zentrierten Angriffen, die auf web3 (die dezentrale Umgebung, die auf der Blockchain geschaffen wird) abzielen. In diesem Zusammenhang hat das Microsoft 365 Defender Research Team den jüngsten Badger DAO-Angriff analysiert, bei dem im November und Dezember 2021 mehr als 120 Millionen Dollar von Blockchain-Nutzern gestohlen wurden. Die Sicherheitsexperten warnen, dass diese Angriffe auf dem Vormarsch sind: „Es gibt mehrere Arten von Phishing-Angriffen in der web3-Welt", schreibt Christian Seifert, Mitglied des Microsoft 365 Defender Research Teams. „Die Technologie ist noch aufkeimend und es können neue Arten von Angriffen entstehen."

Beim Eisfischen wird ein Loch in ein gefrorenes Gewässer geschnitten, um Fische zu fangen. Beim Ice-Phishing, wie es das Defender-Team nennt, wird ein Benutzer durch Social Engineering dazu verleitet, eine Transaktion zu unterzeichnen, die die Genehmigung der Token des Benutzers an den Angreifer delegiert, ohne dass dabei die privaten Schlüssel gestohlen werden. Der Angriff korrumpiert eine gängige Transaktionsart, die Interaktionen mit DeFi-Smart Contracts ermöglicht, da diese verwendet werden, um mit den Token des Nutzers zu interagieren (z.B. Swaps). Bei einem „Ice-Phishing"-Angriff muss der Angreifer lediglich die Adresse des Spenders in die Adresse des Angreifers ändern.

Dies kann sehr effektiv sein, da auf der Benutzeroberfläche nicht alle relevanten Informationen angezeigt werden, die darauf hinweisen, dass die Transaktion manipuliert wurde. Sobald die Genehmigungstransaktion unterzeichnet, eingereicht und abgebaut wurde, kann der Spender auf das Geld zugreifen. Im Falle eines ‚Ice-Phishing'-Angriffs kann der Angreifer über einen gewissen Zeitraum Genehmigungen sammeln und dann alle Geldbörsen der Opfer schnell leeren.

Weitere Phishingmethoden der Bedrohungsakteure

1. Speer-Phishing

Der Cyberkriminelle hat sich entweder über die Gruppe informiert oder Daten von Social-Media-Plattformen gesammelt, um Nutzer zu täuschen. Eine Spear-Phishing-E-Mail geht in der Regel an eine Person oder eine kleine Gruppe von Personen, die diesen Dienst nutzen. Sie enthält eine Form der Personalisierung – vielleicht den Namen der Person oder den Namen eines Kunden.

2. Executive Whaling

Diese Art zielt vor allem auf leitende Angestellte und Verwaltungsangestellte ab, um Geld von Konten abzuschöpfen oder vertrauliche Daten zu stehlen. Diese Art von Betrug zeichnet sich durch Personalisierung und detaillierte Kenntnis der Führungskraft und des Unternehmens aus.

3. Social Engineering

Der Einsatz psychologischer Manipulation, um Menschen dazu zu bringen, vertrauliche Informationen preiszugeben oder Zugang zu Geldern zu gewähren. Die Kunst des Social Engineering kann auch darin bestehen, Informationen von Social-Media-Plattformen zu sammeln. LinkedIn, Facebook und andere Plattformen bieten eine Fülle von Informationen über die Mitarbeiter eines Unternehmens.

Effektive Schutzmaßnahmen

Eine Schulung zum Thema Sicherheit kann die Nutzer und Mitarbeiter in den Unternehmen in die Lage versetzen, diese vielfäl-

tigen Arten von Betrug besser zu erkennen. Die effektivste Maßnahme zur Vorbeugung solcher Angriffe ist, ein umfassendes Security Awareness Training für die Mitarbeiter anzubieten und umzusetzen. Grundsätzlich wird hierbei versucht, mithilfe von simulierten Phishing-Mails zu testen, wie aufmerksam die Mitarbeiter sind. Das Ziel der Trainings ist, eine gesteigerte Sensibilisierung bezüglich der Gefahren und dem Erkennen solcher Attacken zu erreichen. Die Anzahl der erfolgreichen Phishing-Angriffe auf das Unternehmen kann durch ein solches Training sehr stark reduziert werden und neben den technischen Sicherheitsoptionen können die Mitarbeiter somit als „menschliche Firewall" geschult und eingesetzt werden.

Utimaco: Deep Dark Web System

Utimaco, ein weltweit führender Anbieter von IT-Sicherheitslösungen, informierte am 23. Februar 2022 über die Erweiterung des Portfolios an Cybersecurity-Lösungen um ein neues Produkt: das Deep Dark Web System. Es bietet Analysten in Unternehmen und Ermittlern in der Strafverfolgung die erforderlichen hochentwickelten Tools für die Automatisierung und Überwachung des Dark Web, um zu verhindern, dass Kriminelle von gestohlenen Daten profitieren.

