Redaktion: Helmut Reimer

Report

KI macht wissenschaftliche Exzellenz einfacher messbar

Im Projekt Evalitech untersuchten das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI) und das Fraunhofer-Institut für Materialfluss und Logistik (IML), wie man mit Hilfe von Künstlicher Intelligenz Berufungsverfahren für Führungspositionen (Lehrstühle und Institutsleitungen) optimieren kann. Dabei wurde die bisherige Indikatorik für die Technikwissenschaften und speziell für Industrie 4.0 angepasst und ergänzt. Diese Ergebnisse liegen seit dem 22. September 2022 als Bericht vor, der vom Forschungsbeirat der Plattform Industrie 4.0 und acatech – Deutsche Akademie der Technikwissenschaften herausgegeben wurde.

Die Kandidatenauswahl für Führungspositionen in den Technikwissenschaften, speziell im Umfeld von Industrie 4.0, ist komplex. Herkömmliche publikationsbasierte Metriken in Berufungsverfahren an Universitäten und Forschungsinstituten werden der Komplexität nicht gerecht: Noch immer stützt sich die Bemessung wissenschaftlicher Leistungen überwiegend auf die weltweite Wahrnehmung von Wissenschaftlerinnen und Wissenschaftlern in Fachkreisen mit Hilfe von bibliometrischen Indizes. Dazu gehört der h-Index, der lediglich die Anzahl von Zitationen von Publikationen der Wissenschaftlerin oder des Wissenschaftlers in anderen Veröffentlichungen berücksichtigt.

Deswegen legte das Projekt Evalitech im Frühjahr eine Machbarkeitsstudie vor, die neben einer neuen Indikatorik für Industrie 4.0, auch eine Abschätzung der Automatisierbarkeit durch aktuelle KI-Methoden (Web Scraping, Text Mining, etc.) sowie eine pilotartige Implementation in Form einer funktionalen Webapplikation, mit verschiedenen innovativen Interaktionskonzepten enthält.

„Mit Evalitech präsentieren wir erstmals eine differenzierte und speziell an den Bedarfen für Führungspositionen im Forschungsumfeld von Industrie 4.0 ausgerichtete Indikatorik", erklärt Wolfgang Wahlster (DFKI), Mitglied des Forschungsbeirats der Plattform Industrie 4.0. „Sie beruht auf 7 Oberkategorien, 21 Kriterien und 41 Teilkriterien. Diese haben wir zusammen mit erfahrenen Technikwissenschaftlern erarbeitet. Meine ersten praktischen Erfahrungen mit Evalitech sind positiv. Ein darauf aufbauendes Softwarewerkzeug könnte die Arbeit von Auswahlkommissionen systematisch unterstützen."

„Unser Ziel war es, wissenschaftliche Exzellenz einfacher messbar zu machen – und zwar mit einem speziellen Fokus auf Technikwissenschaften und den hier stattfindenden Transfer von Forschungsergebnissen in Unternehmen und ihre Umsetzung in Form von Innovationen", ergänzt Michael ten Hompel (Fraunhofer IML), Mitglied vom Forschungsbeirat der Plattform Industrie 4.0. „Verbreitete Ansätze wie g- und h-Index sind dazu nicht in der Lage. Durch das Evalitech-Projekt und die hier entwickelte flexible Metrik sind wir unserem Ziel einen bedeutenden Schritt nähergekommen."

Im Projekt Evalitech konnte exemplarisch der Mehrwert der neuen Indikatorik sowie einer multidimensionalen Darstellung und einer an die jeweilige Stellenausschreibung angepassten Gewichtung der Kriterien aufgezeigt werden. Aufbauend auf den Ergebnissen soll im nächsten Schritt ein transparentes und öffentliches Portal aufgebaut werden, in dem Bewerber-Profile manuell ergänzt und automatisiert durchsucht werden können. Bei Kriterien, die nicht automatisiert ermittelt werden können, sollte das Evalitech-Portal durch die Option zur Selbstauskunft eine Kontrolle und Nachvollziehbarkeit der Daten ermöglichen. Die Datengrundlage soll durch das System auf diese Weise transparent gemacht werden, so dass das Entscheidungsgremium die Vertrauenswürdigkeit der extrahierten Information prüfen und einschätzen kann. Bei vielen Berufungsverfahren sind in der Vorauswahl Kandidatinnen und Kandidaten bisher aufgrund fehlender Information zu relevanten Kriterien nicht berücksichtigt worden. Hier kann eine automatisierte Informationsextraktion aus öffentlich zugänglichen digitalen Quellen, wie bei Evalitech vorgesehen, eine zusätzliche Hilfe darstellen.

Im Projekt arbeiteten das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI) und das Fraunhofer-Institut für Materialfluss und Logistik (IML) zusammen, unterstützt durch die Ubermetrics Technologies GmbH als industriellen Verbundpartner und Dienstleister. Wolfgang Wahlster, Gründungsdirektor des Deutschen Forschungszentrums für Künstliche Intelligenz (DFKI), und Michael ten Hompel, geschäftsführender Institutsleiter des Fraunhofer IML, die das Evalitech-Projekt mit Unterstützung des wissenschaftlichen Beirats der Plattform Industrie 4.0 und acatech, der Deutschen Akademie der Technikwissenschaften, initiiert haben, betonen den herausragenden Stellenwert von Evalitech für die Technikwissenschaften.

Der Bericht zur „Neuen innovationsorientierten Evaluationsmetrik im Industrie 4.0-Umfeld auf KI-Basis" steht auf der acatech Webseite zum kostenlosen Download zur Verfügung.

Das Projekt wurde vom Bundesministerium für Bildung und Forschung (BMBF) gefördert (Förderkennzeichen 02P17D262).

EU Cyber Resilience Act

Hartmut Rauen, stellvertretender Hauptgeschäftsführer des VDMA am 15. Septenber 2022:

„Die europäische Industrie ist immer häufiger von Cyberangriffen betroffen, die fast ausnahmslos auf Schwachstellen in der Informationstechnik zurückgehen. Produktionsausfälle sind regelmäßig die Folge. Es ist daher richtig, dass die Europäische Kommission jetzt mit dem so genannten Cyber Resilience Act europaweit verpflichtende und einheitliche Vorgaben auf den Weg bringt. Vernetzte Produkte, dazu zählen auch Maschinen und Anlagen, werden in Zukunft nur dann auf dem europäischen Markt zugelassen, wenn diese grundlegende Anforderungen an die Cybersicherheit erfüllen. Damit geht die EU-Kommission in puncto Cybersicherheit aufs Ganze.

Der Vorschlag enthält aus Sicht des Maschinen- und Anlagenbaus viele positive Punkte. Insbesondere das Konzept der eigenverantwortlichen, risikobasierten Umsetzung auf Basis des vielfach erfolgreichen New Legislative Frameworks begrüßt der VDMA ausdrücklich. Auch die klare Abgrenzung zu anderen technischen Re-

gularien, wie der Maschinenverordnung ist geeignet, Doppelanforderungen zu vermeiden.

Problematisch ist allerdings die pauschale Einordnung von Kernkomponenten für vernetzte Maschinen und Anlagen als „kritische Produkte". Diese Generalisierung wird zu unnötigen Mehrbelastungen für die Hersteller führen, da viele Industriekomponenten nur in nicht-kritischen Bereichen eingesetzt werden. Hier würde der Bezug auf die bestimmungsgemäße Verwendung der Produkte helfen.

Entscheidend für den Erfolg des Cyber Resilience Act wird aber die rechtzeitige Verfügbarkeit von harmonisierten Normen sein. Fehlen entsprechende Standards, sind Engpässe bei der Verfügbarkeit zugelassener Produkte unumgänglich. Daher fordern wir die Europäische Kommission auf, frühzeitig entsprechende Normungsmandate zu erteilen, die die Normungsorganisationen im Schulterschluss mit der Wirtschaft zügig annehmen und umsetzen müssen. Die Erarbeitung harmonisierter Normen darf auf keinen Fall verzögert werden."

