Helmut Reimer

Report 08-2021

EU-Kommission schlägt vertrauenswürdige und sichere digitale Identität für alle Europäerinnen und Europäer vor

Die EU-Kommission hat am 03. Juni 2021 einen Rahmen für eine europäische digitale Identität (EUid) vorgeschlagen, die allen Bürgern, Einwohnern und Unternehmen in der EU zur Verfügung stehen wird. Die Bürgerinnen und Bürger werden in der Lage sein, mit einem Klick auf ihrem Handy ihre Identität nachzuweisen und Dokumente in elektronischer Form aus ihren EUid-Brieftaschen weiterzugeben. Sie werden mit ihrer in ganz Europa anerkannten nationalen digitalen Identifizierung europaweit Online-Dienste nutzen können. Sehr große Plattformen werden verpflichtet sein, die Verwendung von EUid-Brieftaschen auf Verlangen des Nutzers, beispielsweise zum Nachweis seines Alters, zu akzeptieren. Die Verwendung von EUid-Brieftaschen wird stets im Ermessen des Nutzers liegen.

Margrethe Vestager, die für das Ressort „Ein Europa für das digitale Zeitalter" zuständige Exekutiv-Vizepräsidentin, sagte: „Dank der europäischen digitalen Identität werden wir in jedem Mitgliedstaat ohne zusätzliche Kosten und mit weniger Hürden dasselbe tun können wie zu Hause, ob wir nun außerhalb unseres Heimatlandes eine Wohnung mieten oder ein Bankkonto eröffnen wollen. Und dies auf sichere und transparente Weise. Wir werden also selbst entscheiden, wie viele unserer persönlichen Informationen wir mit wem und zu welchem Zweck teilen möchten. Dies gibt uns allen die einzigartige Gelegenheit, noch besser nachzuvollziehen, was es bedeutet, in Europa zu leben und Europäerin bzw. Europäer zu sein."

Der für den Binnenmarkt zuständige EU-Kommissar Thierry Breton ergänzte: „Die Bürgerinnen und Bürger der EU erwarten nicht nur ein hohes Maß an Sicherheit, sondern auch an Benutzerfreundlichkeit – ob sie es nun mit nationalen Verwaltungen zu tun haben, z. B. um eine Steuererklärung abzugeben, oder sich an einer europäischen Universität einschreiben wollen und sich dazu ausweisen müssen. Die EUid-Brieftaschen bieten ihnen eine neue Möglichkeit, Daten für alle Arten von Dienstleistungen zu speichern und zu nutzen, angefangen bei der Abfertigung am Flughafen bis hin zur Anmietung eines Autos. Es geht darum, den Verbraucherinnen und Verbrauchern eine Wahl zu geben und zwar eine europäische Wahl. Auch unseren großen und kleinen europäischen Unternehmen wird die digitale Identität zugutekommen: Sie werden ein breites Spektrum neuer Dienstleistungen anbieten können, denn der Vorschlag liefert eine Lösung für einen sicheren und vertrauenswürdigen Identifizierungsdienst."

Der Rahmen für die europäische digitale Identität (EUid-Rahmen)

Die neue Verordnung sieht vor, dass die Mitgliedstaaten den Bürgern und Unternehmen digitale Brieftaschen zur Verfügung stellen, in denen sie ihre nationale digitale Identität mit den Nachweisen anderer persönlicher Attribute (z. B. Führerschein, Abschlusszeugnisse, Bankkonto usw.) verknüpfen können. Diese Brieftaschen können von Behörden oder privaten Einrichtungen bereitgestellt werden, sofern sie von einem Mitgliedstaat anerkannt sind.

Dank der neuen EUid-Brieftaschen werden alle Europäerinnen und Europäer online auf Dienste zugreifen können, ohne private Identifizierungsmethoden nutzen oder unnötig personenbezogene Daten weitergeben zu müssen. Mit dieser Lösung erhalten sie die volle Kontrolle über die Daten, die sie weitergeben.

Der Rahmen für die europäische digitale Identität

- wird für alle zur Verfügung stehen, die ihn nutzen wollen: Alle EU-Bürger, -Einwohner und -Unternehmen, die die europäische digitale Identität nutzen möchten, werden dies tun können.
- weithin nutzbar sein: Die EUid-Brieftaschen werden weithin verwendbar sein, um Nutzer zu identifizieren oder bestimmte persönliche Attribute nachzuweisen und ihnen so Zugang zu öffentlichen und privaten digitalen Diensten in der gesamten Union zu ermöglichen.
- den Nutzerinnen und Nutzern die Kontrolle über ihre Daten geben: Die EUid-Brieftaschen werden es den Menschen ermöglichen, darüber zu entscheiden, welche Aspekte ihrer Identität, Daten und Zertifikate sie an Dritte weitergeben, und den Überblick darüber zu behalten. Die Kontrolle durch die Nutzer sorgt dafür, dass lediglich erforderliche Informationen weitergegeben werden.

Damit der Vorschlag so bald wie möglich umgesetzt werden kann, wird er durch eine Empfehlung ergänzt. Darin fordert die Kommission die Mitgliedstaaten auf, bis September 2022 ein gemeinsames Instrumentarium zu schaffen und unverzüglich mit den erforderlichen Vorarbeiten zu beginnen. Dieses Instrumentarium sollte die technische Architektur, Normen, Leitlinien und bewährte Verfahren umfassen.

Nächste Schritte

Parallel zum Gesetzgebungsverfahren wird die Kommission mit den Mitgliedstaaten und dem Privatsektor an den technischen Aspekten der europäischen digitalen Identität arbeiten. Die Kommission wird die Umsetzung des Rahmens für die europäische digitale Identität als Teil des Programms „Digitales Europa" unterstützen. Zudem sehen viele Mitgliedstaaten in ihren nationalen Plänen im Rahmen der Aufbau- und Resilienzfazilität Projekte zur Umsetzung von Lösungen für elektronische Behördendienste, einschließlich der europäischen digitalen Identität, vor.

Hintergrund

Der Digitale Kompass 2030 der Kommission enthält eine Reihe von Vorgaben und Etappenzielen, zu deren Verwirklichung die europäische digitale Identität beitragen wird. So sollen bis 2030 beispielsweise alle öffentlichen Dienste online verfügbar sein, alle Bürgerinnen und Bürger Zugang zu ihren elektronischen Patientenakten haben und 80 % der Bevölkerung eine eID-Lösung nutzen.