Für Unternehmen, Organisationen und einzelne Personen ist es vorteilhaft zu wissen, ob Informationen über sie, ihre Mitarbeiter oder ihre Kunden auf Darknet-Marktplätzen verfügbar sind. Allerdings bestehen schätzungsweise 96-99 Prozent des Internets aus dem Deep Web, also Seiten, die nicht von Suchmaschinen indiziert werden oder für deren Zugriff spezielle Anmeldedaten erforderlich sind.

Das Utimaco Deep Dark Web System bietet nun ähnlich wie Media-Tracking-Dienste eine Möglichkeit, das Dark Web nach Schlüsselbegriffen zu durchsuchen. So können Unternehmen Bedrohungen aus dem Dark Web erkennen und Informationen über mögliche neue Bedrohungen gewinnen, um sich oder ihre Kunden zu schützen.

Die Funktionalitäten von Utimaco Deep Dark Web System umfassen:

- Umfassender Einblick in die Risiken von Organisationen im Dark Web, damit diese proaktiv auf Bedrohungen reagieren können
- Erstklassige Technologie mit seit mehr als zehn Jahren bewährten Algorithmen
- Gehosted auf sicheren Servern in Deutschland
- Unterstützt dokumentierten Zugang zu allen bekannten Websites im Deep- und Dark-Web (DDW)
- Einzige Lösung, die als SaaS- und als On-Premises-Installation verfügbar ist

Mit seiner einzigartigen Kombination aus leistungsfähiger Technologie und langjähriger Erfahrung von Utimaco im Bereich Cybersecurity als vertrauenswürdiger Partner von Unternehmen aus den Bereichen Banken und Finanzdienstleistungen, Telekommunikation, Automobil, IT, Fertigung und Cloud Service Provider sowie von Regierungen, Behörden und Anbietern kritischer Infrastrukturen bietet das Deep Dark Web System von Utimaco eine überzeugende Lösung für jedes Unternehmen, das im Kampf gegen Cyberkriminalität die Nase vorn haben möchte.

Interessierte Kunden können das Deep Dark Web System von Utimaco testen und erhalten mit einem kostenlosen Testzugang vollen Systemzugang. Weitere Informationen unter *https://utimaco.com/*

Konsortium aus ecsec, Spherity and msg gewinnt das Implementierungsprojekt der Gaia-X Notarization API

Ein Konsortium aus ecsec, Spherity und msg hat die vom Bundesministerium für Wirtschaft und Klimaschutz finanzierte Implementierung der Gaia-X Notarization API gewonnen (Information vom 23, Februar 2022). Gemeinsam mit msg und Spherity entwickelt die ecsec GmbH eine dezentrale Identitätslösung, die es Unternehmen ermöglicht, ihre eigene dezentrale Identität zu verwalten und vorgegebene Stammdaten als W3C-konforme digitale verifizierbare Berechtigungsnachweise (Verifiable Credentials) zu beglaubigen. Die Lösung wird nach der Implementierungsphase als Open Source angeboten und ermöglicht allen Gaia-X-Teilnehmern sie als Referenzimplementierung zu nutzen, um sich Gaia-X und Catena-X oder anderen Ökosystemen anzuschließen, die dieselbe Basistechnologie verwenden.

Die Gaia-X Notarization API im Detail

Die Stammdatenbescheinigung von Unternehmen wird das Vertrauen in das Gaia-X-Ökosystem stärken. Sie wird es den Nutzern ermöglichen, die Herkunft von Informationen und deren Integrität zu überprüfen. Eine Vielzahl von Anwendungsfällen in der Industrie wird durch den Einsatz der neuen Technologie verbessert. Dies umfasst zum Beispiel

- die Erstellung von Berechtigungsnachweisen wie Beschäftigung, Mitgliedschaft oder Rolle im Unternehmen,
- den vertrauenswürdigen Austausch von Bankdaten zwischen Käufern und Verkäufern,
- die Digitalisierung von Produkt- und Unternehmenszertifizierungen, wie Gaia-X-Labels oder ISO-Zertifizierungen,
- den Nachweis der Gesetzeskonformität, z.B. für das US DSCSA oder für das deutsche Lieferkettengesetz und
- das Ausstellen von Produktinformationen für die kommenden digitalen Produktpässe.
- Technisch gesehen wird die Notarization API
- die Zertifikate von GAIA-X-Teilnehmern von klassischen Formaten in digitale, überprüfbare Berechtigungsnachweise (Verifiable Credentials) umwandeln und mit digitalen Signaturen versehen,
- GAIA-X-Teilnehmer samt der zugehörigen Stammdaten (z. B. Name, Adresse, Steueridentifikationsnummer, Bankverbindung, Eintrag im Handelsregister) digitalisieren,
- Unternehmen die Möglichkeit geben ihre „Decentralized Identifiers" (DIDs) für ihr Unternehmen, ihre IOT-Geräte, Produkte und Dienstleistungen zu erstellen und zu nutzen,
- eine Brücke zwischen selbstbestimmten Identitäten (Self-Sovereign Identity, SSI) und der eIDAS-Verordnung für Unternehmenseigentümer (z.B. Verwendung der eID) bilden,
- Organisationen die Möglichkeit geben, als Vertrauensanker zu fungieren (z.B. Regierungen, Gaia-X AISBL).