Alle sieben Minuten ein potenzieller Cyberangriff

CrowdStrike, ein führender Anbieter von Cloud-basiertem Schutz von Endgeräten, Cloud-Workloads, Identitäten und Daten, veröffentlichte am 13. September 2022 seinen vierten jährlichen Threat Hunting Report Nowhere to Hide: 2022 Falcon OverWatch Threat Hunting Report. Der globale Bericht zeigt einen rekordverdächtigen Anstieg von Hands-On-Angriffsversuchen um 50 Prozent im Vergleich zum Vorjahr sowie deutliche Veränderungen bei den Angriffstrends und den Vorgehensweisen der Angreifer. Die Falcon OverWatch Threat Hunter haben mehr als 77.000 potenzielle Angriffsversuche identifiziert, was ungefähr einem Angriffsversuch alle sieben Minuten entspricht. Dabei handelt es sich um Fälle, bei denen durch eine proaktive, von Menschen geleitete, Bedrohungsjagd Angreifer aufgedeckt wurden, die in verschiedenen Phasen der Angriffskette aktiv bösartige Techniken angewendet haben. Dabei setzen sie alles daran, sich den autonomen Erkennungsmethoden zu entziehen.

Falcon OverWatch hat errechnet, dass die Breakout Time (also die Zeit, die ein Angreifer im Durchschnitt benötigt, um von der anfänglichen Kompromittierung zu anderen Hosts innerhalb der Opferumgebung überzugehen) für eCrime-Angreifer auf 1 Stunde und 24 Minuten gesunken ist – im Vergleich zu 1 Stunde und 38 Minuten, die Falcon OverWatch noch für den CrowdStrike Global Threat Report 2022 ermittelte. Darüber hinaus stellte das OverWatch-Team fest, dass bei etwa einem Drittel (30 %) dieser eCrime-Attacken der Angreifer in der Lage war, sich in weniger als 30 Minuten lateral zu bewegen. Diese Ergebnisse unterstreichen die Geschwindigkeit und das Ausmaß, in dem Bedrohungsakteure ihre Taktiken, Techniken und Verfahren (TTPs) weiterentwickeln und in der Lage sind, selbst die fortschrittlichsten technologiebasierten Abwehrsysteme zu umgehen, um ihre Ziele erfolgreich zu erreichen.

„In den letzten 12 Monaten sah sich die Welt mit neuen Herausforderungen konfrontiert, die durch wirtschaftlichen Druck und geopolitische Spannungen ausgelöst wurden und eine Bedrohungslandschaft entstehen ließen, die so kompliziert wie nie zuvor ist", sagt Param Singh, Vice President, Falcon OverWatch bei CrowdStrike. „Um dreiste Bedrohungsakteure auszubremsen, müssen Sicherheitsteams Lösungen implementieren, die zu jeder Tages- und Nachtzeit proaktiv nach versteckten und fortschrittlichen Angriffen suchen. Die Kombination der CrowdStrike Falcon-Plattform mit der Telemetrie, den Werkzeugen, der Threat Intelligence und dem menschlichen Einfallsreichtum der Falcon OverWatch Threat Hunter schützt Unternehmen weltweit vor den raffiniertesten und am schwersten zu erkennenden Bedrohungen."

Weitere wichtige Erkenntnisse aus dem Bericht sind:
eCrime ist hauptverantwortlich für interaktive Einbruchskampagnen. eCrime war für 43 Prozent der interaktiven Einbrüche verantwortlich, während staatliche Akteure 18 Prozent der Aktivitäten ausmachten. Auf Hacktivisten entfielen nur ein Prozent der interaktiven Einbruchskampagnen, während die übrigen Einbrüche nicht zugeordnet werden konnten.

Die Angreifer verlassen sich immer weniger auf Malware. Auf Malware-freie Angriffe entfielen 71 Prozent aller vom CrowdStrike Threat Graph indizierten Entdeckungen. Die Vorherrschaft von Malware-freien Angriffen hängt zum Teil damit zusammen, dass die Angreifer in großem Umfang gültige Anmeldeinformationen missbrauchen, um den Zugang zu und das Verbleiben in den Opferumgebungen zu erleichtern. Ein weiterer Faktor ist die Geschwindigkeit, mit der neue Schwachstellen aufgedeckt werden sowie die Geschwindigkeit, mit der Angreifer in der Lage sind, Exploits zu implementieren.

Die Technologiebranche ist die wichtigste Zielbranche für interaktive Angriffe. Die fünf wichtigsten Zielbranchen sind Technologie (19 %), Telekommunikation (10 %), Fertigung (7 %), Hochschulen (7 %) und das Gesundheitswesen (7 %). Bemerkenswert ist, dass die Technologiebranche beinahe doppelt so oft zum Ziel interaktiver Eindringlinge wurde wie die am zweithäufigsten betroffene Branche.

Der Telekommunikationssektor ist die wichtigste Branche für gezielte Angriffe durch staatliche Akteure. Die fünf wichtigsten Zielbranchen sind Telekommunikation (37 %), Technologie (14 %), Behörden (9 %), Hochschulen (5 %) und Medien (4,5 %). Die Telekommunikationsbranche ist nach wie vor das Ziel staatlich geförderter Überwachungs-, Nachrichten- und Spionageabwehrmaßnahmen. Dabei erfuhr die Telekommunikationsbranche 163 Prozent mehr gezielte Eingriffe durch staatliche Akteure, als die Branche, die am zweithäufigsten ins Visier genommen wurde.

Das Gesundheitswesen befindet sich im Fadenkreuz von Ransomware-as-a-Service (RaaS). Das Volumen der versuchten interaktiven Angriffe auf das Gesundheitswesen hat sich im Vergleich zum Vorjahr verdoppelt. Die überwiegende Mehrheit dieser Einbrüche wird eCrime zugeschrieben.

Der Bericht umfasst die Erkenntnisse der globalen Threat Hunting-Aktivitäten von Falcon OverWatch im Zeitraum vom 1. Juli 2021 bis zum 30. Juni 2022 und enthält detaillierte Angriffsdaten und -analysen, Fallstudien und umsetzbare Empfehlungen.

Hier finden Sie den vollständigen Bericht Nowhere to Hide: 2022 Falcon OverWatch Threat Hunting Report auf der CrowdStrike-Website: *https://www.crowdstrike.com/resources/crowdcasts/nowhere-to-hide-2022-falcon-overwatch-threat-hunting-report/*

Elektronische Unterschrift auf Knopfdruck

Tresorit, der schweizerisch-ungarische Spezialist für Ende-zu-Ende-verschlüsselte („e2ee") Cloud-Kollaboration und Tochtergesellschaft der Schweizer Post, bietet seinen Kunden ab dem 06. Sep-

tember 2022 die Möglichkeit, Dokumente auf Knopfdruck mit elektronischen Unterschriften zu versehen. Die Funktion fügt sich nahtlos in die hochsichere Digital-Workspace-Plattform von Tresorit ein, in der nun auch Unterschriften komfortabel angefordert und entsprechende Dokumente verwaltet werden können. Mit dem neuen Funktionspaket geht das Unternehmen einen weiteren zentralen Schritt hin zu einem umfassenden, geschützten und rechtssicheren Dokumentenmanagement-Workflow, der den gesamten Lebenszyklus sensibler Dokumente integriert in einer Plattform abdeckt.