Bei dieser Initiative baut die Kommission auf dem bestehenden grenzüberschreitenden Rechtsrahmen für vertrauenswürdige digitale Identitäten sowie auf der Initiative für elektronische Iden-

tifizierung und Vertrauensdienste in Europa (eIDAS-Verordnung) auf. Dieser Rahmen wurde 2014 geschaffen und bildet die Grundlage für die grenzüberschreitende elektronische Identifizierung, Authentifizierung und Zertifizierung von Websites in der EU. Rund 60 % der Europäerinnen und Europäer können bereits vom derzeitigen System profitieren.

Die Mitgliedstaaten sind derzeit jedoch nicht verpflichtet, überhaupt ein nationales digitales Identifizierungsmittel zu entwickeln und dafür zu sorgen, dass es mit denen anderer Mitgliedstaaten interoperabel ist. Dies führt zu großen Unterschieden zwischen den Ländern. Mit dem vorliegenden Vorschlag werden diese Mängel behoben, indem die Wirksamkeit des Rechtsrahmens verbessert und sein Nutzen auf den Privatsektor und die mobile Nutzung ausgeweitet wird.

Wachsende Gefahr durch OAuth-Attacken

Mit den bereits vor einigen Jahren eingeführten Applikationen auf Basis von Open Authorization (OAuth) konnten die großen Cloud-Plattformen wie Microsoft 365 und Google Workspace ihren Funktionsumfang vergrößern und gleichzeitig ihre Benutzeroberflächen verbessern. Allerdings begründen diese Apps auch einen neuen Bedrohungsvektor, da Cyberkriminelle verstärkt gefährliche OAuth 2.0-Anwendungen (bzw. Cloud-Malware) einsetzen, um Daten zu stehlen und auf sensible Informationen zuzugreifen. Allein im Jahr 2020 entdeckte der US-amerikanische Cybersicherheits-Experte Proofpoint mehr als 180 dieser gefährlichen Anwendungen. Über 55 Prozent der Kunden des Unternehmens waren davon betroffen und die Erfolgsquote der Angriffe lag bei 22 Prozent – ein äußerst bedenklicher Wert in Zeiten wachsender Cyberrisiken.

Im Zuge seiner Untersuchungen konnte Proofpoint eine Vielzahl von Attacken mittels OAuth-Token-Phishing bzw. dem Missbrauch von OAuth-Apps beobachten. Diese Form von Cyberattacke ist für Angreifer geradezu ideal, um sich Zugang zu einem Unternehmen zu verschaffen, Angriffe auf Mitarbeiter zu initiieren und Dateien sowie E-Mails von Cloud-Plattformen zu stehlen. App-Angriffe mittels OAuth zielen oft auf die Konten des höheren Managements, von Account Managern, Personalverantwortlichen und auf die Finanzabteilung ab – also auf genau die Art von Benutzern, die Zugriff auf hochsensible Daten haben. Ist ein Angriff erst einmal erfolgreich, haben die Cyberkriminellen dauerhaften Zugriff auf E-Mails, Dateien, Kontakte, Notizen, Microsoft Teams-Chats und vieles mehr. In einigen Fällen leiten sie die Benutzer auch auf eine Phishing-Seite um, nachdem diese der Nutzung der Anwendung zugestimmt haben.

Gefährliche OAuth-Apps

Im vergangenen Jahr nutzten Cyberkriminelle eine Vielzahl von Techniken für ihre OAuth-Attacken wie die Imitierung von Anwendungen (durch Homoglyphen und gefälschte Logos bzw. Domains). Es kamen zudem unterschiedliche Köder zum Einsatz, so z.B. COVID-19, eine vorgebliche Mail-Quarantäne und Office-Reviews von Kollegen. Die ausgeklügelten Angriffe stützten sich dabei zuweilen sogar auf Microsofts eigene Plattform, um Einladungen zur Zustimmungsseite für gefährliche Anwendungen zu generieren.

Nähere Informationen zur wachsenden Gefahr durch OAuth-Angriffe finden Sie im aktuellen Blogpost von Proofpoint.

XDR-Lösung von Sophos synchronisiert Endpoint-, Server-, Firewall- und E-Mail-Sicherheit

Sophos stellte am 05.Mai 2021 seine neue Lösung Sophos XDR vor. Dabei handelt es sich um die einzige Extended Detection and Response (XDR)-Lösung der Branche, die Endpoint-, Server-, Firewall- und E-Mail-Sicherheit synchronisiert. Mit diesem umfassenden und integrierten Ansatz bietet Sophos XDR einen ganzheitlichen Überblick über die Security-Umgebung eines Unternehmens, kombiniert mit einem umfangreichen Datensatz sowie tiefgreifenden Analyse-Möglichkeiten zur Erkennung und Untersuchung von Cyberbedrohungen inklusive entsprechender Reaktionsmaßnahmen. So lassen sich selbst raffinierteste Angriffe abwehren – insbesondere solche, die mehrere Zugangspunkte nutzen und sich zunächst unauffällig im Netzwerk bewegen, um der Erkennung zu entgehen.

Detaillierte Bedrohungsanalyse mit umfangreichem Datensatz

Das Herzstück von Sophos XDR ist einer der branchenweit umfangreichsten Datensätze: Es werden zum einen bis zu 90 Tage On-Device-Daten und zum anderen bis zu 30 Tage produktübergreifende Daten im Cloud-basierten Data Lake gespeichert. Der einzigartige Ansatz, On-Device- und Data-Lake-Forensik zu kombinieren, bietet umfassende und kontextbezogene Einblicke. Diese können von Sicherheitsanalysten über Sophos Central und offene Anwendungsprogrammierschnittstellen (APIs) zur Einbindung in folgende Systeme genutzt werden: Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Professional Service Automation (PSA) und Remote Monitoring and Management (RMM).

Der Data Lake enthält wichtige Informationen von Intercept X, Intercept X für Server, Sophos Firewall und Sophos E-Mail. Sophos Cloud Optix und Sophos Mobile werden im Laufe des Jahres ebenfalls in die Datensammlung eingespeist. Dadurch sind Sicherheits- und IT-Teams in der Lage, einfach auf diese Daten zuzugreifen, um produktübergreifende Bedrohungsuntersuchungen durchzuführen und schnell granulare Details zu vergangenen und aktuellen Angriffsaktivitäten zu erhalten. Die Verfügbarkeit des Offline-Zugriffs auf historische Daten schützt zusätzlich vor verlorenen oder beeinträchtigten Geräten.