„Wir sind stolz darauf, eine Kernkomponente für eine zukunftsfähige europäische Cloud-Infrastruktur zu entwickeln und zu implementieren", sagt Steffen Schwalm, Principal Business Consultant bei msg security advisors: „Mit der Notarization API entwickeln wir

einen Kernbaustein für bewährte und sichere SSI als Schlüssel für vertrauenswürdigen Datenaustausch und -nutzung in Gaia-X."

„Die Implementierung der Gaia-X Federation Services wird eine starke Verschiebung hin zu dezentralen Technologien und deren Anwendung in industriellen Anwendungsfällen mit sich bringen. Dezentrale Identitäten werden für Unternehmen, Produkte, IOT-Geräte und auch Menschen genutzt werden, um die Industrie im Allgemeinen und die Lieferkettenprozesse im Besonderen zu digitalisieren", sagt Carsten Stöcker, Gründer von Spherity.

Die Notarization API ist ein Beitrag zu Gaia-X, der die sichere und standardkonforme Ausstellung von verifizierbaren Berechtigungsnachweisen in Kombination mit einer Vertrauenskette zu einem bekannten Vertrauensanker ermöglicht. Diese Lösung wird in einem hybriden Ansatz durch die Integration mit X.509-basierten Public-Key Infrastrukturen implementiert. Diese Technologie wird die Grundlage für allgemeine Beglaubigungsdienste bilden, die eine unendliche Vielfalt an überprüfbaren Berechtigungsnachweisen für Bürger, Organisationen, Maschinen, Algorithmen oder Lieferkettenereignisse ausstellen können.

DIHK-Analyse: Rechtliche Hürden erschweren Nutzung von Daten

Rechtliche Unsicherheiten sind für Deutschlands Betriebe das größte Problem bei der stärkeren Nutzung von Daten. Das hat der Deutsche Industrie- und Handelskammertag (DIHK) in einer Sonderauswertung der bundesweiten IHK-Digitalisierungsumfrage unter 4300 Unternehmen aller Größenklassen ermittelt und am 22. Februar 2022 bekannt gemacht. Danach fühlen sich 57 Prozent der Unternehmen durch „datenschutzrechtliche Hemmnisse" bei der Datennutzung behindert. „Vor allem kleinere und mittlere Unternehmen werden überproportional stark belastet", sagt DIHK-Hauptgeschäftsführer Martin Wansleben. „Hier sind vereinfachte Vorschriften oder Ausnahmeregelungen dringend erforderlich. Wir schlagen vor, Erleichterungen dann einzuführen, wenn die Verarbeitung der Daten nicht der Schwerpunkt der unternehmerischen Tätigkeit darstellt."

Hinzu kommen aus Sicht der Unternehmen weitere juristische Unklarheiten, zum Beispiel über Art und Umfang von Nutzungsrechten, die für 38 Prozent eine Herausforderung darstellen. Ebenso viele führten „technische Hürden" ins Feld. Jeweils 36 Prozent gaben „mangelnde Datenqualität" und „fehlendes Know-how" an.

„Es fehlt den deutschen Unternehmen jedenfalls nicht am Bewusstsein, dass Daten mittlerweile einer der wichtigsten Treiber des wirtschaftlichen Wachstums sind", sagt Wansleben. 60 Prozent der Betriebe bezeichneten den gezielten Einsatz von Daten als „sehr wichtig" für ihre eigene Unternehmensentwicklung, weitere 31 Prozent als „wichtig". Neun von zehn Betrieben gingen davon aus, dass sie künftig stärker mit Daten arbeiten werden. „Der Spirit stimmt", so Wansleben. „Aber die deutschen Unternehmen brauchen jetzt die richtigen Regeln, um ihre Möglichkeiten rechtssicher und zukunftsorientiert nutzen zu können." 71 Prozent der Unternehmen setzen ihre Daten dafür ein, um ihre Kundenbeziehungen zu verbessern. 70 Prozent nannten als Motiv die Optimierung von Geschäfts- und Produktionsprozessen.

Mit großem Interesse blicken die deutschen Unternehmen deshalb nach den Worten von Wansleben auf den europäischen „Data Act". Damit sollen – ohne bestehende Datenschutzstandards (DSGVO) anzutasten – die Möglichkeiten der Datennutzung verbessert werden und der Umgang mit Daten von vernetzten Geräten klar geregelt werden. Eine größere Rolle könnte hier in Zukunft den Nutzern zukommen, die über die Verwendung ihrer Daten entscheiden könnten. Daneben könnten durch den Data Act außerdem öffentliche Stellen erweiterte Befugnisse für den Zugang zu Daten erhalten. „Wir unterstützen im Interesse der wirtschaftlichen Gesamtentwicklung, dass Daten mehr genutzt werden", so Wansleben. „Das macht zusätzlich deutlich, dass Unternehmen verlässliche Spielregeln brauchen. Notwendige Grenzen bei der Offenlegung von Daten sehen wir bei der Sicherheit und dem Schutz von Geschäftsgeheimnissen. Unternehmen müssen sich darauf verlassen können, dass die Grundlage ihres Geschäftsmodells geschützt wird."