„Gerade in der heutigen Zeit ist der papierlose Umgang mit Dokumenten zum zentralen Faktor für sichere und effiziente Arbeitsweisen geworden", sagt Tresorit-CEO und Mitgründer István Lám. „In der Praxis bedeutet dies jedoch nicht selten E-Mail-Chaos und Medienbrüche. Mit unserem neuen Funktionspaket können Unternehmen dem ein Ende bereiten. Denn bei ‚Tresorit eSign' handelt es sich nicht um eine zusätzliche Stand-alone-Lösung, sondern eine integrierte Funktion für unsere hochsichere, Ende-zu-Ende-verschlüsselte Workspace- und Cloud-Kollaborationsplattform. So profitieren Kunden doppelt: von maximaler Sicherheit für ihre sensiblen Dokumente bei gleichzeitig höchstmöglichem Komfort für den Praxisalltag."

Die digitale Unterzeichnung von Dokumenten erfolgt bei „Tresorit eSign" in Form der sogenannten „einfachen elektronischen Signatur" („Simple Electronic Signature", SES). Durch sie wird die Unterschrift des Vertragspartners logisch mit dem jeweiligen Dokument verknüpft, um dessen Zustimmung zum Inhalt zu dokumentieren. Im Gegensatz zur qualifizierten elektronischen Signatur sind hierfür keine weiteren Sicherheits- oder Legitimationsnachweise vonnöten.

Per Knopfdruck können zu unterzeichnende Dokumente mithilfe von Tresorit eSign an die jeweiligen Empfänger gesendet werden, die diese daraufhin sichten, unterzeichnen oder – gegebenenfalls mit einem entsprechenden Kommentar versehen – ablehnen können. Der Anwender hat dabei stets im Blick, welche Unterschriften bereits eingegangen sind und welche noch ausstehen. Sämtliche Schritte, von der Dokumentenerstellung bis zur Ablage, sind somit optimal in den Arbeitsalltag integriert.

Da alle zu signierenden Dokumente in der Ende-zu-Ende-verschlüsselten Tresorit-Umgebung aufbewahrt werden, behalten Unternehmen dabei jederzeit die vollständige Kontrolle über diese und ihre vertraulichen Inhalte: Mithilfe gesetzter Berechtigungen lässt sich etwa definieren, wer die jeweiligen Dokumente einsehen und bearbeiten kann oder wie oft und wie lange diese abgerufen werden dürfen. Für lückenlose Rückverfolgbarkeit werden alle Zugriffe detailliert protokolliert.

Weiterer Schritt auf dem Weg zur zentralen Dokumentenmanagementplattform

Mit der Funktionalität für die einfache elektronische Signatur schafft Tresorit auch die Grundlage dafür, künftig auch rechtssichere digitale Signaturen mit Komfort und Benutzerfreundlichkeit zusammenzubringen sowie mittelfristig den kompletten Lebenszyklus vertraulicher Dokumente zu verwalten.

„Eines unserer übergeordneten Ziele besteht darin, das Dokumentenmanagement vollständig zu digitalisieren, von der Erstellung über die Freigabe bis hin zur Unterzeichnung und Archivierung der Dokumente", sagt Lám. „Dazu erweitern wir unsere Plattform nun Schritt für Schritt um integrierte eSignatur-Dienste, die mittelfristig das rechtlich bindende Unterzeichnen von Dokumenten in weniger als einer Minute ermöglichen."
Möglichkeit zum Download findet sich unter *www.tresorit.com/esign*.

Umfrage in DACH zeigt: IT-Sicherheit ist keine Chefsache

Es gibt zahlreiche gute Gründe, die Sicherheit der Daten in Unternehmen und Organisationen strategisch zur Chefsache zu erklären: Angefangen bei einer fortschreitenden Komplexität der Unternehmens-IT, Datenschutzregularien, Homeoffice, mobilem Arbeiten und Einbindung von IOT (Internet of Things) über prominente Cyberattacken auf Großunternehmen oder Einflussnahmen von Hackergruppen auf politische Entwicklungen bis hin zu spezialisierten Cyberangriffen auf kritische Infrastrukturen oder vulnerable Branchen wie das Gesundheitswesen. Dies sind einige willkürlich gewählte Beispiele, die Liste ist lang. Zunehmend wird ergo auch aus Fachkreisen gefordert, den Schutz der Unternehmens-IT zum Managementthema zu machen.

Welche Bedeutung hat das Thema IT-Sicherheit aber tatsächlich ganz oben in den Chefetagen deutscher, österreichischer und Schweizer Unternehmen? Wie hoch schätzen die Unternehmensführungen die Gefahr cyberkrimineller Angriffe ein und welche Folgen für das operative Geschäft aufgrund von Hacker-Attacken erwarten sie am ehesten? Hat die aktuelle weltpolitische Lage einen Einfluss auf Wahrnehmung und Entscheidungen hinsichtlich der IT-Sicherheit?

Diese und eine Reihe weiterer Aspekte wollte das IT-Sicherheitsunternehmen Sophos in einer breit angelegten am 01. September 2022 veröffentlichten Studie herausfinden. Das Meinungsforschungsinstitut Ipsos hat hierfür im Frühsommer dieses Jahres hohe und höhere Führungskräfte (C-Level) in den drei Ländern befragt. IT-Personal wurde hierbei ausdrücklich ausgenommen.

Einige wichtige Erkenntnisse aus der Studie in der Übersicht:

- IT-Sicherheit ist in Deutschland keine Chefsache. Die IT-Abteilungen sind in der Verantwortung. Ein Drittel der Unternehmen setzt auf externe IT-Dienstleistungen.
- Weltpolitische Lage und Krieg haben wenig Einfluss auf das Sicherheits-bewusstsein bei Managerinnen und Managern. Nur ein Drittel sieht durch die aktuelle weltpolitische Lage den Blick für IT-Sicherheit nochmal geschärft.
- Die Chefetagen wiegen sich bei IT-Sicherheit in Sicherheit. Die Mehrheit gibt an, bereits seit längerem gut gewappnet zu sein.
- C-Level-Verantwortliche erwarten insbesondere wirtschaftliche Folgen durch Cyberangriffe. Wiederherstellungskosten oder Störungen der kaufmännischen Abläufe stehen im Fokus. Den Verlust von Kunden und Beschäftigten sowie mögliche Ausfälle im Rahmen der Lieferketten erwarten die wenigsten.
- Unternehmen in Deutschland, Österreich und der Schweiz mit sehr ähnlichen Ergebnissen
- Höher aufgehängt und doch: IT-Sicherheit ist keine Chefsache. Die IT ist in der Pflicht.

Die große Mehrheit der befragten Manager (rund 81 Prozent) gibt an, ein hohes bis sehr hohes Bewusstsein für IT-Sicherheit zu haben. Auch wurde den Angaben aller Befragten zufolge in der Mehrheit der Unternehmen (über 60 Prozent) die IT-Sicherheit innerhalb der zurückliegenden drei Jahre auf eine höhere bzw. die höchste Hierarchieebene angesiedelt.

Hier offenbart sich ein interessanter Widerspruch, denn bei der Frage nach der tatsächlichen Verantwortung für die IT-Sicherheit zeigt sich dann doch ein anderes, durchaus zu erwartendes Bild: Je größer die Unternehmen sind, desto weniger steht die Führungsebene in der Verantwortung. Dies gilt vor allem für Unternehmen

mit mehr als 200 Mitarbeitenden, hier geben nur 1,9 Prozent der Befragten an, dass die IT-Sicherheit auf Geschäftsführungs- bzw. Vorstandsebene angesiedelt ist. Bei kleineren Unternehmen mit bis zu 199 Mitarbeitenden sowie im Handel liegt dieser Wert deutlich höher, hier ist der Chef zu rund 22 Prozent noch höchstpersönlich mit eingebunden.