Neue EDR-Version

Weiterhin hat Sophos eine neue Version seiner branchenführenden Endpoint Detection and Response-Lösung Sophos EDR veröffentlicht. Neue zeitgesteuerte Abfragen und anpassbare kontextbezogene Pivoting-Funktionen bieten Sicherheitsanalysten und IT-Administratoren eine schnelle und präzise Identifizierung und Untersuchung von Sicherheitsproblemen, um schnell und gezielt reagieren zu können. Durch die Integration mit dem Data-Science-Tool SophosLabs Intelix liefert die neue Version vorkonfigurierte Abfragen und leistungsstarke Threat-Intelligence-Funktionen. Sophos EDR-Kunden können im Data Lake auf Daten zugreifen, die sieben Tage in der Cloud gehostet sind (erweiterbar auf 30 Tage). Bei On-Device-Daten ist dies bis zu 90 Tagen möglich.

Sophos Adaptive Cybersecurity Ecosystem

Sophos XDR und EDR sind Teil des Sophos Adaptive Cybersecurity Ecosystem (ACE), einer neuen, offenen Sicherheitsarchitektur zur

Optimierung von Threat Prevention, Detection und Response. Sophos ACE nutzt Automatisierung und Analysen sowie den kollektiven Input von Sophos-Produkten, -Partnern, -Kunden sowie Entwicklern und anderen Security-Anbietern. So schafft diese Architektur einen Schutz, der sich kontinuierlich verbessert; das System lernt ständig dazu und entwickelt sich weiter. Sophos ACE baut auf eine umfangreiche Datensammlung auf und korreliert verwertbare Erkenntnisse aus Sophos-Lösungen und -Services sowie Threat Intelligence aus den SophosLabs, Sophos AI und dem Sophos Managed Threat Response-Team. Offene Anwendungsprogrammierschnittstellen (APIs) ermöglichen es Kunden, Partnern und Entwicklern, Tools und Lösungen zu erstellen, die mit dem System interagieren und die Vorteile bestehender Integrationen nutzen können. Sophos ist mit diesem Ansatz führend in der Branche und arbeitet bereits mit vielen Anbietern zusammen.

Die Wichtigkeit eines interagierenden und auf möglichst vielen Datensätzen beruhenden IT-Security-Systems wird in der neuen Sophos-Studie „Intervention halts a ProxyLogon-enabled attack" deutlich, die einen Angriff auf ein großes Unternehmen beschreibt. Die Attacke begann damit, dass die Angreifer einen Exchange-Server mit dem aktuellen ProxyLogon-Exploit kompromittierten und sich unbemerkt durch das Netzwerk bewegten. So konnten sie über einen Zeitraum von zwei Wochen Account-Anmeldeinformationen entwenden, Domain-Controller kompromittieren und sich auf mehreren Rechnern einnisten. Dabei verwendeten sie ein kommerzielles Remote-Access-Tool, um den Zugang zu den gehackten Rechnern aufrechtzuerhalten und eine Reihe von bösartigen Programmen zu verteilen. Die Studie zeigt, dass die Angreifer immer wieder zurückkehrten. Dabei setzten sie manchmal das gleiche Tool, wie beispielsweise Cobalt Strike, manchmal aber auch andere Tools auf verschiedenen Rechnern ein. Sie verwendeten ein kommerzielles Fernzugriffsprogramm und nicht das eher standardmäßige RDP, nach dem IT-Security-Spezialisten normalerweise suchen.

Dan Schiappa, Chief Product Officer bei Sophos. „Der Report verdeutlicht die Komplexität von Cyberangriffen, die von Menschen durchgeführt werden, und zeigt, wie schwierig es für IT-Sicherheitsteams ist, mehrstufige Vorfälle mit mehreren Vektoren zu verfolgen und einzudämmen. Oftmals ist es schlicht unmöglich, mit den Angriffsaktivitäten Schritt zu halten, die in allen Teilen des Unternehmens stattfanden. Laut dem Ende April veröffentlichten Sophos-Report State of Ransomware ist dieses Problem weit verbreitet. Mehr als 54 Prozent der befragten IT-Manager gaben an, dass Cyberangriffe zu weit fortgeschritten sind, als dass ihre IT-Teams sie alleine bewältigen könnten. XDR ist hier eine wichtige Verteidigungskomponente."

Verfügbarkeit

Sophos XDR sowie die aktualisierten EDR-Funktionen für Intercept X Advanced with EDR und Intercept X Advanced for Server with EDR sind ab dem 19. Mai weltweit über Sophos Partner erhältlich. Partner und Kunden können alle XDR- und EDR-Produktlösungen auf der Cloud-basierten Sophos Central-Plattform über eine einzige Benutzeroberfläche einfach verwalten.

Hohe Risiken für Patientendaten und medizinische Forschungsergebnisse

Der neue Datenrisiko-Report vom 11. Mai 2021 für den Gesundheitssektor von Varonis Systems, Inc., zeigt ein enormes Ausmaß an Exposition interner und sensibler Dateien in Krankenhäusern, Biotech- und Pharmaunternehmen. So hat jeder Mitarbeiter durchschnittlich Zugriff auf knapp 11 Millionen Dateien, was knapp 20 Prozent des gesamten Datenbestands entspricht. Besonders kritisch: Im Durchschnitt sind 12 Prozent der sensiblen Daten, wie Forschungsergebnisse, geistiges Eigentum und Gesundheitsdaten, für jeden Mitarbeiter zugänglich. In kleineren Krankenhäusern und Unternehmen (bis 500 Mitarbeiter) beträgt dieser Wert sogar 22 Prozent. Für den Report wurden rund drei Milliarden Dateien im Rahmen von Datenrisikobewertungen bei 58 Healthcare-Unternehmen weltweit (unter anderem in den USA, Deutschland, Frankreich und UK) analysiert.

„Der medizinische Bereich kämpft derzeit an mehreren Fronten: So müssen Krankenhäuser nicht nur Pandemie-Opfer versorgen und Pharmaunternehmen die Herstellung von Impfstoffen vorantreiben, sondern gleichzeitig auch eine steigende Anzahl an Cyberangriffen abwehren"; erklärt Michael Scheffler, Country Manager DACH von Varonis. „Allein im letzten Jahr wurden bis November laut Bundesregierung in Deutschland 43 erfolgreiche Angriffe auf Gesundheitsdienstleister registriert – und eine Entspannung der Lage ist nicht in Sicht."