Behörden brauchen sichere Kommunikations-Tools für mobiles Arbeiten

Die Digitalisierung im Behördenumfeld kommt voran, doch sie läuft nach wie vor zu langsam. Im Schlagschatten dieser Entwicklung wird häufig zu unsicheren Kommunikations-Apps gegriffen, die ein erhebliches Risiko für die IT-Sicherheit und den Datenschutz darstellen. Sie müssen dringend durch sichere Lösungen ersetzt werden.

Die Art und Weise, wie Behörden ihre Arbeitsabläufe organisieren und gestalten, befindet sich im Umbruch. Die Präsenzarbeit im Büro ist zwar nach wie vor die Regel, doch der Anteil an Remote Work steigt. Dies ist bedingt durch eine wachsende Zahl mobiler Arbeitsplätze und den stärkeren Anteil an Homeoffice-Tätigkeit. Ohne Heimarbeitsplätze wären behördliche Workflows gekappt worden. Durch die Verlagerung wurden scheinbar festgefügte Strukturen durcheinandergewirbelt und der Druck zur rascheren Digitalisierung verstärkt. Virtual Solution hat die wichtigsten Punkte identifiziert, wie die Digitalisierung die Arbeit und die Kommunikation von Behörden verändert und welche Maßnahmen zu ihrer Umsetzung ergriffen werden müssen:

1. Adaption neuer Technologien: Cloud, Mobile Work und Edge Computing sind etablierte IT-Technologien, die Behörden aber noch viel zu wenig nutzen. Ohne eine rasche Adaption können die Vorgaben zur Digitalisierung nicht umgesetzt werden. Besonders wichtig ist dabei das Thema Mobile Work. Intern wächst der Anteil der Behördenmitarbeiter und -mitarbeiterinnen, die mobil oder im Homeoffice tätig sind. Sie müssen in die Lage versetzt werden, auch von dort effizient und sicher arbeiten zu können.
2. Umgang mit Schatten-IT: Der Mangel an geeigneten mobilen Endgeräten und Kommunikations-Lösungen führt notgedrungen zur ungeregelten Nutzung privater Geräte und unsicherer Anwendungen wie WhatsApp. Damit entsteht ein unkalkulierbares Gefahrenpotenzial, Security-Richtlinien werden unterlaufen und die Umsetzung von Datenschutzvorgaben wird unmöglich.
3. Sicherung der internen Kommunikation: Sowohl für die mobile Kommunikation als auch für die Arbeit im Homeoffice müssen sichere Geräte und Programme zur Verfügung stehen. Die Nutzung privater Apps für berufliche Zwecke muss zwingend verhindert werden. Die Mitarbeiter sollen diese aber weiterhin auf ein und demselben Gerät privat nutzen können, egal ob privates

Handy (BYOD) oder Dienst-Smartphone (COPE). Anders ist eine große Akzeptanz nicht zu erreichen.

4. Umfassende Security-Konzepte: Sowohl für COPE- als auch für BYOD-Szenarien müssen mobile Geräte sicher eingesetzt werden können, ohne Datenschutz- (DSGVO), Datensicherheits- (ISO 27001) oder KRITIS-Vorgaben zu verletzen. Außerdem müssen die Sicherheitsrichtlinien der jeweiligen Behörde berücksichtigt werden. Dabei darf es keine Unterschiede zwischen Präsenzarbeit und Remote Work geben. Beide müssen den gleichen strikten Sicherheitsvorgaben unterliegen.

„Ohne eine sichere mobile Kommunikationslösung werden die gesetzlichen Vorgaben zur sicheren Digitalisierung von Behörden und deren Diensten nicht erreichbar sein", erklärt Sascha Wellershoff, CEO bei Virtual Solution. „Das unkontrollierte Nebeneinander von beruflichen und privaten Anwendungen gefährdet die Sicherheit und muss beendet werden. Nur Lösungen, die durch ihre strikte Trennung höchste Sicherheitsstandards einhalten, sind dafür geeignet."

Dieses Listicle kann unter *www.pr-com.de/companies/virtual-solution* abgerufen werden.

Hybrides Arbeiten und Netzwerksicherheit: die Firewall-Metamorphose

Kommentar vom 17. Februar 2022 von Michael Veit, Sophos

Die momentane Entwicklung der modernen Arbeitswelt legt den Schluss nahe, dass sowohl traditionelle als auch Cloud-Umgebungen zu einer Welt zusammenwachsen, in der Anwendungsfälle für hybride Sicherheitsinfrastrukturen die Zukunft der Netzwerksicherheit dominieren werden. Hier können SASE-Ansätze den Unternehmen ein höchstes Maß an Flexibilität bieten, um auf beiden Seiten des Spektrums zu interagieren und zu arbeiten, während der Übergang in diese neue Arbeitswelt voranschreitet.