Die Hauptverantwortung für Cybersicherheit trägt in größeren Unternehmen zu 49,1 Prozent die eigene IT-Abteilung, bei 36,5 Prozent der kleineren Unternehmen sind ebenfalls die eigenen IT-Teams in der Pflicht. Mit 35,8 Prozent bei den größeren sowie 33,1 Prozent bei den kleineren Unternehmen überträgt zudem jeweils ein gutes Drittel aller Unternehmen die Verantwortung für ihre IT-Sicherheit auf externe Dienstleister.

Wenig Ukraine-Effekt: Deutsche Chefetagen wähnen sich in IT-Sicherheit

Selbstverständlich war es Sophos auch ein Anliegen zu erfahren, ob und inwieweit sich angesichts der weltpolitischen Lage und des aktuellen Kriegs in Europa, der bereits weit lange vor der eigentlichen militärischen Auseinandersetzung auf Cyberebene tobte, die Wahrnehmung und Bedeutung von IT-Sicherheit innerhalb der letzten zwei Jahre verändert haben. Hierzu bestätigten 23 Prozent der Befragten aus Unternehmen mit mehr als 200 Mitarbeitenden sowie knapp 36 Prozent aus kleineren Unternehmen, dass Cybersicherheit noch wichtiger geworden sei.

Mehrheitlich jedoch fühlt man sich offenbar ohnehin sehr sicher: 53 Prozent der kleineren und sogar knapp 70 Prozent der größeren Unternehmen geben an, dass sich hinsichtlich des Bewusstseins für das Thema Cybersicherheit in den letzten zwei Jahren nichts verändert habe und man hierfür bereits gut aufgestellt gewesen sei.

Auch in Bezug auf die bestehenden IT-Sicherheitsstrukturen im Unternehmen herrscht Zufriedenheit: 62,2 Prozent geben an, Ihr Unternehmen sei gut bis sehr gut gegen Cyberattacken gewappnet, bei den Entscheidern unter 45 Jahre liegt dieser Wert sogar noch um 2,5 Prozentpunkte höher.

Einen cyberkriminellen Angriff auf ihr Unternehmen halten gut 58 Prozent für wahrscheinlich bis sehr wahrscheinlich, knapp 39 Prozent betrachten diesen Fall als eher unwahrscheinlich.

Cyberattacken-Folgen: Zusatzkosten größte Sorge, Lieferkette und Belegschaft kaum

Mit Blick auf die Folgen eines Cyberangriffs gilt die in deutschen Chefetagen meistgenannte Sorge den dadurch entstehenden Kosten – etwa durch eine notwendige Wiederherstellung des Geschäftsbetriebs. Die möglichen Unterbrechungen der kaufmännischen Abläufe stehen am zweithäufigsten im Fokus.

Ein Interessanter Aspekt hierbei: Probleme im Rahmen der Lieferketten vermuten insgesamt noch weniger Befragte (23 Prozent) als einen möglichen Imageverlust (28 Prozent). Allein im verarbeitenden Gewerbe, und das ist keine große Überraschung, gehen immerhin insgesamt knapp 37 Prozent der Befragten davon aus, dass die Lieferketten möglicherweise betroffen sein könnten.

Dem Verlust von Kunden oder Beschäftigten als Folge von Cyberattacken messen die Führenden hingegen kaum bis keine Bedeutung bei: Mit Kundenverlusten rechnen 19,4 Prozent und noch weniger (1,5 Prozent) befürchten, Mitarbeitende zu verlieren.

Auch Zahlungsunfähigkeit (9,5 Prozent) und Bußgelder wegen Datenschutzverletzungen (5,5 Prozent) werden kaum als Risiken gesehen, lediglich in der Schweiz regt sich hier etwas mehr Sorge: hier erwarten knapp 22 Prozent eine Zahlungsunfähigkeit sowie 11,8 Prozent Bußgeldzahlungen als mögliche Folgen von Cyberattacken.

Chester Wisniewski: International (leider) ein ähnliches Bild

„Die Ergebnisse in der DACH-Region sind zwar enttäuschend, entsprechen aber dem, was wir in Nordamerika, ASEAN und anderen Regionen beobachten", kommentiert Chester Wisniewski, Principal Research Scientist bei Sophos die Ergebnisse der Studie. „Leider wird die Sicherheit, wenn sie als Bestandteil der IT verwaltet wird, in der Regel auf den Status einer Aufgabe zurückgestuft, anstatt eine Priorität zu sein. Die Rolle des Sicherheitsteams besteht darin, Risiken zu identifizieren und dem Vorstand dabei zu helfen, diese Risiken nach Prioritäten zu ordnen, wohingegen die IT-Abteilung die Aufgabe hat, die erforderlichen Änderungen zu implementieren, je nachdem, wie diese Risiken angegangen werden sollen."

Auch, was die Bedeutung der IT-Sicherheit vor dem Hintergrund der weltpolitischen Lage angeht, scheint für weltweit einhellige Gelassenheit zu sorgen. Wisniewski: „Der Krieg in der Ukraine hat die Einstellungen nicht wirklich verändert, abgesehen von den kritischen US-Infrastrukturen. Die US-amerikanische CISA-Agentur hat ihre Bemühungen zur Verbesserung des Sicherheitsbewusstseins und in einigen Fällen der Meldepflichten für Anbieter kritischer Infrastrukturen verstärkt, aber außerhalb der USA oder in anderen Unternehmen des privaten Sektors sind keine großen Bedenken oder Maßnahmen zu erkennen."

BlackBerry-Studie: Bei smarten Geräten ist vielen der Preis wichtiger als die Cybersicherheit

BlackBerry, ein führender Anbieter von Sicherheitsservices und -dienstleistungen für das IoT, hat am 08. September 2022 eine Studie veröffentlicht, die das Cybersecurity-Risiko aufzeigt, das von Mitarbeitern im Homeoffice ausgeht: In Deutschland haben für 70 Prozent der Käufer von intelligenten Haushaltsgeräten der Preis, die Benutzerfreundlichkeit und die einfache Einrichtung der Geräte Vorrang vor der Sicherheit. Hinzu kommt, dass etwa jedes sechste Unternehmen keinerlei angemessene Sicherheitsvorkehrungen trifft, um die Cybersicherheit auf den privaten Bereich auszudehnen. Zusammen erhöht dies das Risiko von Cyberangriffen für Unternehmen und ihre Mitarbeiter, insbesondere vor dem Hintergrund, dass hybride Arbeitsmodelle und Homeoffice mittlerweile die Norm sind.

Die Umfrage wurde unter 1.000 Teilnehmern, die Deutschland im Homeoffice arbeiten, durchgeführt. Laut der Erhebung geben 17 Prozent der Befragten an, ihr Arbeitgeber habe nichts zum Schutz ihres Heimnetzwerks oder ihrer intelligenten Geräte unternommen oder dazu etwas kommuniziert, und dass sie nicht wissen, ob diese überhaupt geschützt sind. Darüber hinaus gaben fast Dreiviertel der Befragten an, dass ihr Arbeitgeber keine Maßnahmen zur Sicherung der privaten Internetverbindung (74 Prozent) oder zum Schutz von Privatgeräten mittels Software (72 Prozent) ergriffen hat. Die fehlende Ausweitung der Netzwerksicherheit auf private Geräte erhöht das Risiko, dass die durch hybrides und privates Arbeiten entstandenen Schwachstellen erfolgreich ausgenutzt werden. Dabei sind Unternehmen laut des BlackBerry Threat Report 2022 täglich mit bis zu elf Cyberangriffen pro Gerät konfrontiert, was einen rundum Schutz umso wichtiger macht. In Deutschland verlassen sich 33 Prozent der Unternehmen lediglich auf die

Sicherheit von Virtual Private Networks (VPN), die jedoch mit der heutigen Bedrohungslage nicht mithalten können.