Neben der verschärften Bedrohungslage muss vor allem aber auch die eigene Cyberhygiene und das damit verbundene Datenrisiko in den Blick genommen werden. Die jüngste Untersuchung zeigt verschiedene Problemfelder auf, welche die Gefährdung durch Datenschutzverletzungen, Insider-Bedrohungen und Ransomware-Angriffe zusätzlich deutlich vergrößern:

Zu weit gefasste Zugriffsrechte:

Im Durchschnitt sind 31.000 sensible Dateien (wie vertrauliche Forschungsergebnisse, geistiges Eigentum sowie Gesundheits- und andere personenbezogene Daten) für jeden Mitarbeiter zugänglich. Hierbei handelt es sich um besonders sensible Informationen, die enormen Schaden verursachen können. Darüber hinaus vergrößern exzessive Zugriffsrechte die potenziellen Auswirkungen eines Cyberangriffs, da sämtliche Daten, auf die ein kompromittiertes Konto zugreifen kann, entwendet und/oder verschlüsselt werden können (Ransomware).

Zeitlich unbegrenzte Passwörter geben Cyberkriminellen ausreichend Zeit für ihre Angriffe. 77 Prozent der Krankenhäuser und Unternehmen verfügen über mehr als 500 unbefristete Nutzer-Passwörter.

Nicht mehr benötigte, aber noch vorhandene Nutzerkonten und Daten: Durchschnittlich werden mehr als zwei Drittel der Dateien (69 %) nicht mehr genutzt, erhöhen jedoch das Risiko für Verstöße gegen Vorschriften wie die DSGVO und stellen für Angreifer eine interessante Beute dar. Nicht mehr benötigte, aber nicht deaktivierte Nutzerkonten, erlauben ehemaligen Mitarbeitern und Partnern unnötigen Zugang zu Informationen und eignen sich ideal für Cyberkriminelle, um sich unauffällig in den Systemen zu bewegen. 79 Prozent der Unternehmen verfügen über mehr als 1.000 solcher Konten.

Der komplette Report kann hier heruntergeladen werden: *https://www.varonis.com/blog/2021-healthcare-data-risk-report/*

TeleTrusT unterstützt Initiative gegen Mitwirkungspflicht für Kommunikationsdienste

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) unterstützt gemeinsam mit anderen Verbänden und Unternehmen eine konzertierte Initiative gegen die geplante Mitwirkungspflicht für Kommunikationsdienste bei staatlicher Überwachung und gegen die gezielte Schwächung von Verschlüsselung.

Mit Blick auf das anstehende „Gesetz zur Anpassung des Verfassungsschutzrechts" wenden sich Fachkreise gegen eine Ausweitung staatlicher Überwachung und die Schwächung verschlüsselter Kommunikation von Nutzern digitaler Dienste wie E-Mail, VoiP oder Messenger-Anwendungen. Unter der Federführung von facebook Deutschland wird anlässlich der für den 14.05.2021 angesetzten Expertenanhörung im BT-Innenausschuss ein detailliertes Schreiben an Mitglieder des Deutschen Bundestages bzw. die Bundesregierung übersandt.

Im Besonderen geht es dabei um vorgesehene Mitwirkungspflichten für Unternehmen bei der Implementierung von Überwachungsmaßnahmen der Nachrichtendienste und Sicherheitsbehörden. Aus Sicht der Unterzeichner sind Folgewirkungen gravierend für die Cybersicherheit in Deutschland. Beispielsweise drohen nicht nur ernste Gefahren für die sichere Kommunikation zwischen Journalistinnen und Journalisten mit ihren Quellen, sondern ist verschlüsselte Kommunikation oftmals das einzige Mittel für zivilgesellschaftliche Organisationen, um mit besonders Schutzbedürftigen in Verbindung zu treten.

Bedenken und Kritik richten sich gegen die weite und unklare Fassung der Mitwirkungspflicht, wonach ausdrücklich alle Telekommunikationsdienste – was auch Messenger und E-Mail umfasst – Nachrichtendienste bei der Realisierung von Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) unterstützen sollen. So könnten zukünftig Messenger-Dienste wie beispielsweise Threema, Signal oder WhatsApp, aber auch E-Mail- oder Videokonferenzdienste je nach Gesetzesauslegung mit Anfragen und dem Verlangen von Sicherheitsbehörden konfrontiert werden, Schadsoftware auf den Endgeräten der Nutzer zu platzieren. Anbieter müssten potentielle Sicherheitslücken vorhalten. Die Kenntnis darüber könnte fremden Nachrichtendiensten oder Cyberkriminellen nützlich sein. Damit konterkariert die Anpassung des Verfassungsschutzrechts auch die erst kürzlich verabschiedete Novelle des IT-Sicherheitsgesetzes (ITSIG 2.0) und das Datenschutzrecht allgemein, denn einerseits sollen Anbieter größtmögliche Vertraulichkeit und Datensicherheit gewährleisten, andererseits könnten sie zur Mitwirkung bei der Schwächung IT-Sicherheit zum Zwecke staatlicher Ausspähung verpflichtet werden.

Sichere Verschlüsselung ist darüber hinaus ein bedeutsamer Wirtschaftsfaktor. Für viele IT-Unternehmen ist das Angebot sicherer und verschlüsselter Kommunikation (insbesondere mittels Technologie „Made in Germany"/"Made in the EU") auch ein wichtiges und wachsendes Geschäftsfeld. Sollten aufstrebende Unternehmen künftig dazu verpflichtet werden können, Behörden Zugang zur Kommunikation ihrer eigenen Geschäftskreise zu gewähren, wird dies zu einem Vertrauensverlust gegenüber einer ganzen Zukunftsbranche führen. Die Vorhaben der Bundesregierung sind damit vor allem auch schädlich für die Innovationskraft der hiesigen Digitalwirtschaft.

