Redaktion: Helmut Reimer

Report

Confidential Computing Consortium: Datenschutz und Digitalisierung kein Widerspruch

Unternehmen, Krankenhäuser, Schulen und Behörden stehen vor einem Dilemma: Auf der einen Seite lassen sich die aktuellen und zukünftigen Herausforderungen nur durch eine weitgehende Digitalisierung und Vernetzung meistern. Auf der anderen geraten dadurch immer größere Lebensbereiche in Gefahr, von Datendiebstahl oder -missbrauch betroffen zu sein. Die gesetzlich verbrieften Rechte auf informationelle Selbstbestimmung und Privatsphäre müssen auf der einen Seite gewahrt bleiben, dürfen den Fortschritt jedoch auch nicht ausbremsen.

Technologieanbieter wie Intel, IBM und Microsoft haben sich deshalb gemeinsam mit der Linux Foundation zum Confidential Computing Consortium (CCC) zusammengeschlossen. Ziel des CCC ist es eine sichere Infrastruktur zu schaffen, welche die Vertraulichkeit von Daten entlang der gesamten Verarbeitungskette garantiert. Ein wesentlicher Bestandteil ist dabei eine vertrauenswürdige Laufzeitumgebung (Trusted Execution Environment, TEE), die auch als „Enklave" bezeichnet wird (siehe dazu den Beitrag „Die Enklave im Rechner"). Sie schottet Teile des Prozessors und des Arbeitsspeichers von der Umgebung ab und gewährt nur autorisiertem Code Zugriff auf die zu verarbeitenden Daten. Über Befehlserweiterungen wie die Intel Software Guard Extensions (Intel SGX), die in Intel Xeon E und skalierbaren Intel Xeon Prozessoren der dritten Generation verfügbar sind, können Entwickler definieren, welche Funktionen im Code vertrauliche Daten verwenden dürfen. Bei der Ausführung dieser Programmbestandteile werden die Daten dann in die Enklave geladen und von den autorisierten Funktionen verarbeitet.

Die folgenden Beispiele zeigen, wie Confidential Computing die Verarbeitung sensibler Daten im Gesundheitswesen sicherer und vertrauenswürdiger macht, und so die Akzeptanz und Einsatzmöglichkeiten digitaler Lösungen deutlich erweitert:

Datenschutzkonformes Pandemiemanagement

Bei der Pandemiebekämpfung spielen Maßnahmen zur Kontaktnachverfolgung eine große Rolle. Gesundheitsämter müssen möglichst lückenlos erfassen, wo sich eine erkrankte Person in den Tagen vor der Diagnose aufgehalten hat, und mit wem sie Kontakt hatte, um Infektionsketten schnell und effizient durchbrechen zu können. Dafür ist allerdings eine breite Akzeptanz in der Bevölkerung notwendig. Nur wenn die Menschen sich sicher sind, dass ihre Privatsphäre gewahrt wird, sind sie bereit, ihre Daten mit öffentlichen Stellen zu teilen. Auch gesetzliche Vorgaben wie die Europäische Datenschutzverordnung (DSGVO) setzen hohe Maßstäbe an die Erfassung der Daten.

Wie eine sichere und datenschutzkonforme Umsetzung gelingen kann, zeigt die „Pandemic Cohort Management Suite" von Intel und SAP, die auf den skalierbaren Intel Xeon Prozessoren der dritten Generation und der SAP Business Technology Platform basiert. Die Suite ermöglicht es, individuelle und kollektive Pandemierisiken zu berechnen, sowie die Wirksamkeit von Präventions- und Eindämmungsmaßnahmen zu evaluieren. Sie führt dazu Daten von Bürgern, Veranstaltungen und Gesundheitsämtern zusammen und analysiert diese mithilfe von Machine Learning und anderen modernen Verfahren. Dank Confidential Computing sind die sensiblen Daten nicht nur bei Speicherung und Übertragung durch Verschlüsselung geschützt, sondern auch während der Verarbeitung in einer vertrauenswürdigen Laufzeitumgebung.

Durch den Einsatz der Pandemic Cohort Management Suite ergeben sich im Wesentlichen folgende Vorteile:

- Bürger und Bürgerinnen können ihr individuelles Risikoprofil evaluieren und erhalten wertvolle Tipps für eine effektive Risikominimierung, ohne dass ihre Privatsphäre gefährdet wird.
- Unternehmen können das Risiko ihrer Mitarbeiter am Arbeitsplatz oder in Meetings minimieren und bei Infektionen schnell Gegenmaßnahmen ergreifen.
- Veranstalter bekommen die Möglichkeit, eine einfache digitale und datenschutzkonforme Registrierung anzubieten und so Auflagen zur Kontaktnachverfolgung effizient erfüllen zu können.
- Gesundheitsämter und Politiker erhalten schnell und weitgehend automatisiert Einblick in das Infektionsgeschehen, können Infektionsketten effizient nachverfolgen und rasch durchbrechen.

Die Pandemic Cohort Management Suite wird bereits in den SAP Experience Centern auf der ganzen Welt getestet, unter anderem auch am Stammsitz in Walldorf. Bei der Stadtverwaltung von Heidelberg ist der Einsatz ebenfalls geplant.

Elektronische Patientenakte

Seit 2021 sind gesetzliche Krankenkassen in Deutschland verpflichtet, Versicherten eine elektronische Patientenakte (ePA) anzubieten, in der medizinische Befunde und Informationen über Untersuchungen und Behandlungen digital gespeichert sind. Die Vorteile sind vielfältig: Behandelnde Ärzte erhalten schneller Zugriff auf vorhandene Befunde, Doppeluntersuchungen und Falschmedikationen werden verhindert, die Kommunikation zwischen Patienten, Ärzten, Apotheken, Krankenhäusern und Krankenkassen wesentlich vereinfacht und beschleunigt.

Die in der ePA gespeicherten Daten sind allerdings äußerst sensibel und dürfen nicht in falsche Hände geraten. Für den Aufbau einer entsprechenden hochsicheren Telematikinfrastruktur ist die gematik GmbH verantwortlich, ein IT-Unternehmen, das vom Bund und den Spitzenorganisationen des Gesundheitswesens getragen wird. Sie setzt ebenfalls auf Confidential Computing, um die Integrität der Anwendung und den Schutz der Daten bei der Verarbeitung sicherzustellen. Während die erste Version der auf Intel SGX basierenden elektronischen Patientenakte Versicherte vor allem dabei unterstützt, gesundheitsbezogene Daten und Dokumente verschiedenen behandelnden Ärztinnen zugänglich zu machen, werden die Möglichkeiten der Technologie derzeit noch weiter ausgebaut: Da mit den skalierbaren Intel Xeon Prozessoren der dritten Generation die Größe der Enklaven von 256 Megabyte auf 1 Terabyte steigt, können zukünftig auch große Dateien wie Röntgenbilder oder EKGs problemlos in der sicheren Laufzeitumge-

bung verarbeitet werden. Ab Januar 2022 sollen auch Dokumente wie Impfausweis, Mutterpass, Kinderuntersuchungsheft oder das Zahnbonusheft digitalisiert und das e-Rezept ermöglicht werden.

