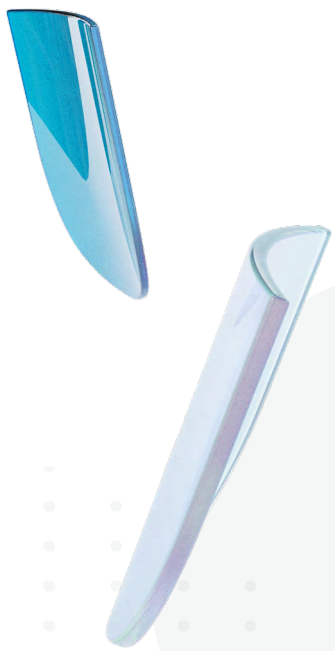
TELEKOM SECURITY

Du bist einzigartig! Sicher?

Keine Digitalisierung
ohne Identity Security

Connecting your world.

Inhaltsverzeichnis



Nichts geht mehr ohne sichere digitale Identitäten

Stellen Sie sich vor, Ihre Unternehmenswebsite wird gehackt und Kriminelle könnten nach Lust und Laune Falschmeldungen verbreiten. Oder Ihr E-Mailkonto würde gekapert und in Ihrem guten Namen fragwürdige Geschäfte getätigt. Stellen Sie sich vor, jemand würde sich in die Verwaltung einer Klinik oder in das Logistiksystem einer Tankstellenkette hacken. Ihr privates Online-Banking übernehmen. Oder die Steuerung einer Anlage zur Wasser- oder Stromversorgung lahmlegen. Das alles ist bereits heute kein schlechter Traum, sondern Realität.

Die Gefahren des Identitätsdiebstahls betreffen alle: Privatpersonen und Unternehmen ebenso wie öffentliche Einrichtungen und Infrastrukturen. Stillstand, Datenklau, Spionage, Erpressung, Reputationsverlust, Sabotage und finanzielle Schäden in unermesslicher Höhe können die Folgen sein, wenn digitale Identitäten in die falschen Hände geraten.

Um dies zu verhindern, müssen digitale Identitäten geschützt werden – durch moderne Sicherheitstechnologien, strenge Sicherheitsprotokolle und die Sensibilisierung von Mitarbeitenden.

Dieses Whitepaper beleuchtet die wachsende Bedeutung von Identity Security im Kontext von Identitätsdiebstahl und Datenmissbrauch, gesetzlichen Rahmenbedingungen und modernen Sicherheitsmodellen wie SASE und Zero Trust. Außerdem werden verschiedene Sicherheitsbausteine für Identity Security skizziert, mit denen Sie die immer zahlreicher werdenden potenziellen Angriffsflächen erfolgreich vor Cyber-Bedrohungen schützen können.

Bist Du es wirklich?

Der Begriff „Digitale Identität" bezieht sich auf die Daten, die Computersysteme verwenden, um Personen, Organisationen, Software-Anwendungen oder Geräte zu identifizieren. Diese Daten können sehr unterschiedlich sein – in Bezug auf Menschen können es etwa Namen, Aliasnamen, Passwörter, Suchhistorien, Kaufpräferenzen, biometrische Daten, Nationalitäten oder Geburtsdaten sein. Auch Standorte oder genutzte Endgeräte können dazu zählen.

Wir alle bewegen uns heute ganz selbstverständlich in der virtuellen Welt des Internets. Dabei nehmen wir für verschiedene Zwecke unterschiedliche Identitäten an: In Chatrooms agieren wir anonym, beim Online-Shopping kaufen wir mit unserem Namen ein, in einigen Social-Media-Kanälen entscheiden wir uns für ein Pseudonym und im Büro weist uns der Arbeitgeber einen Nutzernamen zu.

Digitale Identitäten sind eine notwendige Voraussetzung, damit im Internetzeitalter Interaktionen zwischen verschiedenen Parteien stattfinden können.