INFODAS: SDoT Diode und Gateway Express für den Einsatz in Fahrzeugen

Der Erfolg von militärischen Operationen hängt zunehmend von der digitalen Vernetzung sämtlicher Einheiten, Sensoren und Effektoren ab. Basierend auf den bis GEHEIM, NATO SECRET und EU SECRET zugelassenen SDoT Cross Domain Solutions, wurde die robuste COMP-LAND Serie für den Einsatz auf taktischer Ebene u.a. in Fahrzeugen entwickelt und am 17. Mai 2021 veröffentlicht. Feuchtigkeit, Wärme, Staub oder Vibration stehen dem digitalen Datenaustausch zwischen normalerweise abgeschotteten Systemen unterschiedlicher Geheimhaltungsstufen nicht mehr im Weg.

Der schnelle und kontrollierte Datenaustausch zwischen mobilen, verlegefähigen und stationären Systemen unterschiedlicher Einstufungen unabhängig von ihrer Lage ist Grundlage der militärischen Zukunftsplanungen der NATO Staaten. Dies erhöht die Reaktionsgeschwindigkeit, spart Bandbreite oder Platz in Fahrzeugen durch die direkte Verbindung von Systemen an entfernte Speicher und Computing Umgebungen oder relevante Einheiten mit restriktiveren Zugriffsrechten auf eingestufte Informationen. Das bidirektionale SDoT Security Gateway Express und die unidirektionale SDoT Diode sind nun zusätzlich zur 19-Zoll-Version auch als COMPACT-LAND (COMP-LAND) für den Einsatz in mobilen Systemen und unter extreme Einsatzumgebungen verfügbar.

SDoT COMP-LAND unterstützt TCP und UDP-basierte Kommunikation unter anderem über HTTP/S sowie SMTP/S und erlaubt das Filtern zahlreicher Datenformate wie JREAP, JSON, XML, ASCA, ASTERIX, NMEA, DIS, HLA oder ADatP3. SDoT Produkte werden in Deutschland nach Security by Design Prinzipien entwickelt, produziert und kontinuierlich vom Bundesamt für Sicherheit in der Informationstechnik (BSI) evaluiert. Sie sind im NATO Information Assurance Product Catalogue (NIAPC) gelistet und sind ITAR frei, unterliegen jedoch der Exportkontrolle.

„Daten und Datenaustausch sind stärker denn je Kernelemente zukünftiger Systemarchitekturen Rüstungsvorhaben Mit COMP-LAND erlauben wir der Bundeswehr und Herstellern von Rüstungsgütern den Datenaustausch zwischen Systemen unterschiedlicher Einstufungen auch unter extremen Einsatzbedingungen zu realisieren", so Marc Akkermann, Director National Sales der INFODAS GmbH. „Die SDoT Produktfamile bietet darüber hinaus Betreibern kritischer Infrastrukturen (KRITIS) die Möglichkeit IT/OT Verbindungen für Anlagen in dislozierten Lokationen sicher herzustellen".

150 Millionen Angriffs-E-Mails in 2020, Tendenz weiter steigend

Fast 60 Millionen Angriffs-Mails via Microsoft 365 und 90 Millionen via Google – das ist die erschreckende Bilanz, die der US-Cybersecurity-Spezialist Proofpoint am 20, Mai 2021 nach einer Analyse der Cyberbedrohungen für 2020 veröffentlicht hat. Cyberkriminelle nutzen ganz offensichtlich die umfangreiche Funktionalität und nahezu grenzenlose Skalierbarkeit von Diensten wie Microsoft 365, Azure, OneDrive, SharePoint, G-Suite und Firebase Storage um digitale Angriffe auszuführen. Mehr als ein Viertel davon (27 %) liefen über den Google-Mail-Service Gmail. Da es sich hier ausschließlich um eine Analyse von Angriffen handelt, die auf Kunden von Proofpoint abzielten, ist der tatsächliche Wert kaum zu ermitteln. Der Trend ist jedoch ungebrochen, im ersten Quartal 2021

wurden bereits mittels Microsoft 365 sieben Millionen gefährliche Nachrichten verbreitet und im Falle weiterer 45 Millionen nutzten die Täter die Google-Infrastruktur.

Das Volumen gefährlicher Nachrichten, die mittels dieser in der Wahrnehmung vieler doch sehr vertrauenswürdigen Cloud-Dienste versendet wurden, übertraf dabei sogar das aller Botnets im Jahr 2020. Da die Angreifer hierzu eben auch Domains wie „outlook.com" und „sharepoint.com" nutzen, die bisher häufig als seriöse Quelle galten, wird die Erkennung von Attacken immer schwieriger. Daraus resultiert auch, dass etwa die Hälfte aller betroffenen Unternehmen anschließend mit mindestens einer Kompromittierung konfrontiert war. Bei einem Drittel der von einer Kompromittierung betroffenen Organisationen wiederum konnten Aktivitäten wie Dateimanipulation, E-Mail-Weiterleitung und Vorfälle in Zusammenhang mit OAuth festgestellt werden.

Gleichzeitig missbrauchen Angreifer diese Konten sodann, um scheinbar legitime E-Mails an Kolleginnen und Kollegen, Kunden oder Partner im Namen des Mitarbeiters oder der Mitarbeiterin zu versenden, beispielsweise um ausstehende Zahlungen von Rechnungen oder Gehälter auf Konten der Kriminellen umzuleiten.

Es gilt also, wirklich bei jeder Nachricht die Augen offen zu halten und im Zweifel über einen anderen Kanal, der andere Anmeldedaten nutzt, also z.B. per Telefon nachzufragen, ob die angeblich neuen Kontodaten wirklich diejenigen des mutmaßlichen Absenders oder der Absenderin sind.

Bilanz nach drei Jahren DSGVO

Die DSGVO hat in Sachen Grundrechtsschutz eine Vorreiter-Rolle gespielt, viele Staaten sind mittlerweile ihrem Beispiel gefolgt. Ihre Grundsätze sind Bedingungen für eine lebenswerte, digitale Gesellschaft. Doch bisherige Rechtslücken werfen viele Fragen auf – und werden vor allem von mächtigen Datenverarbeitern, wie globalen Konzernen, ausgenutzt.

„Der größte Erfolg der Datenschutz-Grundverordnung ist, dass sie die Werte zum Ausdruck bringt, auf die sich die Mitgliedstaaten der Europäischen Union für ihren Weg in die digitale Gesellschaft geeinigt haben. Ihre Grundsätze, um die Grundrechte auf Datenschutz und Selbstbestimmung auszugestalten, sind Bedingungen für eine lebenswerte Gesellschaft", so Alexander Roßnagel, Sprecher des Forschungsverbunds „Forum Privatheit" und Professor für Öffentliches Recht an der Universität Kassel am 02. Juni 2021.