Fazit: Kein Gesundheitsschutz ohne Datenschutz

Gesundheitsdaten gehören zu den sensibelsten persönlichen Informationen. Ein Diebstahl oder Missbrauch kann erhebliche negative Folgen für den Betroffenen haben. An die Übermittlung, Speicherung und Verarbeitung sind deshalb besonders hohe Anforderungen zu stellen. Während es für Transport und Storage bereits seit langem zuverlässige Verschlüsselungsmethoden gibt, stellte die Verarbeitung bis vor kurzem ein Risiko dar, da die Daten dazu entschlüsselt werden mussten. Mit Confidential Computing lässt sich diese Lücke schließen. Dank Intel SGX ist die Definition und Bereitstellung vertrauenswürdiger Laufzeitumgebungen für Entwickler einfach umzusetzen, ohne die Leistung auf skalierbaren Intel Xeon Prozessoren der dritten Generation zu beeinträchtigen.

Verband der Datenschutzexperten fordert nächste Bundesregierung auf, Unternehmen von Bürokratie zu entlasten

Die Datenschutzbeauftragten in Deutschland fordern am 25. August 2021 die nächste Bundesregierung auf, den Schutz von personenbezogen Daten endlich als Chance zu begreifen und die bisher ungenutzten Potenziale für eine erfolgreiche Digitalisierung zu nutzen. Dazu bedarf es einer bürokratischen Entlastung der Unternehmen und einer stärkeren Rolle der betrieblichen Datenschutzbeauftragten sowie einheitlicher Rechtsauslegung der Datenschutzaufsichten. „Deutschland braucht Digitalisierung. Datenschutz und Datensicherheit sind Innovationsfaktoren für eine nachhaltige Digitalisierung. Wir fordern die Politik deshalb auf, Rahmenbedingungen zu schaffen, die informationelle Selbstbestimmung mitdenken und Innovationsfreude fördern", sagt Thomas Spaeing, Vorstandsvorsitzender des Berufsverbands der Datenschutzbeauftragten (BvD) e.V. Der Verband legt dazu ein Fünf-Punkte-Papier vor.

Der Berufsverband der Datenschutzbeauftragten sieht nach der Bundestagswahl die Möglichkeit für einen politischen Neustart im Bereich der dringend notwendigen Digitalisierung von Prozessen in Wirtschaft und Verwaltung. Grundlage dafür sind laut Verbandsvorstand Thomas Spaeing ein Paradigmenwechsel bei der Bewertung des Datenschutzes sowie ein Nachsteuern bei der Umsetzung der Datenschutz-Grundverordnung (DSGVO) im Zuge der weiter andauernden Evaluierung des Bundesdatenschutzgesetzes (BDSG).

Im heute vorgestellten Positionspapier skizziert der BvD eine stärkere Rolle des Datenschutzbeauftragten für die Unternehmen. Zwar seien viele Unternehmen verpflichtet, einen Datenschutzbeauftragten zu benennen bzw. tun dies freiwillig, jedoch sehen die gesetzlichen Rahmenbedingungen lediglich eine beratende und überwachende Funktion vor. „In der Praxis erleben wir hier eine Überforderungssituation der Unternehmen, wenn sie zwar einen Datenschutzbeauftragten haben, aber dieser nur eingeschränkt tätig werden kann. Das ist kontraproduktiv und schadet der Akzeptanz", so Spaeing. Mit einfachen Änderungen in BDSG und DSGVO wird die Benennung eines DSB noch wertvoller für Unternehmen. Hierfür sind Anpassungen beispielsweise beim Führen des Verzeichnisses der Verarbeitungstätigkeiten, eine Anpassung der Meldepflichten gegenüber den Datenschutz-Aufsichtsbehörden sowie Änderungen bei der Zuständigkeit für die Datenschutz-Folgenabschätzung konkrete und praxisnahe Optionen.

Des Weiteren könnte die positive Arbeit einzelner Datenschutzaufsichten in den Bundesländern noch verbessert werden. Beispielsweise indem die Datenschutzkonferenz (DSK) verbindliche Entscheidungen treffen kann und somit eine einheitliche Bewertung der datenschutzrechtlichen Vorgaben gewährleistet wird. „Unterschiedliche Auslegungen in 16 Bundesländern sind weder sinnvoll noch zielführend. Die Unternehmen und Betriebe benötigen eine nachvollziehbare und einheitliche Anwendung der Datenschutzgesetze. Dies wäre durch neue Kohärenzverfahren und verbindliche Entscheidungen der Datenschutzkonferenz möglich", heißt es dazu in dem Papier.

Das Fünf-Punkte-Papier des BvD können Sie hier abrufen *https://www.bvdnet.de/wp-content/uploads/2021/08/Forderungen-zur-Wahl_16082021.pdf*

Weltweit 70 Prozent mehr Phishing-Attacken im Homeoffice

Sophos veröffentlichte am 26. August 2021 seinen aktuellen Phishing Insights 2021 Report, der auf die Erfahrungen und die Prozesse hinter Phishing-Angriffen auf Organisationen während des Jahres 2020 zurückblickt. Befragt wurden 5.400 IT-Entscheider:innen in 30 Ländern in Europa, Nord- und Süd-Amerika, dem Asia-Pazifik-Raum, Zentralasien, dem Mittleren Osten und Afrika.

Die Ergebnisse zeigen: Phishing-Attacken auf Organisationen haben während der Pandemie erheblich zugenommen. Millionen von Arbeitnehmer:innen mussten ihre Tätigkeiten ins Home-Office verlagern und wurden zur beliebten Zielscheibe für Cyberkriminelle. Aus globaler Perspektive bestätigte die Mehrheit der IT-Teams (70 Prozent), dass die Anzahl der Phishing-E-Mails, die ihre Belegschaft traf, während 2020 zunahm. Aus länderspezifischer Sicht sind die Ergebnisse ähnlich ernüchternd: In Deutschland sind es 68 Prozent, in Österreich sogar 88 Prozent (der zweithöchste Wert nach Israel) und in der Schweiz 87 Prozent der IT-Teams, die einen Anstieg Phishing-E-Mails verzeichneten. Ein Resultat daraus ist, dass global 82 Prozent der IT-Teams im Jahr 2020 Opfer von Ransomware-Attacken wurden.

Weitere Erkenntnisse des Reports:

- IT-Profis haben keine einheitliche Definition von Phishing. Das am weit verbreitetsten Verständnis von Phishing global mit 57 Prozent (Deutschland: 54 Prozent, Österreich: 55 Prozent, Schweiz: 54 Prozent) lautet: „E-Mails, die fälschlicherweise behaupten, von einer legitimen Organisation zu stammen, normalerweise in Kombination mit einer Bedrohung oder Anfrage nach Informationen."
- 46 Prozent (Deutschland: 30 Prozent, Österreich: 37 Prozent, Schweiz: 45 Prozent) halten Business-E-Mail-Compromise-Angriffe für Phishing, und 36 Prozent (Deutschland: 24 Prozent, Österreich: 53 Prozent, Schweiz: 54 Prozent) denken, dass Thread-jacking (wenn sich Angreifer als Teil eines Angriffs in einen legitimen E-Mail-Thread einfügen) Phishing ist.
- Die meisten Organisationen – weltweit 90 Prozent – verwenden Cybersecurity-Sensibilitätsprogramme, um gegen Phishing vorzugehen. In Deutschland und der Schweiz tun dies mit 86 bzw.