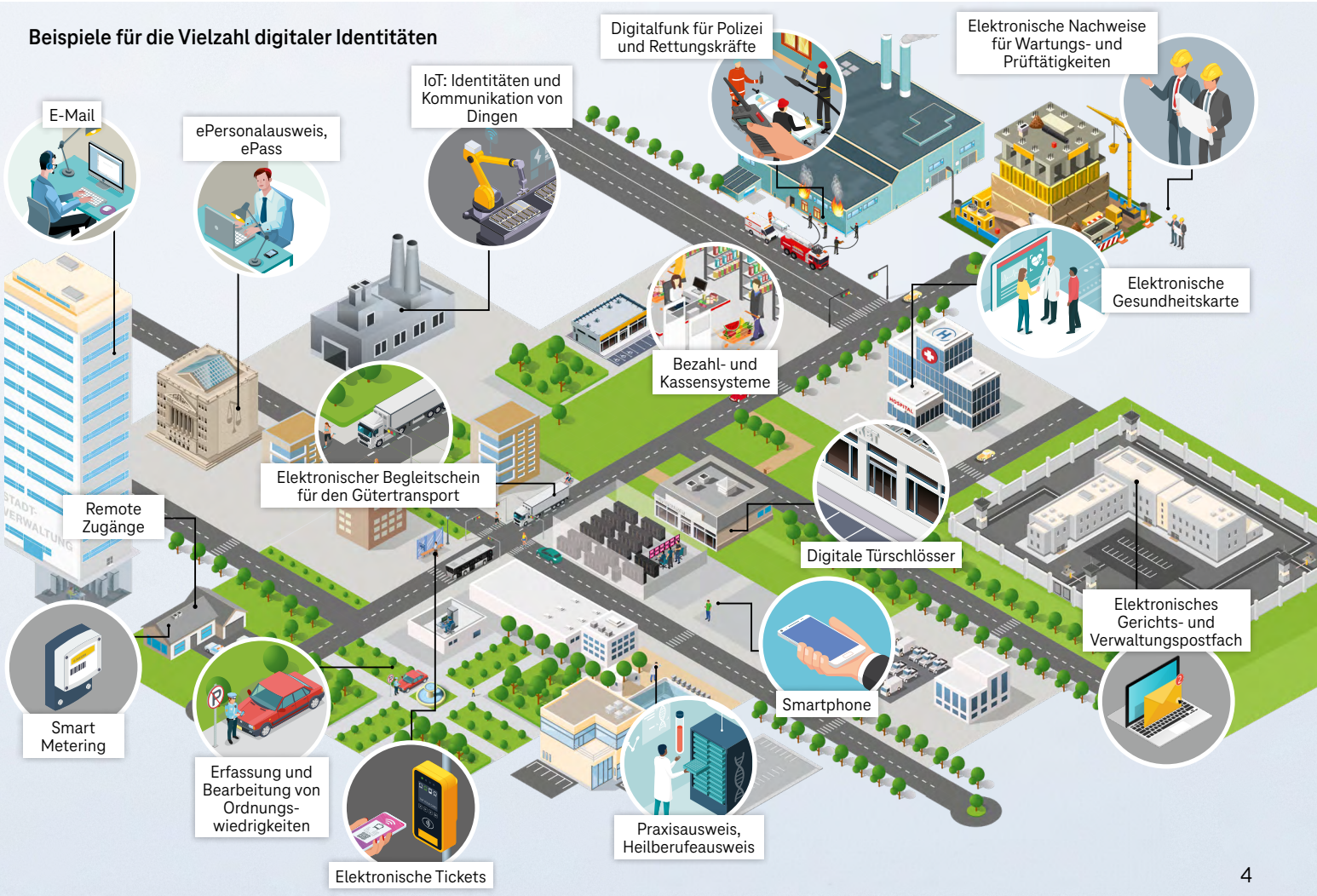
Ein Blick auf das Wimmelbild unten verdeutlicht: In allen Bereichen des täglichen Lebens finden digitale Interaktionen statt, für die digitale Identitäten eine Rolle spielen. Wir weisen uns elektronisch mit unserem (neuen) Personalausweis aus, nutzen E-Mail und Smartphone und bezahlen mit Hilfe elektronischer Bezahlsysteme. Wir öffnen das Büro mit Chipkarte oder greifen vom Homeoffice aus auf IT-Anwendungen der Firma zu. Und wenn wir vergessen, ein (digitales) Parkticket zu kaufen, wird die Ordnungswidrigkeit inzwischen ganz selbstverständlich digital erfasst. Die Szenarien lassen sich nahezu beliebig erweitern und werden mit beschleunigter Digitalisierung immer zahlreicher. Nicht nur Menschen agieren mit digitalen Identitäten, auch Sensoren oder Maschinen, die via Internet der Dinge vernetzt sind, haben eine digitale Identität.