Denn die DSGVO fordere eine ausreichende Transparenz der Datenverarbeitung für die betroffenen Personen, die Bindung der Datenverarbeitung auf die Zwecke einer legitimen Datenerhebung, die Minimierung des Personenbezugs der Daten auf das zur Zweckerreichung Notwendige und die Gewährleistung von Datenschutz durch die technisch-organisatorische Gestaltung der Verarbeitungssysteme. „Damit zeigt die Verordnung einen dritten Weg der weltweiten Digitalisierung auf – zwischen der Kontrolle des Alltagslebens in China und der Datenausbeutung des kalifornischen Digitalkapitalismus", konstatiert Roßnagel. Diesen Weg wollten mittlerweile viele Staaten der Welt mitgehen und gäben sich Datenschutzgesetze, die an der Datenschutz-Grundverordnung orientiert sind.

Einheitlich verbindliche Regelungen für den Datenschutz in der gesamten Europäischen Union

Für den zunehmenden Umgang mit personenbezogenen Daten bietet die Datenschutz-Grundverordnung erstmals einheitliche unmittelbar verbindliche Regelungen für den Datenschutz in der gesamten Europäischen Union. Sie hat damit die Diskussion über Notwendigkeit und Inhalt des Datenschutzes gefördert und den Respekt vor den Grundrechten der betroffenen Personen gestärkt. Insbesondere mit ihren am Wettbewerbsrecht orientierten Sanktionsdrohungen, aber auch mit ihrer Etablierung unabhängiger, starker Aufsichtsbehörden hat sie viel Aufmerksamkeit für den Datenschutz bewirkt.

Trotz dieser Stärkung des Datenschutzes waren die Befürchtungen vor einer unangemessenen Datenschutzbürokratie übertrieben. Die Praxis hat gezeigt, dass die Umstellung auf die neue Datenschutzordnung am Ende gar nicht so aufwändig war, wie ihre Gegner vorausgesagt hatten. Die Datenschutz-Grundverordnung führt weit überwiegend die Regelungen der in Deutschland geltenden vorherigen Datenschutz-Richtlinie fort. Wer sich vor der Geltung der Datenschutz-Grundverordnung bereits an die Datenschutzregeln gehalten hatte, musste nur wenig in seiner praktischen Arbeit umstellen. Gesetzgeberische Innovationen der Verordnung wie der Erlass von Verhaltensregeln oder die Zertifizierung von Verarbeitungsvorgängen sind in der Praxis noch kaum angenommen worden. Sie könnten zu weiteren Erleichterungen führen.

Die Intention war gut – doch bisher bleibt Manches hinter den Erwartungen zurück

Drei Jahre Datenschutzpraxis lassen aber auch Schwachstellen der Datenschutz-Grundverordnung immer deutlicher werden. Sie hat zum einen nicht zu einer einheitlichen Datenschutzpraxis in der Europäischen Union geführt: Die Abstraktheit vieler Regelungen lässt Raum für unterschiedliche Interpretationen und die vielen Öffnungsklauseln eröffnen Spielräume für divergierende Gesetze in den Mitgliedstaaten. Hinsichtlich der Abstimmung der unabhängigen Aufsichtsbehörden hat sie komplizierte Verfahren vorgesehen, die eine einheitliche Zielsetzung und einen Kulturwandel voraussetzen, der (noch) fehlt. Zum anderen hat sie die notwendige Modernisierung des Datenschutzes angesichts der Herausforderungen von modernsten Informationstechniken wie Big Data, Internet der Dinge oder Künstlicher Intelligenz verfehlt: Sie enthält überwiegend abstrakte, technik- und risikoneutrale Regelungen, die in der Praxis nur schwer und hochumstritten zu konkretisieren sind. Beispiele hierfür sind etwa die notwendige Abwägung bei datengetriebenen Geschäftsmodellen zwischen berechtigten Interessen des Verantwortlichen und schutzwürdigen Interessen der betroffenen Person, ohne dass die Verordnung hierfür geeignete Kriterien vorgibt. Ein anderes Beispiel sind die unzähligen Streitverfahren über den Umfang des Auskunftsanspruchs. Die mangelnde Bestimmtheit vieler Regelungen der Verordnung bindet täglich Millionen von Arbeitsstunden und behindert Innovationen und Investitionen.

Rechtslücken werden vor allem von mächtigen Datenverarbeitern ausgenutzt

In Lücken, die das Recht lässt, dringt immer gesellschaftliche Macht ein. Solche Lücken werden vor allem von globalen Konzernen und anderen mächtigen Datenverarbeitern genutzt, um ihre Interessen – oft zu Lasten der betroffenen Personen – durchzusetzen. Defizite in der Gesetzgebung nachträglich auszugleichen, verursacht sehr viel Arbeit für die Aufsichtsbehörden. Fortschritte in der Datenschutzpraxis zeigen sich vor allem dort, wo der Europäische Datenschutzausschuss, die Konferenz der unabhängigen Aufsichtsbehörden des Bundes und der Länder oder einzelne Aufsichtsbehör-

den für Rechtsklarheit gesorgt haben – aber immer unter dem Risiko, dass diejenigen, die damit nicht einverstanden sind, die Gerichte anrufen. Dies hätte oft durch wenige risikoorientierte Festlegungen des Unionsgesetzgebers vermieden werden können.

„Die europäische und die deutsche Gesetzgebung sollte für künftige Digitalisierungsprojekte aus den Erfahrungen mit der Datenschutz-Grundverordnung lernen", meint Forum Privatheit-Sprecher Alexander Roßnagel.

Dieser Wunsch scheint zumindest bei der Europäischen Kommission angekommen zu sein. In ihrem Entwurf für eine Verordnung zur Regulierung künstlicher Intelligenz hat sie die strikte Technik- und Risikoneutralität in der Regulierung aufgegeben und regelt bereichs- und anwendungsspezifisch, wie Risiken für Grundrechte durch Künstliche Intelligenz abgewehrt werden können.