89 Prozent etwas weniger, österreichische Unternehmen setzen zu 98 Prozent entsprechende Programme ein.

Chester Wisniewski, Principal Research Scientist bei Sophos, ordnet die Ergebnisse des Phishing Insights 2021 Reports so ein: „Phishing gibt es seit über 25 Jahren und es bleibt eine effektive Technik für Cyberangriffe. Ein Grund für den Erfolg ist seine Fähigkeit, sich ständig weiterzuentwickeln und zu diversifizieren, Angriffe an aktuelle Themen oder Sorgen anzupassen – wie zum Beispiel die Pandemie – und mit menschlichen Emotionen und Vertrauen zu spielen."

Die Versuchung für Unternehmen, Phishing-Angriffe als eine ziemlich niedrige Bedrohung anzusehen, sei groß, so Wisniewski weiter, würde aber das Potential von Phishing unterschätzen. „Denn dieses ist oft der erste Schritt in einer komplexen, mehrstufigen Attacke." Nach Beobachtungen des Sophos Rapid Response Teams nutzen Cyberkriminelle häufig Phishing-E-Mails, um die Nutzer dazu zu verleiten, Malware zu installieren oder sensible Daten zu teilen, die Zugang zum gemeinsamen Netzwerk ermöglichen. „Das Rapid Response Team hat hautnah miterlebt, wie eine scheinbar harmlose E-Mail zu einer Millionen-Dollar Ransomware-Attacke führte. Cryptojacking, Daten- sowie Vermögensdiebstahl sind mögliche Resultate, wenn ein Phishing-Vorfall die Tür für Cyberkriminelle geöffnet hat."

Am besten wäre es, so der Experte, Phishing-E-Mails daran zu hindern, überhaupt beim vorgesehenen Empfänger zu landen. „Effektive E-Mail-Sicherheitslösungen können hierbei einen großen Beitrag leisten, aber das sollte begleitet sein von aufmerksamen und qualifizierten Mitarbeiter:innen, die in der Lage sind, verdächtige Nachrichten zu erkennen und zu melden und zwar bevor diese im Unternehmen weiterkommen."

Zahlreiche Details, Zahlen und Grafiken finden Sie hier im aktuellen Phishing Insights 2021 Report: *https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-phishing-insights-2021-report.pdf*

Einheitliche digitale europäische Identität: Beitrag zur Öffnung des europäischen Marktes

Die Idee dahinter ist, dass es Bürgern ermöglicht werden soll, über ein Smartphone oder einen Computer ihre Identität nachzuweisen und elektronische Dokumente aus ihrer „Europäischen Digitalen Identitätsbörse" auszutauschen. Dieser Ausweis soll in ganz Europa einheitlich sein und dadurch den Zugriff auf verschiedene Dienste, bei denen eine Identitätsprüfung notwendig ist, ermöglichen.

In den letzten zwei Jahren erlebten wir öfter Schwierigkeiten dabei, Termine von Angesicht zu Angesicht wahrzunehmen, die für die Durchführung wichtiger Verfahren notwendig gewesen wären. Dies beschleunigte den Übergang zu digitalen Plattformen und die Notwendigkeit einer gesicherten Identität für bestimmte Transaktionen, die ein hohes Maß an Vertrauen erfordern. Trotz entspannterer Gesundheitslage wollen Kunden und Bürger jedoch nicht mehr auf die erlebten Vorteile des digitalen Onboardings verzichten. Durch asynchrone Videoidentifikation und Qualified Electronic Signature (QES) konnten viele Behörden oder ganze Marktsegmente wie der Finanzsektor, Banken und Versicherungen nicht nur vollständig aus der Ferne, sondern auch mit erheblicher Zeitersparnis weiterhin Kunden generieren oder Bürger betreuen.

Die Aufforderung zur weiteren Digitalisierung und zur europaweiten Vereinheitlichung der digitalen Identitäten ebnet den Weg für Dienstleister, die sich schon seit geraumer Zeit mit diesem Thema befassen. Darunter ist etwa Electronic IDentification (eID), der als aktuell einziger eTrust-Provider mit patentierten und europaweit zertifizierten End-to-End-Lösungen für QES mittels asynchroner Videoidentifizierung diese Entwicklung begrüßt. „Technologien zur abgesicherten und rechtskonformen Online-Identitätsprüfung gestatten es bereits heute, dass Kund*innen und Bürger*innen in den Genuss von Dienstleistungen kommen – etwa mit der öffentlichen Verwaltung zu interagieren oder online einen Bankkredit aufzunehmen, ein Bankkonto zu eröffnen, einen Mietvertrag zu unterschreiben oder eine Versicherungskarte in digitaler Form auf dem Smartphone zu haben. Mit europaweit einheitlichen digitalen Ausweisen werden diese Verfahren noch unmittelbarer ablaufen und können länderübergreifend erfolgen. Das Konzept einer starken und benutzerfreundlichen digitalen Identität wird immer notwendiger und allgegenwärtiger", bestätigt Iván Nabalón, Gründer und CEO von Electronic IDentification.

Wie sicher ist die QES wirklich?

Die QES gilt seit Langem als „digitales Alter Ego" einer Person und, nach Ansicht der EU-Mitglieder, als die vollständigste und sicherste Methode zur Validierung der Identität einer Person. Die qualifizierte elektronische Signatur ist eine elektronische Unterschrift, die mit einem qualifizierten digitalen Zertifikat zur Identifizierung des Unterzeichners geleistet wird. Dieses Zertifikat besteht aus einem elektronischen Dokument, das die Daten des Unterzeichners und die Validierung der Signatur mit der eindeutigen Identifikation der Person verbindet. Das Zertifikat muss von einer qualifizierten Zertifizierungsstelle ausgestellt werden. Electronic IDentification erfüllt bereits die Compliance-Anforderungen (GDPR, AML5 und 6, ISO 27001, eIDAS) aller EU-Länder und verfügt hierfür über alle notwendigen europaweit gültigen Zertifizierungen.

Die digitale Identität hat sich in den letzten Jahren bereits verändert, und dieser Wandel wird sich auch in den kommenden Jahren fortsetzen. „Die Idee der digitalen Identität gibt es bereits seit vielen Jahren, doch erschwerte es die ihr zugrundeliegende Technologie, eine solche zu erhalten oder zu nutzen: Ein erster Antrag musste physisch gestellt werden. Sie funktionierte nicht auf Smartphones, und deren Einsatz mit verschiedenen Betriebssystemen oder beim Wechsel des Endgerätes war sehr komplex. Mit anderen Worten: Sie war nicht so interoperabel, wie sie es jetzt sein sollte und könnte", so Nabalón weiter.

Deshalb, und auch, um das von der Europäischen Kommission geförderte Projekt der europäischen digitalen Identität zu entwickeln, wird die Unterstützung von Unternehmen benötigt.

Bisher waren der Zugang und die Nutzung einer digitalen Identität alles andere als einfach. eID ist jedoch durch seine hochmoderne Technologie bestens darauf vorbereitet die Europäische Kommission dabei zu unterstützen, eine starke und gleichzeitig einfach zu nutzende digitale Identität zu schaffen, die einerseits für die Bürger zugänglicher und andererseits für Institutionen und Organisationen leichter zu implementieren und in eigene Verfahren zu integrieren sein wird.