„Die Zunahme ungesicherter intelligenter Geräte in Europa bietet eine verheerende Angriffsfläche für Cyberangreifer", sagt Hans-Peter Bauer, Senior Vice President EMEA, BlackBerry Cybersecurity. „Wenn Verbraucher weniger wachsam sind und Unternehmen ihre Sicherheitsvorkehrungen nicht ausbauen, werden Cyberkriminelle jeden ungesicherten Zugangspunkt verstärkt ausnutzen."

Selbst über scheinbar harmlose Geräte können Kriminelle auf Heimnetzwerke zugreifen, die mit Unternehmensgeräten verbunden sind und so die Gelegenheit nutzen, um wertvolle Daten und geistiges Eigentum zu stehlen. Da die Cybersicherheit von smarten Geräten für Käufer weit hinter dem Preis rangiert und der Schutz von Smart-Home-Geräten durch den Arbeitgeber nur von wenigen in Anspruch genommen wird, öffnet sich Tür und Tor für Cyberkriminelle, die sich den Boom bei intelligenten Geräten im Haushalt zunutze machen.

„Die aktuellen Bedingungen erschweren die Umsetzung effektiver Arbeitspraktiken in hybriden oder Homeoffice-Umgebungen in Haushalten, die zwar immer intelligenter, aber nicht unbedingt cybersicherer werden. Daher ist es von entscheidender Bedeutung, dass Unternehmen die Geräte außerhalb ihrer unmittelbaren Reichweite nicht vergessen, wenn sie über ihren Cybersecurity-Schutz nachdenken und sich auf die kommenden schwierigen wirtschaftlichen Zeiten vorbereiten", ergänzt Bauer.

Weitere Informationen darüber, wie die umfassenden, präventionsorientierten und KI-gesteuerten Cybersicherheitslösungen von BlackBerry Ihr Unternehmen bei der Vorbereitung auf Cyberbedrohungen sowie bei der Prävention, Erkennung und Reaktion darauf unterstützen können, finden Sie hier: *https://www.blackberry.com/us/en/products/blackberry-cyber-suite*

Eine neue Arbeitswelt, ein neuer Sicherheitsansatz: Der Nutzer im Mittelpunkt

Als Mitarbeiter noch jeden Tag im Büro auf verwalteten Geräten arbeiteten, verfolgten IT-Abteilungen ein klares Sicherheitsziel: Angreifer mussten aus dem Unternehmensnetzwerk ausgesperrt werden. Dies funktioniert heute jedoch nicht mehr wie bisher, denn die Mitarbeiter arbeiten zunehmend an Orten und Geräten ihrer Wahl. Um diese Flexibilität sicher zu gewähren und dabei die Unternehmensressourcen erfolgreich zu schützen, müssen IT-Verantwortliche das Thema Sicherheit ganz neu denken: Nämlich von den Mitarbeitern her. Wie dies gelingt, zeigte am 07. September 2022 Saša Petrovic, Digital Strategy Director bei Citrix.

Ob zu Hause, unterwegs oder am Urlaubsort – der Workation etabliert sich zunehmend als Option, um Erholung und Arbeit miteinander zu verbinden: Arbeit kann heute nahezu überall stattfinden. Gerade für viele Wissensarbeiter sind häufig nur noch Internet- und Stromzugang entscheidend, um den Laptop aufzuklappen und loslegen zu können. Und Mitarbeiter erwarten vielerorts inzwischen genau dieses Maß an Flexibilität, das sich bis auf die verwendeten Geräte und Anwendungen erstreckt.

Für Unternehmen ergibt sich aus dieser Situation eine Herausforderung: Sie müssen diese Flexibilität sicher und zuverlässig ermöglichen, notwendige Sicherheitsmaßnahmen und -kontrollen dürfen aber nicht auf Kosten der Nutzererfahrung gehen. Die Verantwortlichen müssen ein Gleichgewicht finden und dafür ihren Sicherheitsansatz modernisieren.

Ständige, unsichtbare Kontrollen

Zunächst ist es aber entscheidend, IT-Sicherheit als elementaren, geschäftskritischen Bestandteil des Unternehmens zu verstehen und zu führen. Das heißt, Risiken werden in Zahlen bewertet und diese den Stakeholdern kommuniziert. Im Anschluss lässt sich festlegen, wofür und wie die vorhandenen Ressourcen – Zeit, Geld, Personal – eingesetzt werden sollten. In einem Unternehmen, in dem Mitarbeiter hybrid oder gänzlich remote arbeiten, sollten sie genutzt werden, um eine moderne Zero Trust Network Access (ZTNA)-Sicherheitsarchitektur aufzubauen.

Diese bietet zwei große Vorteile: Zum einen wird der Nutzerzugriff zu Unternehmensressourcen auf Grundlage des aktuellen Kontextes gewährt (oder blockiert). Zum anderen werden das Benutzer-, Anwendungs- und Netzwerkverhalten kontinuierlich überwacht, Sicherheitsrichtlinien dynamisch durchgesetzt und bei Bedarf zusätzliche Sicherheitskontrollen durchgeführt. Es gilt das Prinzip „Never trust, always verify".

Umsetzen lässt sich Zero Trust beispielsweise mithilfe einer cloudbasierter Desktop-as-a-Service (DaaS)-Lösung, denn IT-Security ist ein integrierter Bestandteil von DaaS. Damit können IT-Abteilungen beispielsweise:

- Einen vertrauenswürdigen Netzwerkzugriff auf alle genehmigten Anwendungen mit adaptiver Authentifizierung bereitstellen, unabhängig davon, ob diese On-Premises oder in der Cloud genutzt werden. Der Zugriff wird hier kontinuierlich auf Grundlage von Endnutzerrollen, Standorten, Gerätestatus und Nutzerrisikoprofilen bewertet und reguliert.
- Verteiltes Arbeiten und die Nutzung verwalteter, nicht verwalteter und privater Geräte sicher unterstützen und Sicherheitskontrollen durchführen.
- Die IT vereinfachen und gleichzeitig die User Experience mithilfe von KI und ML für die Mitarbeiter verbessern. So kann die Notwendigkeit zur Authentifizierung durch die ständige Bewertung des Risikos minimiert werden.

Sicherheit für die Zukunft der Arbeit

Die Umstellung auf hybride und remote Arbeitsmodelle ist im vollen Gange und nimmt immer mehr an Geschwindigkeit auf. Die Gewinner dieses Rennens werden Unternehmen sein, die ihren Mitarbeitern ein sicheres und konsistentes Arbeitserlebnis bieten können, und das über jeden Arbeitskanal, jedes Gerät hinweg und an jedem Ort. Das Ergebnis: motivierte, engagierte und produktive Mitarbeiter, die in einer selbst gewählten Arbeitsumgebung ihre beste Leistung bringen können. Gleichzeitig werden Unternehmenswerte und -ressourcen optimal geschützt. Damit profitieren am Ende beide Seiten von einem modernen, auf ZTNA-basierten Sicherheitsansatz.

Cybersicherheit im Gesundheitswesen: Risiken und Nebenwirkungen fehlender Sicherheitsmaßnahmen

Cyberattacken im Gesundheitsbereich können schwerwiegende Konsequenzen mit sich bringen. Laut dem aktuellen State of Email Security Report von Mimecast, einem der führenden Anbieter für

Daten- und E-Mail-Sicherheit, bemerkten 71 % der befragten deutschen Unternehmen aus dem Gesundheitsbereich einen Anstieg an bedrohlichen E-Mails im vergangenen Jahr. Vor allem das Gesundheitswesen muss sich besser gegen Bedrohungen aus der digitalen Welt schützen – denn hier blüht den Opfern mehr als Reputations- oder monetäre Verluste: Im schlimmsten Fall leidet die menschliche Gesundheitsversorgung durch die Machenschaften von Cyberkriminellen. Für Hacker ist das Gesundheitswesen ein äußerst lohnendes Ziel: Zum einen ist die IT-Infrastruktur in vielen Krankenhäusern und Gesundheitseinrichtungen veraltet und das Sicherheitsbudget oft eher knapp bemessen. Zum anderen wird hier eine Vielzahl sensibler, personenbezogener Daten erzeugt und verarbeitet – für Hacker also eine wahre Goldgrube.