Folge der aktuellen Entwicklung ist, dass immer mehr Unternehmen Ressourcen und Infrastruktur in die Cloud verlagern. Diese Migration hat die Grenzen herkömmlicher Firewalls aufgezeigt, die nicht mehr in der Lage sind, die für hybride und virtualisierte Umgebungen typischen Sicherheitsprobleme zu bewältigen. Daraus ergeben sich zwei der wichtigsten Anforderungen und Eigenschaften, die eine Netzwerk-Firewall der Zukunft erfüllen muss:

- Das Management einer zerstreuten Verwaltungs- und Kontrollebene, in der die Steuerung und Kontrolle der Firewall-Funktionen in den eher „traditionellen" Perimeter-Anwendungsfällen flexibel beibehalten werden kann, während gleichzeitig ein Richtlinienkonstrukt übernommen wird, das auch in der Cloud anwendbar ist. Eine Technologie, die über beide Bereitstellungstypen und Anwendungsfälle hinweg sicherstellen kann, dass die Kundenerfahrung und damit die Übernahme des neuen Ansatzes positiv sein wird, ist deshalb essenziell.
- Die Skalierbarkeit der Verarbeitungsdatenebene muss ebenfalls ein Schlüsselfaktor sein. Die noch notwendige On-Premise-Bereitstellung erfordert Dinge wie SD-WAN, interne Sicherheitsverarbeitung und Konnektivität – muss aber aufgrund von Upgrades in Konnektivitätsinfrastrukturen wie 5G auch in der Lage sein, noch höhere Geschwindigkeiten als zuvor zu verarbeiten. Wohingegen in der Cloud bereitgestellte Firewalls den plötzlichen Anstieg der Verarbeitungsanforderungen bewältigen müssen, da die Benutzer immer mehr mobil und in verschiedenen Zeitzonen online arbeiten. Daher ist eine Datenebene, die für beide Szenarien funktioniert und gleichzeitig eine ähnliche Benutzererfahrung bietet, ebenfalls sehr wichtig.

In Folge dieser Entwicklung werden wir immer mehr Dienste wie Secure Web Access, Zero Trust Network Access und SAAS Access Security sehen – und sie werden zu einer Hauptstütze für Unternehmen werden, da sie für Kunden bequem sind und bald auch vertraut sein werden. Bei näherer Betrachtung dieser Services wird schnell klar, dass sie sich im Wesentlichen mit dem Zugriff auf öffentliche Websites und öffentliche/private Anwendungen befassen. Die nächste natürliche Entwicklung für diese Angebote wird nun darin bestehen, den gesamten Datenverkehr und alle Daten an diese Dienste zu senden. Es entsteht ein natürlicher Ort, an dem Firewalls as a Service als Angebot hinzugefügt werden können. Während bislang vor allem Großkonzerne diese Plattformen nutzen, stehen die Angebote mittlerweile zu einem immer besseren Preis-Leistungs-Verhältnis zur Verfügung und werden so auch für KMU-Kunden interessant. Auf diese Weise werden wir letztendlich eine immer größere Verschiebung von On-Premise-Firewalls hin zu zu SASE-Plattformen sehen.

Allerdings werden Firewalls immer einen Platz im Zero-Trust-Modell haben, sofern wir nicht glauben, dass alle Formen von Netzwerken aufhören zu existieren und die Netzwerk-zu-Netzwerk-Kommunikation sich praktisch auflöst. Momentan stellt die Perimeter-Platzierung für Organisationen einen immer wichtigeren Faktor dar – aber diese Transformation wird nicht von heute auf morgen stattfinden. Genau in diesen Unsicherheiten einer hybriden Arbeitswelt kann das flexible SASE-Modell punkten, Firewalls in verschiedenen Formen einbeziehen und damit kohärent mit den Zero-Trust-Prinzipien arbeiten. Die Möglichkeiten sind hier endlos.

LinkedIn: *https://www.linkedin.com/groups/9054356/*

Imperva-Studie: Deutsche Unternehmen sind auf Cyberangriffe nicht ausreichend vorbereitet

Die Fakten:

- 44 Prozent der betrachteten Unternehmen haben keinen aktuellen Krisenplan
- Fast jeder fünfte befragte IT-Manager hat berichtet, dass Cyberangriffe zu Kundenverlusten geführt haben, 46 Prozent erlitten einen Ausfall der Systeme
- 47 Prozent der Befragten rechnen mit einem deutlichen Anstieg der Cyber-Attacken in 2022

Die Bedrohungslage durch Cyberangriffe hat sich in den letzten zwölf Monaten für die untersuchten deutschen Unternehmen verschärft; gleichzeitig ist jedoch ein großer Teil von ihnen nicht adäquat auf solche Angriffe vorbereitet. Das legt eine am 03. März 2022 veröffentlichte von Studie von Imperva, Inc. (@Imperva) nahe, die auf einer Befragung des Marktforschungsunternehmens YouGov unter Angestellten mit weitgehender bzw. alleiniger Entscheidungsbefugnis im Berufsbereich IT basiert.