Electronic IDentification (eID)

Electronic IDentification (eID) brachte die disruptive Lösung der asynchronen Video-Identifikation auf Basis von Video-In-Streaming mit durchgängiger Abdeckung des Identifikationsprozesses auf den Markt. In Kombination mit ihrem Dienst der Qualifizierten Elektronischen Signatur (QES) erzeugt dies einen starken,

vollständig digitalen Identifikations-Workflow. eID, ein führendes spanisches Unternehmen in seinem Bereich, begann mit der Vermarktung seiner Produkte im Jahr 2016 und kann derzeit eine starke Erfolgsbilanz mit mehr als 250 Kunden in 30 Ländern vorweisen. Weitere Informationen über Electronic Identification: *www.electronicid.eu/de*.

XDR: Wie Sicherheitsteams Cyber-Angriffe frühzeitig erkennen und abwehren können

Sicherheitsteams haben aufgrund der Implementierung von neuen Technologien und Remote-Work-Prozessen zunehmend Schwierigkeiten, die Kontrolle über die komplexe Unternehmens-IT zu behalten. In Sachen IT-Sicherheit kann dies zu Problemen führen, da sich Cyber-Bedrohungen nicht mehr effektiv abwehren lassen. Eine einheitliche Plattform, die sämtliche Sicherheitsfunktionen zentralisiert, schafft Transparenz und effizientes Bedrohungs-Management. Tanja Hofmann, Lead Security Engineer bei McAfee Enterprise, erklärte am 04. September 2021 die Vorteile von Extended Detection and Response (XDR).

Im vergangenen Jahr dominierten in Sachen Cyber-Kriminalität vor allem Phishing-Scam- und Ransomware-Kampagnen, die die Ungewissheit und Neugierde der Menschen ausnutzten: Mithilfe von infizierten E-Mail-Anhängen oder auf Fake-Webseiten verteilten Cyber-Kriminelle Malware und eigneten sich auf diese Weise sensible, personenbezogene Informationen und kritische Unternehmensdaten an Die Lockmittel: Neuigkeiten über die Entwicklung der Pandemie oder die bevorstehende Impfung sowie Angebote für günstige Masken und Desinfektionsmittel.

Aktuelle Untersuchungen von McAfee zeigen nun, dass Cyber-Kriminelle seit einigen Monaten ihre Vorgehensweisen anpassen, weiterentwickeln und andere Ziele wählen. So verschieben sie ihren Fokus mittlerweile unter anderem auf lukrative Großunternehmen, das Internet-of-Things oder das Geschäft mit Kryptowährungen.

Steigende Komplexität der Unternehmens-IT

Neben der steigenden Anzahl und Flexibilität von Cyber-Bedrohungen sehen sich Unternehmen mit einer weiteren, nicht zu verachtenden Herausforderung konfrontiert. Im Zuge der Pandemie migrierten viele Unternehmen erstmals in die Cloud – die Cloud-Nutzung stieg zeitweise um 50 Prozent –, um Remote Work und folglich den Fortlauf ihres Geschäfts zu gewährleisten. Ein Großteil der Anwendungen und Prozesse spielten sich nicht mehr nur im lokalen Netzwerk, sondern auch in der Cloud ab.

In einer solch komplexen Umgebung, die mit jeder Anwendung, jedem Service und jedem System weiterwächst, müssen Sicherheitsteams laufend den Überblick behalten können, um jede Instanz abzusichern. Dies schließt sowohl lokale Netzwerke und Daten als auch die Cloud sowie den Datentransferweg mit ein. Um diese Mammutaufgabe zu stemmen, setzen Sicherheitsteams oftmals unterschiedliche Lösungen von verschiedenen Anbietern ein. Das ist nicht nur ressourcenintensiv, sondern höchst ineffizient, da sie zumeist unabhängig voneinander arbeiten und isolierte Analysedaten generieren. Die Folge: An mehreren Fronten entstehen gleichzeitig zahlreiche Warnmeldungen, die Sicherheitsteams managen müssen.

Extended Detection and Response als einheitliche Lösung

- Mithilfe einer SaaS-basierten Extended Detection and Response (XDR)-Plattform lässt sich nicht nur das System-Chaos überblicken. Sie unterstützt Sicherheitsteams zudem bei der flexiblen Erkennung, Abwehr und Behebung von potenziellen sowie akuten Cyber-Angriffen. Im Zuge dessen führt sie alle internen Sicherheitsfunktionen und -daten zentral zusammen, sortiert sowie kombiniert diese mit externen Bedrohungsdaten und sorgt somit für Transparenz als auch Kontrolle über sämtliche Endgeräte, Netzwerke und die Cloud hinweg.
- Mithilfe der kontextbasierten Analyse und Korrelation der Daten entlastet eine XDR-Plattform nicht nur Sicherheitsteams, indem sie Warnmeldungen auf ihre Ursache hin prüft und False-Positives aussortiert. Sie ist zudem in der Lage, das Ausmaß des Risikos und der potenziellen Folgen abzuschätzen. Auf dieser Grundlage können Sicherheitsteams Bedrohungen und Angriffe priorisieren, was ihnen eine gezielte Bedrohungserkennung und -abwehr vom Endgerät bis in die Cloud erlaubt.
- Mithilfe von XDR können Sicherheitsteams sowohl präventiv gegen Bedrohungen vorgehen, als auch während und nach einem Angriff Handlungsempfehlungen erhalten, wodurch IT-Systeme zu jeder Zeit bestmöglich geschützt bleiben.

Forderungen an die Politik: Bundesverband IT-Sicherheit e.V. (TeleTrusT) veröffentlicht „IT-Sicherheitsagenda 2029“

Deutschland und Europa müssen angemessen und souverän die digitale Zukunft gestalten können. Dazu hält es der Bundesverband IT-Sicherheit e.V. (TeleTrusT) für dringend erforderlich, dass Deutschland im Bereich der IT-Sicherheit eine Vorreiterrolle einnimmt. Für die nächsten beiden Legislaturperioden des Deutschen Bundestages hat TeleTrusT am 02. September 2021 deshalb mit seiner IT-Sicherheits-Agenda 2029 wichtige und dringende Forderungen aufgestellt.

Zentrale Forderungen:

- Klares Bekenntnis zu unbeschränkter IT-Sicherheit
- Technologische Souveränität im Bereich IT-Sicherheit schaffen – für eine werteorientierte, sichere und vertrauenswürdige digitale Zukunft
- Auf- und Ausbau von IT-Sicherheitsinfrastrukturen für Bürger, Unternehmen und Verwaltung fordern und fördern
- Mehr IT-Sicherheitstechnologie „Made in Germany“ in der Praxis
- Verbot der Kompromittierung von IT-Sicherheit, keine Backdoors, Staatstrojaner oder geschwächte Verschlüsselung
- Europäische IT-Sicherheitsgesetze für eine erhöhte Rechts- und Investitionssicherheit – klar, konsolidiert und agil

TeleTrusT-Vorstandsvorsitzender Prof. Dr. Norbert Pohlmann: „Die IT-Sicherheitsprobleme und daraus resultierende Schäden nehmen stetig zu. Vor vier Jahren mit 50 Mrd. EUR beziffert, über 100 Mrd. vor zwei Jahren, betragen sie mittlerweile mehr als 220 Mrd. EUR. Die neue Bundesregierung muss auf allen Ebenen und gemeinsam mit den relevanten Stakeholdern dafür sorgen, dass diese Schäden deutlich vermindert werden. Denn nur so erreichen wir das Ziel, eine souveräne, sichere und vertrauenswürdige digitale Zukunft zu schaffen.“

RA Karsten U. Bartels LL.M., stellvertretender TeleTrusT-Vorstandsvorsitzender: „Wenn wir eine technologische und digitale Souveränität Deutschlands und Europas wollen, muss die Politik in den nächsten zwei Legislaturperioden die IT-Sicherheit massiv stärken. Unsere sechs Kernforderungen stellen zusammen, was dazu erforderlich ist: der Staat hat IT-Sicherheit aktiv zu fördern und nicht zu kompromittieren. Das betrifft auch das Recht auf Verschlüsselung ohne staatliche Hintertüren. IT-Sicherheitsinfrastrukturen sind so auszubauen und vom Staat selbst zu nutzen, dass Sie im privaten und geschäftlichen Alltag ankommen."