Gefahren durch Ransomware, Phishing und unvorsichtige Mitarbeiter:innen

Ransomware-Angriffe im Gesundheitswesen können besonders schwerwiegende Konsequenzen nach sich ziehen: Sie sind in der Lage, Systeme zu sperren, die einen Einfluss auf das menschliche Leben haben – beispielsweise medizinische Geräte zur Überwachung von Patientenzuständen. Zudem können sie den Zugriff auf wichtige Patientendaten verschlüsseln. Die Attacke auf die Münchner Caritas ist hier nur das jüngste Beispiel. Die Organisation rechnet mit erheblichen Beeinträchtigungen, die wohl bis weit über eine Woche andauern werden. Umso gravierender ist es, dass 66 % der in der Studie befragten Organisationen im vergangenen Jahr eine Beeinträchtigung ihrer Geschäftsabläufe im Zuge einer Ransomware-Attacke erlebten. Die Ausfallzeit betrug dabei im Schnitt 5,7 Tage – im Ernstfall kann das lebensbedrohliche Konsequenzen für die Patient:innen bedeuten.

Aber nicht nur Ransomware treibt ihr Unwesen im Gesundheitsbereich. 63 % der Teilnehmer:innen bemerkten einen Anstieg an Phishing und ungefähr die Hälfte der Befragten gibt an, einen Missbrauch der Unternehmensmarke durch Spoofing-E-Mails festgestellt zu haben. Allerdings verfügen lediglich 42 % über ein E-Mail-Sicherheitssystem, welches Malware oder infizierte Links aufspürt.

Als Haupteinfallstor gelten jedoch nach wie vor unbedachte Handlungen der Mitarbeiter:innen selbst. 84 % der Befragten halten es für wahrscheinlich, dass die Angestellten einen schwerwiegenden Sicherheitsfehler im persönlichen Umgang mit E-Mails begehen. Zudem befürchten 84 % bzw. 79 %, dass es aufgrund mangelnder Passworthygiene oder durch unbeabsichtigte Datenlecks der Mitarbeiter:innen zu einem ernsthaften Sicherheitsfehler kommen könnte.

Methoden zum Schutz von Gesundheitsorganisationen

1. **Erhöhung der Cyber-Resilienz**
   Durch das akute Bedrohungsszenario ist eine ausgereifte Cyber-Resilienz-Strategie eines der bewährtesten Mittel, um Hackern dauerhaft standzuhalten – allerdings verfügen aktuell nur 32 % der Gesundheitsorganisation über adäquate Sicherheitsstrategien. Im Kern sichert eine Cyber-Resilienz-Strategie den Weiterbetrieb der Geschäftsabläufe – beispielsweise durch den kontinuierlichen Zugriff auf E-Mails und weitere Systeme – und beinhaltet Abwehr- und Gegenmaßnahmen bei Cyberangriffen.
2. **Ausbau der Cloud-Infrastruktur**
   Gerade im Gesundheitswesen fallen Unmengen an sensiblen Daten an, die sicher gelagert und jederzeit abrufbar sein müssen. Die Nutzung der Cloud ist einerseits extrem anwenderfreundlich, da die Prozesse automatisiert im Hintergrund geschehen. Andererseits optimiert die Archivierung von Daten in der Cloud Kosten und senkt gleichzeitig die Risiken für die internen Rechts- und Compliance-Teams.
3. **Einsatz von Künstlicher Intelligenz und Maschinellem Lernen**
   Eine schnelle Reaktion auf Cyberattacken kann im Gesundheitswesen im Ernstfall Leben retten – beispielsweise, wenn Kriminelle lebenserhaltende Geräte unter ihre Kontrolle bringen wollen (oder dies bereits geschafft haben). Die Hälfte der befragten Gesundheitsorganisationen nutzt schon KI oder ML – weitere 34 % planen eine Integration bereits in diesem Jahr. Sicherheitslösungen, die auf Künstlicher Intelligenz und Maschinellem Lernen basieren, können Gefahren weitaus schneller identifizieren, als es menschlichen Sicherheitsteams möglich wäre.
4. **Regelmäßige Security-Awareness-Trainings**
   Durch Sicherheitstrainings werden die Mitarbeiter:innen hinsichtlich verschiedener Cybergefahren sensibilisiert – und sind somit weniger anfällig, Hackern ins Netz zu geraten. 37 % der Befragten trainiert die Mitarbeiter:innen regelmäßig darauf, Cyberattacken zu identifizieren. Als bevorzugte Methode nutzen davon 66 % Gruppentrainings mit internen IT-Teams.
5. **Integration einer mehrschichtigen Sicherheitsarchitektur**
   Den besten Schutz gegen die kontinuierlich steigenden Cyberrisiken stellt eine mehrschichtige Sicherheitsstrategie dar, also eine Kombination unterschiedlicher Methoden. In jedem Fall sollte darauf verzichtet werden, lediglich ein einziges Sicherheitsprodukt zu verwenden. Externe Dienstleister wie Mimecast bieten in der Zusammenarbeit mit Partnern über APIs maßgeschneiderte Lösungen, die einfach zu integrieren und dabei besonders benutzerfreundlich sowie effektiv sind. 95 % der Gesundheitsorganisationen geben an, dass es bei der Auswahl eines Sicherheitsdienstleisters einen Einfluss habe, ob dieser über eine offene API-Plattform verfügt.

„Krankenhäuser und andere Pflegeeinrichtungen müssen rund um die Uhr funktionieren, um die Gesundheit ihrer Patient:innen gewährleisten zu können. Die Aufrechterhaltung des Geschäftsbetriebs hat daher höchste Priorität", sagt Bernd Hohlweg, Director Marketing DACH bei Mimecast. „Cyberattacken bedrohen zunehmend diesen Auftrag – und im schlimmsten Fall Patientenleben. Nur die Entwicklung einer robusten Cyber-Resilienz-Strategie und die Implementierung mehrerer Sicherheitsebenen schützen Organisationen zuverlässig vor Cyberangriffen und stellen den Betrieb und die Patientenversorgung im Falle eines Angriffs sicher."

Den zugehörigen Blogartikel, inklusive globaler Statistiken, finden Sie hier: *https://www.mimecast.com/de/blog/10-cybersecurity-best-practices-for-healthcare/*

BSI stellt Automotive-Lagebild 2021/2022 vor

Die Digitalisierung moderner Autos schreitet weiter schnell voran. Mitunter sind über 100 einzelner digitaler Steuerungsgeräte in heutigen Autos verbaut, die miteinander verbunden sind oder zentral gesteuert werden können. Durch das autonome Fahren und den Einsatz Künstlicher Intelligenz wird die Komplexität der Software-Architektur in Fahrzeugen weiterhin rasant zunehmen. Und auch die Unternehmen selbst sind mehr denn je auf sichere IT-Systeme angewiesen. Dies stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in der zweiten Ausgabe seines Branchenlagebilds Automotive vom 19. September 2022 fest.