Eine Kernfrage in all den Szenarien lautet:
Wer verbirgt sich tatsächlich hinter einer digitalen Identität?

- Ist es wirklich die Kollegin aus dem Homeoffice, die auf unseren Server zugreift?
- Stammt diese E-Mail tatsächlich von meiner Bank?
- Sind das die echten Verbrauchsdaten meines Stromzählers?

Der sichere Nachweis digitaler Identitäten ist für fast alle Lebensbereiche relevant. Ohne Datenschutz, Sicherheit und darauf gründendes Vertrauen geht es nicht.

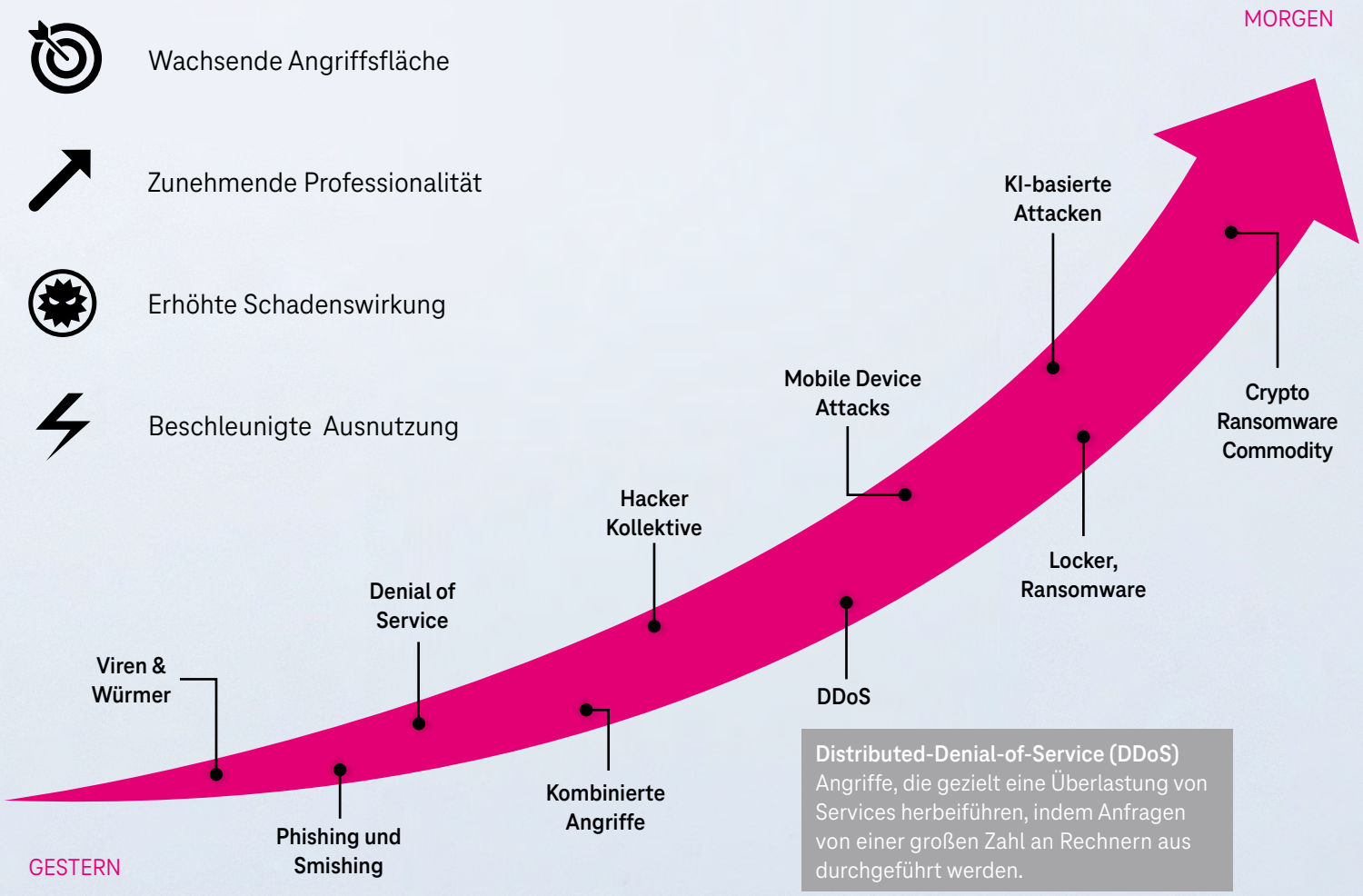
Beispiele für die Vielzahl digitaler Identitäten