Technologische und digitale Souveränität kann nur durch ein zielgerichtetes und langfristiges Vorgehen erfolgreich umgesetzt werden. Derzeit existieren zu viele Einzelinitiativen, die kaum Wirkung zeigen. Es bedarf einer Umsetzungsstrategie, die Ziele definiert, Maßnahmen priorisiert und festlegt sowie eine Aufgabenverteilung zwischen Politik, Verwaltung, Hersteller- und Anwendungsunternehmen und Forschung vornimmt. Die Politik ist aufgerufen, den Startimpuls für die Umsetzungsstrategie zu setzen und sie langfristig zu unterstützen. Andere Staaten verfolgen bereits konsequent entsprechende Umsetzungspläne. Demzufolge muss Deutschland und Europa seine Konkurrenzfähigkeit gegenüber anderen Regionen neu erlangen und erhalten, um weitestgehend unabhängig die digitale Zukunft zu gestalten. *https://www.teletrust.de/teletrust-it-sicherheitsagenda/*

G DATA Bedrohungsreport: Angriffe ohne Schadsoftware nehmen zu

Der aktuelle Bedrohungsreport vom 06. September 2021 von G DATA CyberDefense verzeichnet einen deutlichen Rückgang der abgewehrten Angriffsversuche im ersten Halbjahr 2021 im Vergleich zum Vorjahreszeitraum. Der Grund dafür ist, dass für Angriffe nicht mehr nur Schadsoftware zum Einsatz kommt. Die Gefahr für Unternehmen bleibt unverändert hoch.

Um mehr als 40 Prozent ist die Zahl der abgewehrten Cyberattacken im Vergleich zum ersten Halbjahr 2020 zurückgegangen. Das belegt der aktuelle Bedrohungsreport von G DATA für das erste Halbjahr 2021 im Vergleich zum Vorjahreszeitraum. Der starke Rückgang hängt auch mit den extrem hohen Zahlen im Jahr 2020 zusammen. Gerade im zweiten Quartal 2020 hatten Cyberkriminelle die Verunsicherung der Menschen infolge der Corona-Pandemie besonders stark ausgenutzt, was damals zu einer massiven Zunahme der abgewehrten Angriffe führte (plus 156 Prozent). Vom ersten zum zweiten Quartal 2021 beträgt der Rückgang 15,6 Prozent. Die aktuellen Zahlen bestätigen aber auch den Trend, dass Unternehmen weiterhin verstärkt im Fokus der Angreifer sind. Während die Zahl abgewehrter Attacken auf Privatkunden um fast 20 Prozent gesunken ist, beträgt der Rückgang im Unternehmensumfeld nur knapp drei Prozent.

„Die Zeit der großflächigen Angriffe ist vorbei. Cyberkriminelle gehen bei Attacken auf Unternehmen zunehmend gezielt vor", sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense. „Wir gehen davon aus, dass gerade im vergangenen Jahr viele Unternehmen auf Grund des hastigen Umzugs ins Homeoffice einer Cyberattacke zum Opfer gefallen sind, das aber noch nicht gemerkt haben."

Gezieltes Vorgehen

Für gezielte Attacken nutzen Cyberkriminelle weiterhin bestehende Schwachstellen aus. Gerade in den ersten sechs Monaten des Jahres haben verschiedene kriminelle Gruppierungen mehrere größere Sicherheitslücken in Microsoft Exchange Servern aktiv ausgenutzt und die Netzwerke von Unternehmen infiltriert.

Ein weiteres Beispiel für das Vorgehen von Cyberkiminellen ist der sogenannte AMSI-Bypass. Immer wieder versuchen Angreifer, das von Microsoft entwickelte Antimalware Scan Interface (AMSI) zu umgehen. Eigentlich scannen Sicherheitslösungen dank AMSI Anwendungen auf ihre Schadhaftigkeit. Allerdings versuchen Malware-Autoren mit automatisierten Tools, diese Schnittstelle auszuschalten oder einen Weg an ihr vorbeizufinden – insbesondere, um dateilose Schadsoftware einzusetzen.

Malware Top 10: Remote Access Trojaner in der Überzahl

Nach wie vor zählt QBot nicht nur zu den aktivsten, sondern auch den gefährlichsten Schadprogrammen. Bei einem Großteil der aktuellen Angriffe im ersten Halbjahr kam der Emotet-Nachfolger zum Einsatz. Der ursprüngliche Bankingtrojaner wurde von den Angreifern nach und nach ebenfalls zu einer Allzweckwaffe für Cyberkriminelle weiterentwickelt. Weiterhin sind viele Remote Access Trojaner (RAT) aktiv. Sieben der zehn aktivsten Schadprogramme zählen zu dieser Gruppe. RATs ermöglichen eine vom Nutzer unbemerkte Fernsteuerung und administrative Kontrolle eines fremden Rechners. So können Angreifer unter anderem den Desktop des Opfers einsehen, Tastatureingaben protokollieren, auf die Kamera zugreifen sowie die in Browsern gespeicherte Anmeldeinformationen kopieren oder Dateien hoch- bzw. herunterladen.

Malware-as-a-Service: Gootloader

Wie trickreich Cyberkriminelle ihre Angriffsbemühungen weiterentwickelt haben, verdeutlicht ein Blick auf die aktuelle Angriffswelle der Gootloader-Malware-Familie. Die Malware-Autoren haben Gootloader so weiterentwickelt, dass sie verschiedene Malware nachladen und installieren kann. Dabei pushen die Angreifer*innen ihre eigenen Seiten mit Search-Engine-Poisoning nach oben. Diese sehen aus wie legitime Seiten, sodass auch technisch versierte User einer derartigen Täuschung zum Opfer fallen.

„Trotz der sinkenden Zahlen kann von Entspannung keine Rede sein. Unternehmen sollten vielmehr ihre Hausaufgaben erledigen und ihre IT absichern. Technische Maßnahmen sind wichtig, aber mindestens genauso wichtig ist es, die Belegschaft im Umgang mit Gefahren zu schulen – denn längst nicht alle Risiken bestehen nur aus Schadsoftware", so Berghoff.

ECOS Technology warnt vor langfristigem Ausspähen

Beim Umgang mit ihren Daten nutzen Unternehmen und Behörden oft abgestufte Sicherheitsmaßnahmen. Was besonders wichtig und kritisch ist, wird auch besonders gut geschützt. Für (vermeintlich) weniger schützenswerte Informationen liegt das Sicherheitsniveau hingegen unter Umständen niedriger. Ein Ansatz, der unter kommerziellen und operativen Gesichtspunkten vernünftig ist und ein Fundament gängiger Informations-Sicherheits-Management-Systeme darstellt.