Cyberangriffe mit massiv geschäftsschädigenden Folgen

36 Prozent der befragten IT-Manager konstatieren, dass die Zahl der Cyberattacken auf ihr Unternehmen in den letzten zwölf Monaten etwas oder sogar in hohem Maße zugenommen hat. Dabei dominierten vor allem Ransomware- (20 %) und DDoS-Angriffe (18 %): bei ersterer Variante erlangen Hacker mittels Schadsoftware die

Kontrolle über den Computer und geben das Gerät erst nach Zahlung von Lösegeld wieder frei. Bei DDoS-Angriffen versuchen Hacker, so viele Anfragen an das System zu stellen, bis dieses letztlich zusammenbricht. Die Konsequenzen dieser und anderer Angriffe waren gravierend. Fast jeder fünfte befragte IT-Manager hat berichtet, dass Cyberangriffe zu Kundenverlusten geführt hätten; bei 46 Prozent kam es zu einem Ausfall der Systeme. Weitere genannte Folgen waren finanzielle Erpressung (16 %), Verkaufseinbußen (15 %), Reputationsschäden (14 %) und behördliche Sanktionen (10 %).

Zudem wurden im Kontext der Cyberangriffe bei den befragten Unternehmen verschiedene Kategorien von Daten kompromittiert oder missbraucht: am häufigsten waren Mitarbeiter- (20 %) und Kundendaten (17 %) Ziel von Manipulationen, aber auch geschütztes geistiges Eigentum, Managementinformationen (beide 16 %) sowie Budget- und andere Finanzplanungsunterlagen (13 %).

Keine Transparenz in der Nutzung von Daten – ganzheitliche Sicherheitsstrategie erforderlich

Auf die Angriffe haben die Unternehmen mit verschiedenen Maßnahmen reagiert: 50 Prozent der Befragten gaben an, dass die Cybersecurity-Strategie überarbeitet wurde; 48 Prozent haben ihre Investitionen in Cybersecurity-Tools und -Lösungen erhöht. Zudem hat fast jedes vierte Unternehmen zusätzliches Personal im Bereich der IT- und Cybersecurity eingestellt. Der Bedarf an einer strategischen Kurskorrektur und technischer Ausstattung ist hoch; so hat beispielsweise laut der Umfrage nicht einmal jedes zweite Unternehmen einen aktuellen Krisenplan (44 %). Zudem setzt nur knapp die Hälfte der befragten Unternehmen (49 %) Tools zur Datenermittlung und -klassifizierung oder Tools zur Überwachung von Datenbankaktivitäten (44 %) ein, die Aufschluss darüber geben, wie sensible Daten im Unternehmen verwendet werden.

Die Studienergebnisse haben über diese Befunde hinaus auch klar gezeigt, dass die befragten IT-Manager hinsichtlich Datenmanagement und -nutzung ihren Blick auch über den eigenen Betrieb hinaus richten müssen. Denn gerade digitale Geschäftsmodelle, aber beispielsweise auch die Zusammenarbeit mit Lieferanten erfordern zunehmend das Teilen von Daten, was weitere Sicherheitsrisiken birgt: nur 23 Prozent der befragten Unternehmen verfügen aktuell über eine vollständige und automatisierte Liste aller Drittparteien, mit denen sie interne Daten austauschen. 39 % aktualisieren eine solche Liste manuell und 16 Prozent geben an, überhaupt keine Listen an Drittanbietern zu führen. Mehr als 30 Prozent haben keine oder keine sicheren Systeme und Verfahren, die festlegen, auf welche Daten Dritte zugreifen können.

„Ein großer Teil der befragten Unternehmen zieht aus der aktuellen Bedrohungslage immer noch keine ausreichenden Konsequenzen. Und dabei beginnen die meisten Unternehmen erst jetzt so richtig, datengetriebene Geschäftsmodelle wirklich umzusetzen", konstatiert Kai Zobel, Area Vice President EMEA Imperva. „Für einen wirksamen Schutz von Daten brauchen Unternehmen eine neue Kultur, die Sicherheit und Innovation zusammen denkt, sowie Investitionen in Prozesse, Systeme und Mitarbeitende. Vor allem aber brauchen sie eine ganzheitliche Sicherheitsstrategie, die Messgrößen aus allen Unternehmensbereichen in einer zentralen Plattform zusammenbringt. Nur so lässt sich die eigene IT-Infrastruktur wirksam schützen – vor Angriffen von außen wie von innen."

Knackpunkt „Sicherheit" bei Cloud-Modellen

Zwiegespalten sind darüber hinaus viele der befragten IT-Manager auch, wenn es um das Thema Datensicherheit im Kontext der Einführung und Nutzung von Cloud-Modellen geht. Immerhin 23 Prozent bezeichnen die Einführung der Cloud unter Datenschutzaspekten als größte Cybersicherheits-Herausforderung bei Projekten zur digitalen Transformation. Zudem sind 29 Prozent der Befragten überzeugt, dass die Übersicht über die Daten On-Premises größer ist als in der Cloud (30 %: Übersicht ungefähr gleich groß). Und 31 Prozent der Befragten glauben, dass die Daten ihres Unternehmens in der Cloud weniger sicher sind als On-Premises; nur 18 Prozent sehen die Daten in der Cloud besser aufgehoben.