BSI-Präsident Arne Schönbohm: „Das BSI gestaltet Informationssicherheit in der Digitalisierung für Staat, Gesellschaft und auch Wirtschaft. Die Automobilindustrie nimmt dabei auf Grund ihrer volkswirtschaftlichen Bedeutung und ihrer umfangreichen Lieferketten eine besondere Stellung ein. Mit dem Lagebild Automotive 2021/22 wird einmal mehr deutlich, dass Cyber-Sicherheit in allen Gliedern der Lieferkette mitgedacht werden muss – von Anfang an bis zum fertigen Produkt. Cyber-Sicherheit ist der Schlüssel für eine funktionierende Automobilindustrie."

Das Branchenlagebild Automotive 2021/2022 ist die zweite Ausgabe eines branchenspezifischen Überblicks aus Sicht des BSI zur Lage der Cyber-Sicherheit im Bereich „Automotive", sowohl hinsichtlich der Produktion, als auch der Fahrzeuge selbst. Es macht deutlich, dass künftige Automobile noch viel stärker als heute schon von IT-Funktionen abhängig sein werden. Die Steuerung des Fahrzeugs selbst, aber auch die Vernetzung mit der Infrastruktur (car-to-x) wird rasant digitalisiert. So wurde in Deutschland im vergangenen Jahr die weltweit erste Genehmigung für ein automatisiertes KFZ (Spurhaltesystem) erteilt. Daher ist es aus Sicht des BSI von besonderer Bedeutung, dass die dazu notwendigen, neuen Technologien nicht manipulierbar sein dürfen und mögliche Cyber-Angriffe keinen Einfluss auf die Fahrsicherheit haben dürfen. Das BSI begrüßt daher, dass die Hersteller Cyber-Sicherheit frühzeitig im Entwicklungszyklus neuer Fahrzeugmodelle berücksichtigen und die Umsetzung nach EU-Typgenehmigungsrecht auch nachweisen müssen.

Im Berichtszeitraum waren erneut mehrere Automobilzulieferer von Ransomware-Vorfällen betroffen. Dadurch kam es bei den Betroffenen zu massiven Unterbrechungen der Leistungserbringung. Die durch das BSI grundsätzlich festgestellte Tendenz, dass Dritte mittelbar ebenfalls von IT-Sicherheitsvorfällen in Mitleidenschaft gezogen werden, bestätigt sich auch hier. So war auch ein weltweit führender Automobilhersteller von Ransomware-Angriffen bei Zulieferern betroffen und musste seinerseits seine Produktion drosseln. Im Hinblick auf die operative Cyber-Sicherheit in den Betrieben stellen Ransomware-Angriffe aus Sicht des BSI aktuell die größte Bedrohung dar. Neben den bestehenden Auswirkungen der COVID-19-Pandemie, insbesondere in den Bereichen von Zulieferteilen, -produkten oder –dienstleistungen, wird die Lage maßgeblich durch den Krieg in der Ukraine und den damit verbundenen wirtschaftlichen, aber zunehmend auch cyber-sicherheitsrelevanten Auswirkungen auf die deutsche Automobilindustrie geprägt. Dies sind u. a. Verfügbarkeitsangriffe auf Webseiten durch DDoS-Angriffe sowie intensive Hacktivisten-Aktivitäten.

Um die Cyber-Sicherheit für den Wirtschafts- und Automobilstandort Deutschland zu erhöhen, arbeitet das BSI in Fragen der Cyber-Sicherheit eng mit dem Kraftfahrtbundesamt (KBA), dem Verband der Automobilindustrie (VDA) sowie weiteren Behörden und aus der Wirtschaft betroffenen Unternehmen zusammen.

NIS-2 setzt Unternehmen unter Druck: Abwarten? Funktioniert nicht!

KOMMENTAR von Bernhard Kretschmer, Vice President Services und Cybersecurity bei NTT Ltd.

Deutsche Unternehmen stehen massiv unter Druck: Der Gesetzgeber verschärft Stück für Stück die Sicherheits- und Compliance-Auflagen, etwa im KRITIS-Bereich mit § 8a Absatz 1a BSIG. Dieser verpflichtet die betroffenen Organisationen, adäquate Systeme zur Angriffserkennung bis spätestens Mai 2023 umzusetzen. Und ein Ende ist nicht in Sicht – denn mit NIS-2 steht eine Richtlinie vor der Tür, die für etliche Unternehmen Konsequenzen haben wird, derer sie sich vermutlich nicht einmal annähernd bewusst sind. Fakt ist, viele Firmen setzen nur symbolische Maßnahmen im Bereich der Cybersicherheit um und nur wenige überprüfen regelmäßig die Wirksamkeit dieser Lösungen. Angesichts der zunehmenden Abhängigkeit von funktionierenden IT-Umgebungen und der Tatsache, dass die Kriminellen immer raffinierter vorgehen, ist ein geringes Schutzniveau jedoch geradezu fahrlässig.

Eben diese Laissez-faire-Haltung in der Abwehr von Hackerangriffen, die verstärkt durch die Corona-Pandemie und den Ukraine-Krieg die Diskussion über die europäische Sicherheitsstrategie bestimmt, will die EU-Kommission mit der Neufassung der NIS-Richtlinie eindämmen. Es sollen EU-weite Standards für Cybersecurity definiert werden, die nun auch die Industrie verpflichtend umsetzen muss. Dadurch soll die gesamte Infrastruktur resilienter werden. So werden Unternehmen nicht mehr vor die Wahl gestellt – nein, sie müssen einen Mindeststandard an Sicherheit erfüllen.

Und diese Pflicht trifft künftig viel mehr Firmen als bisher. Einerseits hat die EU die Richtlinie auf zahlreiche weitere Branchen mit Versorgungsfunktionen ausgeweitet. Die Vorgaben schließen künftig etwa Anbieter öffentlicher elektronischer Kommunikationsdienste und digitaler Dienste, die Abwasser- und Abfallwirtschaft, Hersteller kritischer Produkte, Post- und Kurierdienste und die öffentliche Verwaltung sowohl auf zentraler als auch regionaler Ebene ein, wobei die Kommission zwischen Marktteilnehmern mit einer entscheidenden und mit einer essenziellen Bedeutung für Wirtschaft und Gesellschaft unterscheidet. Ferner können die Mitgliedstaaten beschließen, dass sie auch für einschlägige Stellen auf kommunaler Ebene gelten. Außerdem werden nun auch Betriebe mit über 250 Mitarbeitern und über zehn Millionen Jahresumsatz als schützenswert eingestuft und müssen künftig Cybersicherheitsstandards wie Audits, Risikoabschätzungen, das zeitnahe Einspielen von Sicherheitsupdates und Zertifizierungen beachten.

Die Umsetzung von NIS-2 stellt die Industrie jedenfalls vor zahlreiche Herausforderungen. Ein Beispiel sind die Meldefristen: Innerhalb von 24 Stunden nach Kenntnisnahme des Sicherheitsvorfalls muss eine erste Meldung als Frühwarnung bei den zuständigen Behörden eingehen. In dieser wird angegeben, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist. Innerhalb von 72 Stunden muss dann ein weiterer Bericht ausgehändigt werden, der die sogenannten Indicators of Compromise beschreibt und der ohne dediziertes Security-Knowhow zu einer fast unlösbaren Aufgabe wird. Spätestens einen Monat nach dem Vorfall ist schließlich noch ein Abschlussbericht fällig, der mindestens eine ausführliche Beschreibung des Sicherheitsvorfalls, seines Schweregrads und seiner Auswirkungen sowie Angaben zur Art der Bedrohung und den getroffenen Abhilfemaßnahmen beinhalten muss. Wer schon einmal ein Unternehmen direkt nach einer Hackerattacke erlebt hat, weiß, wie groß einerseits das Chaos ist und wie knapp andererseits Ressourcen und Zeit sind. Vor allem im Mittelstand ist davon auszugehen, dass die Expertise für die Umsetzung der Richtlinie im Haus nicht vorhanden ist.