Die IT-Security-Experten von ECOS Technology (*www.ecos.de*) warnen in diesem Zusammenhang allerdings vor häufig unterschätzten Gefahren durch langfristiges Ausspähen beziehungsweise Langzeit-Tracking. Cyberkriminelle setzen dabei darauf, jeglichen zugänglichen Datenverkehr eines Unternehmens oder einer Organisation über einen längeren Zeitraum aufzuzeichnen, zu entschlüsseln und mit weiteren Informationen in Zusammenhang zu bringen. Daraus lassen sich Rückschlüsse auf Strukturen, Beziehungen und Gewohnheiten innerhalb der Organisation gewinnen. Diese können dann beispielsweise die Grundlage für die erfolgreiche Durchführung von Social-Engineering-Angriffen bilden.

Die besondere Gefahr solcher Angriffe liegt darin, dass sie den Betroffenen in der Regel gar nicht bewusst ist. Denn für sich betrachtet, erscheinen die einzelnen Informationen häufig weitgehend belanglos. Mit der einzelnen E-Mail mit Flug- und Hoteldaten für die nächste Geschäftsreise etwa, die ein Mitarbeiter aus dem Homeoffice seiner Abteilungsleiterin schickt, wird sich in der Regel zunächst eher wenig anfangen lassen. Anders sieht es aus, wenn unbefugte Dritte mit kriminellen Absichten durch Langzeit-Beobachtung in den Besitz umfangreicher Mengen von Daten dieser Art gelangen. Daraus gewonnene Erkenntnisse können zum Beispiel die Basis für einen sogenannten „CEO Fraud" Angriff bilden. Hierbei wird mit gefälschten, vermeintlich von der Geschäftsführung stammenden E-Mails zur Überweisung von Geldbeträgen oder zur Bereitstellung von Informationen aufgefordert. Ähneln solche E-Mails in Inhalt und Stil einer typischen Spam-Nachricht, werden sie in der Regel sofort erkannt. Ganz anders kann es jedoch aussehen, wenn sie von einem Hacker verfasst werden, der den Kommunikationsstil der beteiligten Personen über einen längeren Zeitraum genau beobachtet hat. Vergleichbares gilt für E-Mails, die zum Einschleusen von Ransomware beziehungsweise Verschlüsselungstrojanern genutzt werden. Die Erfolgsquote solcher Attacken ist umso höher, je besser der Angreifer sein Opfer kennt und je genauer die entsprechende E-Mail-Kommunikation zugeschnitten werden kann.

„Bei der Vorbereitung größerer, gezielter Angriffe auf die IT-Netzwerke von Firmen oder Organisationen geht es Kriminellen nicht darum, sofort die gewünschten Daten zu erbeuten oder unmittelbar einen Erpressungs-Trojaner einzuschleusen", erklärt Paul Marx, Geschäftsführer der ECOS Technology GmbH. „Vielfach steht bei professionelle Attacken eine eher langfristig angelegte Strategie im Vordergrund. Das Abgreifen einzelner E-Mails erscheint vermeintlich harmlos. Die Gefahr entsteht dadurch, dass Unbefugte über einen längeren Zeitraum in den Besitz umfangreicher Datenmengen gelangen und daraus entsprechende Schlüsse ableiten."

Zur Abwehr derartiger Attacken empfiehlt ECOS am 08. September 2021, auch bei vergleichsweise unkritischen Informationen ein hohes Sicherheitsniveau beizubehalten. Dies gilt insbesondere auch beim Arbeiten von unterwegs oder im Homeoffice – Szenarien, in denen beispielsweise spezielle, sichere Remote-Access-Lösungen oder VPN-Zugänge zum Einsatz kommen sollten.

Die ECOS Technology GmbH hat sich auf die Entwicklung und den Vertrieb von IT-Lösungen für den hochsicheren Fernzugriff (Remote Access) sowie die Verwaltung von Zertifikaten und Smartcards spezialisiert. Zu den Kernprodukten, die in unterschiedlichsten Branchen eingesetzt werden, zählen der ECOS SecureBootStick und die PKI-Appliance ECOS TrustManagementAppliance. Unternehmen, Behörden und Organisationen sind damit zum Beispiel in der Lage, eigene Zertifikate zu erstellen, zu verlängern oder zurückzuziehen, Mitarbeiter im Home Office anzubinden, schnell nutzbare, kosteneffiziente Notfallarbeitsplätze für Krisenfälle vorzuhalten oder Industrieanlagen sicher und geschützt fernzuwarten. Durch die kostenoptimierten Thin-Client-Lösungen von ECOS können außerdem in vielen Szenarien die Hardwarekosten massiv gesenkt werden (Lifecycle Extension). ECOS beschäftigt sich bereits seit 1999 mit der IT-Sicherheit im Rahmen von Netzwerk-Infrastrukturen. Das deutsche Unternehmen hat seinen Hauptsitz in Oppenheim bei Mainz.

Weitere Informationen: *https://www.ecos.de*

Bundeskabinett: Ziele für die Cybersicherheit beschlossen

Die Cybersicherheitsstrategie für Deutschland 2021 beschreibt die grundsätzliche, langfristige Ausrichtung der Cybersicherheitspolitik der Bundesregierung. Das Kabinett hat sie am 08. September 2021 beschlossen. Ausgangspunkt ist eine verschärfte Bedrohungslage.

Die Covid-19-Pandemie hat der technologischen Entwicklung einen weiteren Schub gegeben. Die Verlagerung vieler Prozesse, unabhängig ob im privaten, beruflichen oder behördlichen Kontext, in den Cyberraum oder in eine digitalisierte Welt bieten viele Möglichkeiten. Einhergehende Risiken dürfen dabei aber nicht vergessen werden. Der Kabinettsbeschluss schreibt daher zum einen die Strategien aus den Jahren 2011 und 2016 fort und berücksichtigt zum anderen die Entwicklungen der Digitalisierung in der Wirtschaft, Wissenschaft und Zivilgesellschaft.

Enthalten sind vier übergreifende Leitlinien:

- Cybersicherheit als gemeinsame Aufgabe von Staat, Wirtschaft, Gesellschaft und Wissenschaft etablieren,
- Digitale Souveränität von Staat, Wirtschaft, Wissenschaft und Gesellschaft stärken,
- Digitalisierung sicher gestalten und
- Ziele messbar und transparent ausgestalten.

Diese Leitlinien beschreiben Aspekte, die für alle vier folgenden Handlungsfelder der Cybersicherheitsstrategie gelten.

Sicheres Handeln in einer digitalisierten Umgebung

Die zehn strategischen Ziele des ersten Handlungsfeldes sollen dazu beitragen, dass Bürgerinnen und Bürger die Chancen digitaler Technologien nutzen und sich hierbei sicher und selbstbestimmt in der digitalisierten Umgebung bewegen können. Erreicht werden kann das durch die verstärkte Sensibilisierung und die Steigerung von Cyberkompetenz in der Bevölkerung.

Gemeinsamer Auftrag von Staat und Wirtschaft

Die 13 strategischen Ziele des zweiten Handlungsfeldes sehen die Stärkung der Cybersicherheit in der Wirtschaft insgesamt vor. Neben dem Fokus auf kritischen Infrastrukturen, deren Ausfall oder Beeinträchtigung zu Versorgungsengpässen und damit einer Gefahr für die öffentliche Sicherheit führen kann, werden auch kleine und mittlere Unternehmen in den Blick genommen. Die Zusammenarbeit von Staat und Wirtschaft soll hier fortgeführt werden.