Deutlicher Anstieg der Cyberangriffe prognostiziert – bei Prävention Mitarbeitende im Fokus

Für das Jahr 2022 rechnen 47 Prozent der Befragten mit einem deutlichen Anstieg der Cyberangriffe: 31 Prozent gehen von einem Plus von bis zu 50 Prozent aus; weitere 16 Prozent rechnen sogar mit noch mehr Attacken. Am stärksten wird die Bedrohung durch Ransomware-Attacken eingestuft (35 %); jeweils 13 Prozent der Befragten nennen DDoS-Angriffe und Insider-Bedrohungen als größtes Risiko.

Bei der Eindämmung der Bedrohungslage spielen strategische Maßnahmen, vor allem aber aktuelle Arbeitsmodelle und die Einbindung der Mitarbeitenden eine bedeutende Rolle. 50 Prozent der befragten Unternehmen planen, in den nächsten zwölf Monaten verstärkt Schulungen anzubieten, um für das Thema Cybersicherheit zu sensibilisieren. Ein Drittel der befragten Unternehmen (32 %) will die Richtlinien zur Remote-Arbeit und 18 Prozent wollen ihre BYOD-Richtlinien (Bring your own Device) überprüfen. Die Aktualisierung des Krisenplans für den Fall eines Angriffes wird als zweithäufigste Maßnahme genannt (37 %).

Über die Studie:

Die Online-Umfrage, auf der die Studie basiert, wurde im Zeitraum vom 10. – 20. Dezember 2021 von YouGov Deutschland GmbH durchgeführt. Befragt wurden insgesamt 528 Personen mit weitgehender bzw. alleiniger Entscheidungsbefugnis im Berufsbereich IT, die in Unternehmen mit mindestens zehn Mitarbeitern arbeiten.

Hier kann die Studie heruntergeladen werden: *https://www.imperva.com/resources/lp/Deutschland-YouGov-Datenschutzstudie-2022-Ende.pdf*

KPMG e-crime-Studie: Mailserver beliebtestes Einfallstor

61 Prozent der Unternehmen in Deutschland schätzen ihr Risiko, von Computerkriminellen angegriffen zu werden, als „hoch" oder „sehr hoch" ein. Besonders bedenklich: Fast allen Unternehmen fällt es immer schwerer, erste Anzeichen einer Cyberattacke überhaupt zu erkennen (84 Prozent). Und über die Hälfte geht davon aus, dass das Risiko eines Cyberangriffs in den nächsten zwei Jahren noch steigen wird. Das sind die Kernergebnisse einer KPMG-Umfrage <https://home.kpmg/de/de/home/themen/2022/02/computerkriminali taet-in-der-deutschen-wirtschaft.html> unter 1.000 repräsentativ nach Branche und Umsatz ausgewählten Unternehmen zu ihren Erfahrungen mit Computerkriminalität.

KPMG-Partner Michael Sauermann: „Computerkriminalität frisst sich wie ein Geschwür durch die deutsche Unternehmenslandschaft. Vor allem Mailserver stellen ein attraktives Angriffsziel dar. Phishing-Mails, Business E-Mail Compromise- oder Ransomware-

Angriffe sind praktisch überall an der Tagesordnung. Dabei werden die Angriffe immer vielfältiger, durchschlagender, entsprechend brisanter und teurer für die Unternehmen. Die zunehmende Komplexität der eingesetzten Technologien stellt für über drei Viertel der Befragten eine große Herausforderung dar."

Unachtsamkeit und unzureichend geschulte Mitarbeitende (95 bzw. 81 Prozent) zählen zu den meistgenannten Faktoren, die Computerkriminalität begünstigen. Zudem sehen die Unternehmen eine mangelnde Sicherheitskultur beziehungsweise ein mangelndes Risikoverständnis bei ihren Mitarbeitenden (86 Prozent) als wesentliche Risikofaktoren an. Michael Sauermann: „Angemessene Schulungen sowie Sensibilisierung der Mitarbeitenden sind von zentraler Bedeutung, um Computerkriminalität im eigenen Unternehmen zu verhindern. Ideal wäre es, wenn Menschen ein Bewusstsein ähnlich einer ‚Human Firewall' entwickeln könnten."

Mailserver im Visier – Betrugsdelikte sind am häufigsten

39 Prozent der befragten Unternehmen gaben an, seit 2019 von Computerkriminalität betroffen gewesen zu sein. Das mit Abstand häufigste Ziel der Täter sind die Mailserver der Unternehmen (67 Prozent). Unter den Straftaten verzeichnen vor allem Betrugsdelikte einen auffälligen Anstieg:

Sie machen bereits die Hälfte aller Fälle aus, gefolgt von Erpressung und Datendiebstahl mit jeweils rund 25 Prozent. Knapp ein Viertel der Befragten sah sich bereits einem erfolgreichen Ransomware-Angriff ausgesetzt, weitere 31 Prozent konnten entsprechende Versuche abwehren.