Im Forum Privatheit setzen sich Expertinnen und Experten aus sieben wissenschaftlichen Institutionen interdisziplinär, kritisch und unabhängig mit Fragestellungen zum Schutz der Privatheit auseinander. Das Projekt wird vom Fraunhofer ISI koordiniert. Weitere Partner sind das Fraunhofer SIT, die Universität Duisburg-Essen, das Wissenschaftliche Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel, die Eberhard Karls Universität Tübingen, die Ludwig-Maximilians-Universität München sowie das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein. Das Bundesministerium für Bildung und Forschung fördert das Forum Privatheit, um den öffentlichen Diskurs zu den Themen Privatheit und Datenschutz anzuregen.

Empfehlungen zum Datentransfer in Drittländer nach dem „Schrems II"-Urteil

Der Europäische Datenschutzausschuss (EDSA) gibt Empfehlungen zu ergänzenden Maßnahmen für Übertragungsinstrumente zur Gewährleistung des EU-Schutzniveaus. Eine Roadmap in englischer Sprache informert über die Schritte einer zulässigen Datenübermittlung. Außerdem gibt der EDSA Hinweise zu grundlegenden europäischen Garantien für Überwachungsmaßnahmen.

Beide Dokumente wurden im Anschluss an das „Schrems II"-Urteil des Europäischen Gerichtshofs (EuGH) von den europäischen Datenschutzaufsichtsbehörden ausgearbeitet. Ziel ist die einheitliche Anwendung der Datenschutz-Grundverordnung (DS-GVO) und des Urteils.

Die Empfehlungen zu den ergänzenden Maßnahmen werden bis zum 30. November 2020 einer öffentlichen Konsultation unterzogen.

Als Folge des „Schrems II"-Urteils sind für die Verantwortlichen weitere Pflichten entstanden. Sie sind verpflichtet zu prüfen, ob das Recht des Drittlandes für die übermittelten personenbezogenen Daten im Wesentlichen ein im Europäischen Wirtschaftsraum garantiertes Schutzniveau gewährleistet. Das betrifft insbesondere das Instrument der Standardvertragsklauseln (SCC).

Wenn die in den SCCs enthaltenen Schutzmaßnahmen für die Übermittlung in ein bestimmtes Drittland nicht ausreichen, fordert der EuGH ergänzende Maßnahmen.

Die Empfehlungen unterstützen die Verantwortlichen und Auftragsverarbeiter, die als Datenexporteure tätig sind, bei ihrer Pflicht, geeignete ergänzende Maßnahmen aufzufinden und umzusetzen. Dazu enthalten die Empfehlungen Prüfschritte,

Beispiele für zusätzliche Maßnahmen und Bedingungen für die Wirksamkeit von zusätzlichen Maßnahmen.

Außerdem hat der EDSA dazugehörige Empfehlungen zu den grundlegenden europäischen Garantien für Überwachungsmaßnahmen verabschiedet. Diese helfen Datenexporteuren festzustellen, wie der Rechtsrahmen im Drittland, der den Zugang von Behörden zu Daten für Überwachungszwecke regelt, die Verpflichtungen des Übertragungsinstruments nach Artikel 46 DS-GVO berührt.

Datenexporteure müssen ihren Entscheidungsprozess wegen der Rechenschaftspflicht gründlich dokumentieren. Die Datenexporteure sind dafür verantwortlich, die konkrete Beurteilung im Zusammenhang mit der Übermittlung, dem Recht des Drittlandes und dem Übertragungsinstrument, auf das sie sich stützen, vorzunehmen.

Verbraucherdaten in Treuen Händen?

Mit der zunehmenden Digitalisierung durchdringen internetbasierte Dienste den Konsumalltag von Verbraucher:innen. Der Schutz der eigenen Daten wird immer komplexer und aufwändiger. Verbraucher:innen müssen sich mit einer Vielzahl von Sicherheits- und Datenschutzthemen auseinandersetzen, die sich zudem häufig ändern. Dabei wird die Verantwortung für die digitale Selbstbestimmung vor allem den Verbraucher:innen zugeschoben, ohne dass diese in die Lage versetzt werden, diese Verantwortung auch übernehmen zu können.

Eine Möglichkeit zur Entlastung der Verbraucher:innen sind Datentreuhänder, die insbesondere durch die Fokussierung auf Personal Information Management-Systemen (PIMS) im Gutachten der Datenethikkommission aus dem Jahr 2019 in den Fokus geraten sind. Der Begriff des Datentreuhänders ist aber nicht klar definiert, unterschiedliche Dienste und Angebote fallen unter diesen Oberbegriff.

Deshalb möchte die Verbraucherzentrale NRW mit Unterstützung durch das Institut für Verbraucherinformatik der Hochschule Bonn-Rhein-Sieg (IVI) die wissenschaftliche Expertise zum Thema Datentreuhänder in einer durch das Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen geförderten Online-Vortragsreihe bündeln und mit verbraucherpolitischen Akteuren sowie einer interessierten Öffentlichkeit diskutieren. Angesichts des fortschreitenden Tempos der europäischen und nationalen Regulierung in diesem Bereich und der aktuellen Unklarheit über Ausgestaltung, Rolle und Zielsetzung ist eine wissenschaftliche Auseinandersetzung über dieses Thema unerlässlich.

Geplant sind monatliche Vortragstermine, die separat angekündigt werden. Der letzte Vortrag ist für den Februar 2022 geplant. Zur Vortragsreihe gibt es einen Call for Papers. Interessierte Wissenschaftler:innen können bis zum 17. Januar 2022 ihre Beiträge einreichen.

Die Reihe startete im Rahmen des bundesweiten Digitaltags 2021 am 18. Juni 2021.

Weitere Informationen zu der Online-Vortragsreihe, zur An-meldemöglichkeit und zum Call for Papers: *www.verbraucherforschung.nrw/zu-treuen-haenden-tagungsreihe-datenintermediaere-datentreuhaender-60831*

Künstliche Intelligenz / Menschen gehen mit Maschinen rücksichtslos um

Wissenschaftler der Ludwig Maximilians Universität München (LMU) und der Universität London haben untersucht, ob sich Menschen im Umgang mit Systemen der Künstlichen Intelligenz (KI) genauso kooperativ verhalten wie gegenüber ihren Mitmenschen.

- Von Künstlicher Intelligenz wird erwartet, dass sie Rücksicht auf den Menschen nimmt. Doch umgekehrt kann davon keine Rede sein.
- Online-Experimente belegen, dass Menschen Maschinen ausnutzen und dabei keine Schuldgefühle entwickeln.