Leistungsfähige und nachhaltige Architektur

Das dritte Handlungsfeld betrifft die staatlichen Akteure in der Cybersicherheit. Der Fokus liegt hierbei auf der Kompetenzverteilung beziehungsweise der Zusammenarbeit zwischen den Behörden.

Als effektive Antwort auf neue Herausforderungen gilt es, Strukturen und Prozesse permanent zu überprüfen, Fähigkeiten fortzuentwickeln und behördliche Befugnisse gegebenenfalls anzupassen.

Aktive Positionierung Deutschlands

Schließlich ist das Engagement Deutschlands in der EU und in der NATO auch in Fragen der Cybersicherheit unverzichtbar. Die Zusammenarbeit mit den internationalen Partnern und die Einbindung nationaler Maßnahmen in europäische und internationale Prozesse sind für die Gewährleistung eines hohen Niveaus an Cybersicherheit in Deutschland essenziell.

Deutliche Zunahme von Cyberangriffen

Der beschlossenen Strategie ist eine Analyse der Bedrohungslage vorausgegangen, die sowohl eine deutliche Zunahme der Schwere von Cyberangriffen als auch deren Anzahl aufgezeigt hat. Mehr als 70 Akteure aus Wirtschaft, Wissenschaft, Gesellschaft und Staat sind aktiv in den Entwurf eingebunden gewesen.

Die Cybersicherheitsstrategie umfasst zudem erstmals einen transparenten Ansatz für Umsetzung, Berichtwesen und Controlling der Strategie.

Die dynamische Bedrohungslage sowie der hierfür vorgesehene Fünfjahresrhythmus erforderten einen Beschluss noch vor Ende der aktuellen Legislaturperiode. Nach dem Beschluss wird die Strategie dem Deutschen Bundestag und dem Bundesrat zugeleitet werden. *bundesregierung.de/breg-de/aktuelles/neue-cybersicherheitsstrategie-1958144*

DsiN zur Cybersicherheitsstrategie 2021

Dazu erklärt DsiN-Geschäftsführer Dr. Michael Littger:

„Die Cybersicherheitsstrategie 2021 setzt verstärkt auf Cyberkompetenzen von Internetnutzenden. Tatsächlich sind Menschen die größte Schwachstelle in der heutigen IT-Sicherheitsarchitektur. Über 90 Prozent der Sicherheitsvorfälle im privaten und beruflichen Umfeld sind durch einfache Schutzvorkehrungen vermeidbar. Wenn es gelingt, die neuentstandenen Transferinfrastrukturen der vergangenen Jahre kraftvoll weiterzuentwickeln, kann Deutschland zum Vorbild bei digitaler Kompetenzvermittlung werden.

Die Cybersicherheitsstrategie benennt konkrete Engagements des Bundes mit Deutschland sicher im Netz wie die Digitale Nachbarschaft fürs Ehrenamt, den Digital-Kompass für ältere Menschen, den Digitalen Engel für ländliche Regionen sowie PolisiN – Politiker:innen sicher im Netz und den DsiN-Digitalführerschein. Aber auch TISiM, die Transferstelle IT-Sicherheit im Mittelstand vermittelt bundesweit schon heute an 80 regionalen Anlaufstellen konkrete Hilfestellungen für Berufstätige und Unternehmen. Insbesondere den digitalen Mittelstand gilt es mit der neuen Bundesregierung dauerhaft zu stärken."

Über die Cybersicherheitsstrategie der Bundesregierung:

Die Cybersicherheitsstrategie für Deutschland 2021 beschreibt die grundsätzliche, langfristige Ausrichtung der Cybersicherheitspolitik der Bundesregierung. Das Kabinett hat sie nun beschlossen. Ausgangspunkt ist eine verschärfte Bedrohungslage.

EU SECRET Zulassung für SDoT Security Gateway Cross Domain Solution

Die Security Appliance „SDoT Security Gateway" erhielt am 15. September 2021 nach unabhängiger Evaluation einer EU-Sicherheitsbehörde die allgemeine SECRET UE / EU SECRET Zulassung durch den Europäischen Rat. Die INFODAS GmbH ist damit der weltweit einzige Cybersecurity Hersteller von Cross Domain Solutions, dessen Produkte in Deutschland, EU und NATO bis GEHEIM eingesetzt werden können. Das SDoT Security Gateway erlaubt die Filterung von strukturierten und unstrukturierten Daten. Durch die Zulassung wird die Akkreditierung von Domänenübergängen bis EU SECRET eingestuften Systemen für EU Institutionen und EU Mitgliedsstaaten einfach.

Früher setzte man auf die physische Trennung von geheimen Systemen und Daten in militärischen und behördlichen Hochsicherheitsbereichen. Dieser Ansatz steht einer konsequenten Prozessdigitalisierung (Ende zu Ende) in diesen Bereichen entgegen. Durch die Zulassungen können eingestufte Systeme EU / EC SECRET direkt mit Systemen einer niedrigeren Einstufung wie CONFIDENTIEL UE/EU CONFIDENTIAL oder RESTREINT UE/EU RESTRICTED verbunden werden. Cross Domain Solutions (CDS) werden meist mit Firewalls kombiniert, so dass geheime Systeme vor externen Gefahren, wie Malware, geschützt sind.

Die SDoT-Familie enthält neben dem Security Gateway weitere Hochsicherheitsprodukte: Das SDoT Security Gateway Express, optimiert für den bidirektionalen, latenzarmen Austausch strukturierter Daten wie XML in echtzeitnahen Szenarien, verfügt ebenso wie die SDoT Diode für den unidirektionalen Datentransfer bis 9.1 Gbit/s bereits seit längerem über eine allgemeine Zulassung bis GEHEIM, NATO SECRET und EU SECRET. Der SDoT Labelling Service erlaubt den Umgang mit unstrukturierten Daten wie MS Office Dokumente durch Datenklassifizierung mittels NATO STANAG 4774/8 konformer XML Security Labels die kryptographisch an Daten gebunden werden – und das mit einer allgemeinen Zulassung bis GEHEIM. Medienbrüche und Drehstuhlschnittstellen gehören mit SDoT der Vergangenheit an.

Das SDoT Security Gateway wird in Deutschland nach Security by Design Prinzipien entwickelt, produziert und wird kontinuierlich vom Bundesamt für Sicherheit in der Informationstechnik (BSI) evaluiert. Er ist seit über 10 Jahren in sensitiven Umgebungen im Einsatz. „Das unabhängige Urteil vom Europäischen Rat und den EU-Mitgliedsstaaten bestätigt die kontinuierliche Arbeit unseres Teams an sicheren und innovativen Netzübergängen. Die SDoT Produkte sind eine Erfolgsgeschichte für Security Made in Germany", so Dr. Alexander Schellong, VP Global Business, INFODAS GmbH.

Identität als Menschenrecht: G+D betont Bedeutung für globale Entwicklung

Nach Schätzungen der Weltbank besitzen etwa eine Milliarde Menschen bislang keine legale Identität. Für die Wahrung von Grundrechten und die Teilnahme am gesellschaftlichen Leben ist diese allerdings zwingend erforderlich. Giesecke+Devrient (G+D) unterstützt daher aktiv das UN-Nachhaltigkeitsziel, bis 2030 jedem Menschen eine rechtliche Identität zu geben und verweist auf dessen Bedeutung.