Bei 40 Prozent der von einem Ransomware-Angriff betroffenen Unternehmen kam es zu einem Betriebsausfall mit gravierenden Konsequenzen, was einen deutlichen Anstieg im Vergleich zur Vorgängerstudie 2019 bedeutet (27 Prozent). Bei jedem zweiten Unternehmen waren mehr als 75 Prozent der IT-Landschaft vom Ausfall betroffen.

Michael Sauermann: „Bei fast der Hälfte dieser Unternehmen dauerte es anschließend mindestens zwei Tage, bis sie den Betrieb wieder aufnehmen konnten. In der Praxis sehen wir Fälle, in denen Unternehmen Wochen oder sogar Monate brach liegen." Was besonders ärgerlich ist: Die Identifikation der Täter bereitet immer noch große Schwierigkeiten. Die überwiegende Mehrheit muss der Kategorie ‚unbekannte Externe' zugeordnet werden.

Corona-Pandemie zwingt Unternehmen zum Aufrüsten

Knapp die Hälfte der befragten Unternehmen gab an, angesichts der Covid-19-Pandemie Maßnahmen ergriffen zu haben, um die IT-Sicherheit zu erhöhen (45 Prozent). Besonderes Augenmerk galt dabei der Einrichtung sicherer Kommunikationskanäle für den Zugriff auf das Firmennetzwerk (91 Prozent) sowie die Definition und Kommunikation klarer Regelungen und Vorgaben zum Arbeiten aus dem Homeoffice (90 Prozent).

Hinweis: Die gesamte Studie finden Sie hier: *https://home.kpmg/de/de/home/themen/2022/02/computerkriminalitaet-in-der-deutschen-wirtschaft.html*

Rezensionen

Veranstaltungen

Christian Geminn

Selbstbestimmung, Künstliche Intelligenz und Demokratie

Am 18. und 19. November 2021 fand im Musiksaal des Hessischen Landtags die Jahrestagung des Forum Privatheit als gemeinsame Veranstaltung des Forum Privatheit und des Hessischen Beauftragten für Datenschutz und Informationsfreiheit statt. Das Forum Privatheit widmet sich der interdisziplinären Analyse von digitalisierungsrelevanten Themen und möchte im Rahmen einer aktiven Wissenschaftskommunikation diese Themen auch in die Gesellschaft tragen. Gerade Künstliche Intelligenz kann in besonderem Maße sozialnützliche oder sozialschädliche Effekte entfalten und bedarf deshalb einer intensiven gesellschaftlichen Debatte.

Die hybrid ausgestaltete Veranstaltung stand unter dem Titel „Auswirkungen der Künstlichen Intelligenz auf Selbstbestimmung und Demokratie". Moderiert wurde die Veranstaltung von Miriam Janke. Mehr als 200 Teilnehmende diskutierten Herausforderungen und mögliche Lösungen im Spannungsfeld von Privatheit, Demokratie und Anwendungen der künstlichen Intelligenz.

Ausgewählte Vorträge der Tagung können unter forum-privatheit.de abgerufen werden. Die Beiträge zur Veranstaltung wurden ferner von Magdalena Vollmer im Wege der Live-Visualisierung in Illustrationen gebannt, die ebenfalls unter forum-privatheit.de abgerufen werden können. Die grafische Aufzeichnung der Veranstaltung in einzelnen Bildern sollte die Reflexion und Kommunikation der Inhalte der Veranstaltung unterstützen.

Der Tagungsband zur vorherigen Jahrestagung des Forum Privatheit ist im Verlag Springer Vieweg unter dem Titel „Selbstbestimmung, Privatheit und Datenschutz – Gestaltungsoptionen für einen europäischen Weg" erschienen. Die nächste Jahrestagung des Forum Privatheit findet am 13. und 14. Oktober 2022 in Berlin statt und ist dem Thema „Daten-Fairness in einer globalen Welt – Grundrechtsschutz und Wettbewerb für eine internationale Data Governance" gewidmet. Vortragsvorschläge können noch bis zum 18. Mai 2022 eingereicht werden.

Grußworte sprachen zum Auftakt der Veranstaltung Karin Müller (Vizepräsidentin des Hessischen Landtags) sowie Ina Schieferdecker (Abteilungsleiterin „Forschung für technologische Souveränität und Innovationen", BMBF). Frau Müller stellte dabei den Bezug der Tagungsstätte zum Datenschutz heraus: Hier war mit dem Hessischen Datenschutzgesetz 1970 das weltweit erste formelle Datenschutzgesetz verabschiedet worden. Frau Schieferdecker betonte in ihrem Grußwort den Balanceakt, der notwendig sei, um angesichts der Herausforderungen der Digitalisierung die Bedingungen für Datenschutz und informationelle Selbstbestimmung auszuhandeln. Das Bundesministerium für Bildung und Forschung fördert das Forum Privatheit seit 2013.

Keynote: Predictive Privacy

Rainer Mühlhoff (Universität Osnabrück) widmete sich in der ersten von drei Keynotes dem Thema prädiktive Privatheit. Im Mittelpunkt