Viel Zeit zum Umsetzen bleibt übrigens nicht. Die Verhandlungen sind seit Mai 2022 abgeschlossen, jetzt muss das EU-Parlament den Entwurf mit einem Mehrheitsvotum absegnen, was als reine Formalität gilt und bis Ende des Jahres über die Bühne gehen sollte. Sobald das passiert ist, haben die EU-Mitgliedsstaaten 21 Mona-

te Zeit, die Richtlinie umzusetzen. Wenn man bedenkt, dass manche Hardwarekomponenten derzeit eine Lieferfrist von bis zu eineinhalb Jahren haben, ist der Zeitrahmen, um ein adäquates Sicherheitspaket zu schnüren, mehr als knapp bemessen.

Trotzdem: Eine schlechte oder gar nicht vorhandene Security-Lösung kostet am Ende deutlich mehr als eine gute. Den Mehrwert sehen viele leider erst, wenn sie tatsächlich angegriffen wurden und Produktionsausfälle zu finanziellen Schäden führen. Jedes Unternehmen tut also gut daran, seine Schutzmaßnahmen zu überdenken. Die NIS-2-Richtlinie verschärft sowieso die Ausgangslage – die Behörden können bei Nichteinhaltung der Empfehlungen zum Risikomanagement analog zur DSGVO erhebliche Geldstrafen verhängen. Nach derzeitigem Kenntnisstand müssen Betreiber entscheidender Dienste mit Geldbußen in Höhe von 2 Prozent des Jahresumsatzes rechnen, Anbieter essentieller Services mit 1,4 Prozent. Hinzu kommt: Die Unternehmensführung wird für etwaige Verstöße in Verantwortung genommen und ist damit haftbar.

Rezensionen

Bücher

Thilo Weichert

Knüppel, Kai-Niklas: Datenfinanzierte Apps als Gegenstand des Datenschutzrechts, Duncker & Humblot Berlin, 2022, ISBN 978 3 428 18665 5, 417 S., 109,90 €

Das Phänomen datenfinanzierter Apps ist in der digitalen Realität allgegenwärtig. Dessen datenschutzrechtliche Bewertung war schon bisher immer wieder Gegenstand der rechtlichen, praktischen, ökonomischen und soziologischen Erörterung. Knüppel legt mit seiner 2021 eingereichten datenschutzrechtlichen Dissertation nun eine sehr konsistente Darstellung des aktuellen Diskussionsstands vor. Diese ist durch Aktualisierungen bis April 2022 auch sehr aktuell und bezieht z.B. das Ende 2021 erfolgte Inkrafttreten des Telekommunikations-Telemedien-Datenschutzgesetzes (TTDSG) mit ein. Die Anfang 2022 umgesetzte Digitale-Inhalte-Richtlinie der EU wird berücksichtigt.

Angesichts der Komplexität des Themas ist zunächst auf einige Restriktionen hinzuweisen, denen sich der Autor selbst unterworfen hat: Wir haben es hier mit einer ausschließlich rechtsdogmatischen Arbeit zu tun, in der soziale und wirtschaftliche Aspekte allenfalls am Rande erwähnt werden und technisch-organisatorische Sicherungen nicht im Fokus stehen. Die Realität der Datenverarbeitung wird beschrieben, aber nur soweit sie für die rechtliche Darstellung nötig ist. Die rechtliche Analyse erfolgt generisch, also ohne – abgesehen von den ganz Großen wie z.B. Google oder Facebook – Nennung von Unternehmensnamen. Als Ersatz werden in kurzen instruktiven Beispielsabsätzen eine „Navigations-App A" und eine „Messenger-App B" dargestellt und erörtert.

Der Autor macht mit seiner Doktorarbeit einen in diesem Genre weit verbreiteten „Fehler", den man bei der interessierten Lektüre überspringen könnte: Er lässt sich ausführlich über „die Grundlagen des Datenschutzrechts" und über die „Grundsätze und Prinzipien des Datenschutzes" aus. Derartiges kann an vielen Stellen nachgelesen werden und sollte in einer Dissertation nur soweit auftauchen, wie es eine praktische Relevanz für das Thema hat. Dessen ungeachtet: Auch hier wie auch später bei der titelspezifischen Bearbeitung ist der Autor äußerst präzise und klar.

Die Stärke der Arbeit liegt in der dogmatischen durchgängig grundrechtsfreundlichen und zugleich sehr pragmatischen Durchdringung des Themas. Er beschreibt die Offenheit der Zweckfestlegungen im – hier anwendbaren – privaten Bereich. Er behandelt die Rechtsgrundlagen – insbesondere „Vertrag" und „Einwilligung" und als Zwischenstücke das Koppelungsverbot und den Wechsel der Rechtsgrundlagen. Dabei vertritt er die weit geteilte Ansicht, dass Einwilligungen eine zentrale Rechtsgrundlage sein können und korrekterweise, dass der Einwilligungswiderruf zwangsläufig zur Unzulässigkeit der weiteren Verarbeitung führt. Beim Koppelungsverbot nach Art. 7 Abs. 4 DSGVO plädiert er – sehr pragmatisch – für eine Güterabwägung. Er weist die weit verbreitete Ansicht mit guten Argumenten zurück, die DSGVO sei zu paternalistisch.

Die Abstraktheit der Darstellung führt dazu, dass die Übertragbarkeit der Ausführungen auf die digitale Realität zu kurz kommt. So behandelt der Autor etwa die Verarbeitungszwecke so allgemein, dass sich dahinter verbergende konkrete Zwecke und Verarbeitungen nicht klar erschließen. So lassen sich kommerzielle Zwecke, um die es hier ausnahmslos geht, differenzieren nach Werbung, Kundenbindung, Markterforschung, politische Beeinflussung… Diese Konkretisierungen werden aber, obwohl sie abwägungsrelevant sind, nicht durchdekliniert, sondern nach drei sehr groben Kategorien eingestuft: I Sofortnutzung von Daten, II Speicherung und spätere Nutzung, IIIa Offenlegung im Konzern sowie IIIb an Dritte. Bei der Kategorie III wird grundsätzlich – richtig – ein berechtigtes Interesse zurückgewiesen. Doch bleiben die abstrakten Lösungsansätze – etwa der Hinweise auf Anonymisierung und Pseudonymisierung – weit hinter den z.B. in der Internetwerbung zu findenden Praktiken von wirksamer Aggregierung einerseits bis zum hochdifferenzierten Real-Time-Bidding oder zu Auswertungen à la Deep Learning andererseits unerwähnt. Komplexität wird vielmehr unter dem unpräzisen Begriff „Big Data" abgehandelt. Ein weiteres, weniger entschuldbares Defizit besteht darin, dass das Thema „sensitive Daten" (Art. 9 DSGVO) nicht einmal angerissen wird, wo doch gerade hier in der Praxis gewaltige – in Zukunft sicher zunehmende – Probleme bestehen.

Der Autor beschreibt praktische Defizite und Probleme bei datenfinanzierten Apps – von fehlender Transparenz über das sog. Datenschutzparadox bis hin zum Einsatz von Marktmacht. Und er macht am Schluss der Arbeit praktische Vorschläge. So kann er sich vorstellen bei datenfinanzierten Apps eine rechtliche Pflicht zur geldfinanzierten verarbeitungsfreien Alternative einzuführen. In Bezug auf Transparenzdefizite vertieft er das Thema „One-Pager" und „Icons".

Die Argumentation der Doktorarbeit ist klassisch und dabei gut nachvollziehbar, indem Ansicht und Gegenansichten dargestellt werden, um am Ende in eine gut begründete, manchmal meinungsstarke eigene Position zu münden. Die Sprache ist präzise und – für Juristen – gut verständlich. Übersichtlichkeit besteht durch viele aussagekräftige Überschriften und ein dementspre-