Das Geschäft mit dem Identitätsdiebstahl

Immer mehr Cyberkriminelle entdecken für sich ein attraktives Geschäftsfeld: Den Identitätsdiebstahl. Sie greifen Daten ab, die zur digitalen Identität eines Menschen, einer Organisation, wichtiger Steuerungskomponenten von Industrieanlagen oder wichtigen Infrastruktureinrichtungen gehören. Nach Angaben des Bundeskriminalamts werden dabei meist zunächst Daten gesammelt und erst später ein Geschäftsmodell für den Missbrauch der Daten entwickelt[1]. Auch der Verkauf digitaler Identitäten über das Darknet ist eine übliche Praxis – verkauft werden z. B. Logins, elektronische Schlüssel zur Anmeldung an IT-Systemen oder personenbezogene Daten.

Angriffe werden professioneller, Schäden steigen



[1] BKA - Identitätsdiebstahl/Phishing

Wer wird angegriffen?

Leider werden alle Arten von Unternehmen und Organisationen von Cyberattacken bedroht, egal ob Mittelständler, börsennotierter Konzern oder Behörde. Besonders kritische Infrastrukturen werden zunehmend attackiert. Laut der auf IT-Security spezialisierten Onlineplattform CSO wurden im Jahr 2023 58 deutsche Unternehmen Opfer einer Cyberattacke, wobei von einer deutlich höheren Dunkelziffer auszugehen ist. Betriebsstörungen, Umsatzeinbußen, hohe Kosten für die Datenwiederherstellung sowie Reputationsschäden sind die Folge.[2]

LastPass-Hack: Ein besonders perfider Identitäts-Diebstahl war der Hack des Passwortmanagers LastPass, den das Unternehmen 2022 meldete. Wie sich herausstellte, haben sich die Kriminellen dabei auch Zugriff auf die Kennwort-Sammlungen der LastPass-Kunden verschafft[3].

Wer greift an?

Sogenannte **Skript Kiddies** sind in der Regel unerfahrene Individuen, die einfache, vorgefertigte Hacking-Tools verwenden, um in Netzwerke einzudringen oder Störungen zu verursachen. Ihre Motivation ist häufig Neugier oder der Wunsch nach Anerkennung in ihrer Peer-Gruppe. Die Zahl der Angriffe durch diesen Personenkreis hat in den vergangenen Jahren deutlich abgenommen.

Zugenommen hat hingegen die Zahl der Angriffe durch sogenannte **Hacktivisten.** Sie nutzen ihre Fähigkeiten, um Websites zu hacken, Daten zu leaken oder Dienste lahmzulegen. Dabei geht es ihnen nicht um Geld, sondern darum, politische oder soziale Missstände aufzudecken.

Stark zugenommen haben die Cyber-Angriffe **krimineller Akteure.** Darunter zählen zum einen Kriminelle, die aus finanziellem Interesse handeln. Zunehmend mischt hier auch die organisierte Kriminalität mit. Darüber hinaus werden staatliche Akteure, die (Industrie-) Spionage oder Desinformation betreiben oder Sabotage-Akte ausüben, zu dieser Gruppe gerechnet.

[2] Cyberangriffe in Deutschland 2023/2024
[3] LastPass-Hack: Angreifer hackten Privat-PC von DevOps-Entwickler | heise online

Wie wird angegriffen?

Analoger Diebstahl: Der einfachste Weg des Diebstahls digitaler Identität ist ein analoger Klassiker: Diebe stehlen Smartphones samt den gespeicherten Daten. Wer hier seine PINs und Passwörter unverschlüsselt abgelegt hat, wird dann schnell zum Opfer. Gleiches gilt für den Diebstahl anderer digitaler Endgeräte, Ausweise, Kreditkarten oder Post mit wichtigen Unterlagen. Selbst das Durchwühlen von Papiermüll – Dumpster Diving – ist eine gängige Praxis, um an fremde Identitätsdaten zu gelangen.