Eine Thematik, die in Zukunft eine besondere Relevanz in unserem Alltag haben wird, wenn wir an das Autonome Fahren denken.

„Kooperation hält unsere Gemeinschaft zusammen. Sie erfordert Kompromiss- und Risikobereitschaft, da das Vertrauen, das wir anderen entgegenbringen, immer auch ausgenutzt werden kann", erklärt Jurgis Karpus, Ph.D., Mitarbeiter am Lehrstuhl für Philosophy of Mind der LMU. „Der Autoverkehr ist dafür ein gutes Beispiel: Wir verlieren etwas Zeit, wenn wir jemandem Vorfahrt gewähren, und sind verärgert, wenn andere es uns nicht gleichtun."

Im Rahmen der Studie wurden in Online-Experimenten verschiedene Situationen mit Methoden der verhaltensorientierten Spieltheorie modelliert, in denen Mensch und Maschine zusammentreffen.

„Unsere Studie zeigt, dass Menschen Maschinen zunächst dasselbe Vertrauen entgegenbringen wie ihren Mitmenschen: Die meisten gehen davon aus, auf Kooperationsbereitschaft zu treffen", sagt Karpus. Doch dann beginnen die Unterschiede: „Menschen sind sehr viel weniger bereit, sich einer KI gegenüber reziprok zu verhalten als gegenüber einem Menschen. Sie beuten sogar die ‚Gutmütigkeit' der Maschine zum eigenen Vorteil aus. Im Autoverkehr würde ein Mensch einem menschlichen Fahrer die Vorfahrt gewähren, nicht jedoch einem selbst fahrenden Auto."

Im Laufe der Experimente erwies sich dieses Muster als so konsistent, dass in der Studie die Rede von einer „Ausbeutung von Algorithmen" ist. „Dieser Widerwillen zur Kooperation mit Maschinen ist eine Herausforderung für die zukünftige Interaktion zwischen Mensch und KI", sagt Jurgis Karpus.

Kontakt:

Lehrstuhl für Philosophy of Mind, Ludwig-Maximilians-Universität München: *https://ots.de/rdnZES*

Der neue MIFARE® DESFire® EV3 Chip von NXP

Im Juni 2020 präsentierte NXP erstmals die dritte Generation des MIFARE® DESFire® Chips. Mit dem EV3 setzt NXP neue Maßstäbe in Sachen Sicherheit, Konnektivität und Nutzerkomfort. Im Vergleich zu seinen Vorgängern bietet das neue Mitglied der MIFARE-Familie eine höhere Leistung mit größerer Lesereichweite und verbesserter Transaktionsgeschwindigkeit. Doch die wohl größten Neurungen des DESFire EV3 finden sich in den Sicherheitsfeatures:

Transaction Timer

Der neue Transaktions-Timer ermöglicht es, eine maximale Dauer pro Transaktion für jede Applikation vorzugeben. Läuft der Timer aus, bevor eine Transaktion abgeschlossen ist, werden die Änderungen zurückgesetzt und die aktuelle Transaktion abgebrochen. Diese Funktion dient der Abwehr sogenannter Man-in-Middle-Angriffe, bei der ein Angreifer Daten auf dem Kommunikationsweg zwischen Lesegerät und Transponder unbemerkt abfängt und modifiziert weiterleitet. Mit dieser Methode kann ein Hacker auch eine Transaktion bewusst verzögern und die Karte im aktiven Status halten, auch wenn Sie bereits vom Lesegerät entfernt wurde. So verschafft er sich beispielsweise Zugang zu einem öffentlichen Verkehrsmittel, obwohl das Ticket bereits abgelaufen ist.

Secure Unique NFC (SUN)

Auch Secure Unique NFC Message (SUN) gehört zu den neuen Sicherheitsfunktionen des EV3. Bereits bekannt vom NTAG® 413 DNA Chip, wird bei jedem Tap, also jedem Auslesen einer NFC-Information, ein eindeutiger Code und eine kryptosichere URL generiert, die an die NDEF-Nachricht (die NFC Information) angehangen wird. Der Code kann zur verifizierung direkt über den URL an einen Backendserver übertragen werden. Ist er einzigartig und authentisch sind Vertraulichkeit und Integrität der Daten gegeben. Dieses Verfahren ist bisher die sicherste Kommunikationsform zwischen einem NFC-Tag und Endgerät.

MIFARE 2GO

Der MIFARE DESFire EV3 ist kompatibel mit dem neuen Cloud-basierten Service MIFARE 2GO von NXP. Dieser verwaltet digitale Berechtigungen und macht Sie für sämtliche NFC-fähige Geräte wie Smartcards, Smartphones, Tags und Wearables zugänglich und nutzbar. Mit der passenden Infrastruktur können Nutzer mit MIFARE 2GO neue Funktionen selbstsändig auf Ihre Karte, das Smartphone oder die Watch laden.

Natürlich ist der EV3 vollständig abwärts kompatibel und bringt alle Funktionen der vorherigen Generationen mit. Wie bereits beim EV2 ist die Sicherheit von Hard- und Software des neuen DESFire nach Common Criteria EAL 5+ zertifiziert. Es steht eine breite Auswahl an offenen Kryptoalgorithmen auf Basis des "Data Encryption Standard" (DES) 2K3DES, 3K3DES oder des Advanced Encryption Standard (AES) zur Verfügung. Ein kartengenerierter MAC hilft zusätzlich bei der sicheren Authentifizierung von Transaktionen. Für die Abwehr von Delay-Angriffen ist auch der bekannte Proximity-Check mit dem MIFARE DESFire EV3 möglich.

Zusammenfassung der wichtigsten Features

- Transaction-Timer zur Abwehr von Man-in-the-Middle-Angriffen
- SUN (Secure Unique NFC) Nachrichtenauthentifizierung für erweiterten Datenschutz
- Flexible Dateistruktur ermöglicht so viele Anwendungen wie die Speichergröße unterstützt
- NFC-Forum-Tag-Typ-4-konform
- Kartengenerierter MAC zur Authentifizierung von Transaktionen
- Proximity Check zur Abwehr von Delay-Angriffen

Typische Anwendungen

- SmartCity
- ÖPNV – Öffentliche Verkehrsmittel
- Zutrittsmanagement
- Mikropayment (in geschlossenen Kreisläufen)
- Campuskarten, Studentenausweise und Schülerausweise
- Kundenkartensysteme