Eine legale Identität ist die Grundvoraussetzung für die gesellschaftliche, politische und finanzielle Teilhabe eines Menschen. Erst die Identität befähigt eine Person, Rechte und Pflichten in der Gesellschaft wahrzunehmen, zum Beispiel das Wahl- und Erbrecht. Auch für den Zugang zu staatlichen Gesundheits- und Sozialleistungen oder Finanzdienstleistungen ist die legale Identität unverzichtbar. Und nicht nur der einzelne Mensch, sondern auch Staaten profitieren von Identitätsnachweisen und entsprechenden Systemen. So kann die umfassende Registrierung aller Bürgerinnen und Bürger eines Landes zu einer dynamischen wirtschaftlichen Entwicklung beitragen, beispielsweise durch höhere Steuereinnahmen des Staates und bessere Planbarkeit von hoheitlichen Aufgaben.

Die Vereinten Nationen unterstreichen die hohe Bedeutung einer legalen Identität. Sie ist Bestandteil ihrer 17 Ziele für die nachhaltige Entwicklung auf ökonomischer, sozialer sowie ökologischer Ebene. Im Nachhaltigkeitsziel 16.9 fordert die UN alle Staaten auf, bis 2030 dafür zu sorgen, dass jeder Mensch eine rechtliche Identität erhält. Vor diesem Hintergrund hat die Nichtregierungsorganisation ID4Africa eine Bewegung ins Leben gerufen, die den 16. September offiziell zum „International ID Day" erklärt.

Grundvoraussetzung für eine legale Identität ist es, Infrastrukturen und Lösungen für den Identitäts- und Geburtsnachweis einzurichten. Elementare Aspekte sind dabei ein zuverlässiges Registrierungssystem, Identitätsnachweise und ein Schutz vor Identitätsmissbrauch. Vor allem muss eine sichere Personalisierung und Ausgabe von hoheitlichen Identitätsdokumenten wie Geburtsurkunden, Pässen, Personalausweisen oder Führerscheinen gewährleistet sein.

Die Bereitstellung solcher Lösungen gehört zu den Kernkompetenzen des internationalen Technologiekonzerns G+D. Das Unternehmen ist Mehrheitsgesellschafter der Veridos, einem weltweit führenden Anbieter von integrierten Identitätslösungen. In einer Vielzahl von Projekten haben beide Unternehmen bereits Infrastrukturen für Identitätslösungen von ePässen bis hin zu Führerscheinen aufgebaut. Dazu gehören Länder wie Bangladesch, Irak oder Uganda.

„Wir sind der Überzeugung, dass die legale Identität ein Menschenrecht darstellt. Nur damit können Menschen ihre Rechte und Pflichten in der modernen Welt wahrnehmen", betont Ralf Wintergerst, CEO von Giesecke+Devrient. „Zu unseren Kernfeldern gehört der Schutz und die Absicherung von Identitäten. Mit unseren Lösungen wollen wir weltweit Länder bei der Einführung von Identitätssystemen unterstützen."

Rezensionen

Kai E. Wünsche

Bienemann, Linda: Reformbedarf des Kunsturhebergesetzes im digitalen Zeitalter – Eine rechtsdogmatische Untersuchung unter besonderer Berücksichtigung der Einflüsse von DSGVO und InfoSoc-RL, Nomos Baden-Baden, 2021, 268 S., 62 €

Die Regelungen des Kunsturhebergesetzes stammen aus dem Jahr 1907 und sind seitdem weitgehend unverändert geblieben. Sie haben technische und gesellschaftliche Veränderungen wie das Aufkommen der Bildberichterstattung und des Fernsehens überstanden. Mit dem digitalen Fortschritt und den internetspezifischen Handlungsmöglichkeiten haben sich nun allerdings Umwälzungen eingestellt, welche die Frage, inwieweit die Regelungen des KUG den aktuellen Herausforderungen noch gerecht werden, mehr denn je herausfordern. Dieser Frage geht Bienemann in ihrer Arbeit von auf den Grund.

Die Arbeit gliedert sich in zwei Kapitel. Während das umfangreichere zweite Kapitel *der* Frage nachgeht, welche der Titel des Werkes nahelegt (Reformbedarf des Kunsturhebergesetzes, S. 118-241), klärt die Verf. im ersten Kapitel (S. 27-117), welcher Anwendungsbereich dem Kunsturhebergesetz neben der Datenschutzgrundverordnung verbleibt. Denn die jeweiligen Regelungsgegenstände „Bildnis" und „personenbezogene Daten" überschneiden sich in großen Teilen; und nur dann, wenn dem Kunsturhebergesetz ein eigenständiger Anwendungsbereich verbleibt, kann über eine Reform der Regelungen nachgedacht werden.

In diesem ersten Kapitel stellt Bienemann in einem ersten Abschnitt (A, S. 30-35) zunächst den Bereich dar, in dem es zu einer Kollision der Regelungswerke kommt. Dies sei nur dann der Fall, wenn es sich um ein digitales Bildnis handelt, auf dem eine lebende natürliche Person realitätstreu abgebildet ist, das in seiner Gesamtheit verbreitet oder öffentlich zur Schau gestellt wird und die abgebildete Person berechtigten Anlass zur Annahme der Erkennbarkeit wenigstens durch ihren weiteren Bekanntenkreis hat; zudem ist erforderlich, dass der Bildnisverwender/-zurschausteller über rechtlich zulässige Mittel und Zusatzinformationen verfügen kann, um die abgebildete Person zu bestimmen. Mangels Anwendbarkeit der Datenschutzgrundverordnung besteht eine Kollision dort nicht, wo das Verbreiten und öffentliche Schaustellen ausschließlich der Ausübung persönlicher oder familiärer Tätigkeiten dient (Art. 2 Abs. 2 lit. c DSGVO). Im Abschnitt B (S. 35-43) setzt sich die Verf. in angemessenem Umfang mit der in der Literatur vertretenen Ansicht auseinander, wonach Abweichungen und Ausnahmen von den Kapiteln II bis VII und IX der Datenschutzgrundverordnung nur aufgrund Art. 85 Abs. 2 DSGVO im Hinblick auf das Medienzivilrecht möglich sind. Hiernach wären dann nur noch die § 23 Abs. 1 Nr. 1 und Nr. 4, Abs. 2 KUG unmittelbar anwendbar, während es für § 23 Nr. 2 und Nr. 3, Abs. 2 KUG an einer ausreichenden Verknüpfung mit den privilegierten (journalistischen, wissenschaftlichen, künstlerischen) Zwecken des Art. 85 Abs. 2 DSGVO fehlt. Dieses Ergebnis würde allerdings, wie Bienemann überzeugend ausführt, nicht nur erhebliche Abgrenzungsschwierigkeiten schaffen, sondern auch zu unterschiedlichen Rechtsfolgen bei vergleichbaren Lebenssachverhalten führen.

Sodann kommt die Verf. zum Kernstück des ersten Kapitels (C, S. 43-80), in dem sie nach sorgfältiger Analyse zum Ergebnis kommt, dass es sich bei Art. 85 Abs. 1 DSGVO um eine fakultative allgemeine Öffnungsklausel handelt. Der gut begründbaren Gegenauffassung räumt sie dabei angemessen Platz ein. Die Einordnung der Vorschrift als fakultative allgemeine Öffnungsklausel ermöglicht, die §§ 22, 23 KUG weiter anzuwenden. Für die Interessenab-