Social Engineering: Bei dieser Angriffsmethode konzentrieren Hacker sich nicht auf technische Tricks, sondern versuchen, über soziale Interaktionen an Informationen wie Zugangsdaten zu gelangen. Dabei geben Sie sich am Telefon beispielsweise als Techniker aus, und behaupten, Daten zu benötigen, um ein wichtiges Update abschließen zu können. Oft recherchieren die Angreifer zuvor ausgiebig, um ihre Opfer besser täuschen zu können.

Schadsoftware: Die am weitesten verbreitete Methode ist der Einsatz von Schadsoftware, mit der sich Daten beliebiger Art von Computern abgreifen lassen. Um Schadsoftware auf einem Fremdrechner zu platzieren, entwickeln Hacker ihre Methoden ständig weiter. So fälschen Betrüger seriöse Internetseiten und verstecken dort z. B. Viren oder Verweise auf schadhafte Seiten in Werbebannern. Auf diese Weise werden täglich tausende Webseiten infiziert.

Phishing: Ein weiterer Betrugstrick läuft über E-Mail. Absender der Mails scheinen seriöse Banken, bekannte Firmen oder ein Bekannter des Opfers zu sein. Über einen verseuchten Link werden die Empfänger aufgefordert, einen Anhang zu öffnen oder Daten auf einer Website zu aktualisieren. Tatsächlich führt der Link zu einer manipulierten Website, und die Kriminellen greifen die dort einzugebenden Daten, nicht selten Kreditkartennummern oder Passwörter(!), einfach ab, um sich die Identität des Opfers anzueignen. Auch per SMS werden verseuchte Links verschickt - dann spricht man von Smishing.

Schwachstellen ausnutzen: Hacker nutzen Schwachstellen von Softwareprodukten oder von Sicherheitssystemen aus, um Zugriff auf vertrauliche Dateien mit sensiblen Daten zu erhalten oder gar große Datenbanken zu kompromittieren.

Ein bedeutender Aspekt für den starken Anstieg von Identitätsdiebstahl ist, dass es mit Unterstützung von künstlicher Intelligenz sehr viel einfacher geworden ist, Schadsoftware zu programmieren. Der Kampf zwischen angreifenden und abwehrenden Kräften hat damit nochmals deutlich an Fahrt aufgenommen. Daher ist es wichtiger denn je, die potenzielle Angriffsfläche so gering wie möglich zu halten. Identity Security kann dazu einen entscheidenden Beitrag leisten.

Gesetzliche Anforderungen

Die gesetzgebenden Instanzen reagieren auf die zunehmende Bedeutung der Digitalisierung und versuchen über Verordnungen, Cybersicherheitsstandards durchzusetzen, die sichere digitale Interaktionen ermöglichen und Datenmissbrauch verhindern. Im Folgenden behandeln wir einige für das Thema Identity Security wichtige gesetzliche Regulierungen.

eIDAS: Standards für die "Elektronische Identifizierung"

Die eIDAS-Verordnung (Electronic IDentification, Authentication and Trust Services) enthält verbindliche europaweit geltende Regelungen in den Bereichen "Elektronische Identifizierung" und "Elektronische Vertrauensdienste". Die EU-Verordnung schafft einheitliche Rahmenbedingungen, die sich auf elektronische Identifizierung und Vertrauensdienste, elektronische Signaturen, qualifizierte digitale Zertifikate, elektronische Siegel, Zeitstempel und andere Nachweise für Authentifizierungsmechanismen beziehen. Ziel ist es, elektronische Transaktionen zu ermöglichen, die den gleichen rechtlichen Status haben wie Transaktionen, die auf Papier durchgeführt werden.

Die Absicht von eIDAS ist es außerdem, einen Dialog aller sicherheitsrelevanten Akteure (öffentliche Stellen und Unternehmen) über die besten Technologien und Sicherheits-Tools zu führen und Unternehmen durch Richtlinien dazu zu drängen, ein höheres Maß an Informationssicherheit und Innovation voranzutreiben.

Beispiel elektronische Signatur: Die Mitgliedstaaten sind verpflichtet, elektronische Signaturen anzuerkennen, welche den Standards der eIDAS-Verordnung entsprechen. eIDAS bietet hierzu unter anderem eine Liste vertrauenswürdiger Dienste, die für digitale Signaturen verwendet werden können. Die Verordnung bietet damit eine sichere Grundlage, um Online- Verträge und digitale Transaktionen grenzüberschreitend abzuwickeln.

KRITIS und NIS-2: Regelungen zum Schutz kritischer IT-Infrastrukturen

Ausgeklügelte Angriffe auf IT-Infrastrukturen stellen in einer Welt, in der nichts mehr ohne IT-Unterstützung funktioniert, ein ernstes Problem dar. Deshalb ist es erforderlich, entsprechende technische und organisatorische Selbstschutzmaßnahmen zu treffen, um in der Lage zu sein, auf Schwachstellen schnell zu reagieren.

KRITIS: Bei Cyberrisiken geht es um weit mehr als nur um Passwort- und Identitätsdiebstahl oder um einzelne Unternehmen und Institutionen. Cyberrisiken sind auch eine ernstzunehmende Sicherheitsbedrohung für die sogenannte kritische Infrastruktur.

Betreiber von kritischen Infrastrukturen (KRITIS) werden deshalb zur Einhaltung von Standards, welche branchenspezifisch definiert und umzusetzen sind, gesetzlich verpflichtet. Die bisherige KRITIS-Regulierung wurde neu geordnet und ab 2024 regelt das neue KRITIS-Dachgesetz (in Umsetzung der EU Richtlinie EU RCE/CER in Deutschland) zusätzliche Pflichten für Betreiber kritischer Anlagen, um die Resilienz und physische Sicherheit kritischer Infrastrukturen sicherzustellen.

NIS-2: Ergänzend zum KRITIS-Dachgesetzes etabliert die europäische Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2) ein robustes Cybersicherheitsniveau, um Sicherheitslücken und Hackerangriffen aktiv begegnen zu können.

Die Richtlinie betrifft insgesamt 18 Industriesektoren von Wasser bis Weltraum, für die umfassende Anforderungen an das Risikomanagement und die Cybersicherheit gelten, einschließlich der Meldung von Cybersicherheitsvorfällen an die zuständigen Behörden. Darüber hinaus wird die Betrachtung von Cyberrisiken auch in Lieferketten gefordert und ein proaktives Risikomanagement sowie aktuelle Sicherheitsstandards und Technologien in Bereichen wie Netzwerksicherheit und Krisenmanagement festgeschrieben.

Das NIS-2-Umsetzungsgesetz setzt hierzu die NIS-2-Direktive für Cybersecurity in deutsches Recht um, welche für die „Gestaltung der digitalen Zukunft Europas" einen weiteren wichtigen gesetzlichen Grundpfeiler darstellt, um Organisationen und kritische Infrastrukturen vor Cyberbedrohungen zu schützen. Der bisherige Geltungsbereich der KRITIS-Regulierung wird ausgedehnt und betrifft nun mindestens 30.000 Unternehmen in Deutschland in Branchen wie Energie, Wasser und Abwasser, Gesundheit, Transport und Verkehr, IT und TK, Finanzen und Versicherungen, Weltraum, Ernährung, Entsorgung, Post/Kurier, Chemie, Verarbeitendes Gewerbe, Digitale Dienste, Forschung sowie den Bund selbst.

Bisherige KRITIS-Normen in Deutschland sollen durch die genannten Vorschriften ab Oktober 2024 abgelöst werden.

> Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.
>
> – KRITIS-Definition des Bundesamtes für Sicherheit in der Informationstechnik

EU Cyber Resilience Act (CRA): Haftung für Cybersicherheit

Als Ergänzung zu NIS-2 wird voraussichtlich Mitte 2024 der Cyber Resilience Act (CRA) durch das EU-Parlament beschlossen und ist danach innerhalb von zwei Jahren durch die Mitgliedsstaaten umzusetzen. Der CRA gilt für alle Hard- und Softwareprodukte aus dem Consumer- und Industriebereich, die miteinander oder dem Internet verbunden werden können.

Hafteten Hersteller bisher ausschließlich für die physische Sicherheit ihrer Produkte, unterliegen dann alle in der EU produzierten oder in die EU importierten Geräte Regularien, bei denen Hersteller gewährleisten müssen, dass ihre Geräte keine bekannten (Cyber-) Sicherheitslücken aufweisen. Dies beginnt bereits während der Entwicklungsphase und umfasst sicherheitsrelevante Maßnahmen während des ganzen Lebenszyklus von Produkten. Hersteller sind außerdem dazu verpflichtet, den verantwortlichen Behörden sicherheitsrelevante Vorfälle und bekannt gewordene Sicherheitslücken aktiv zu melden.

Sanktionierungen und Folgen von Sicherheitslücken

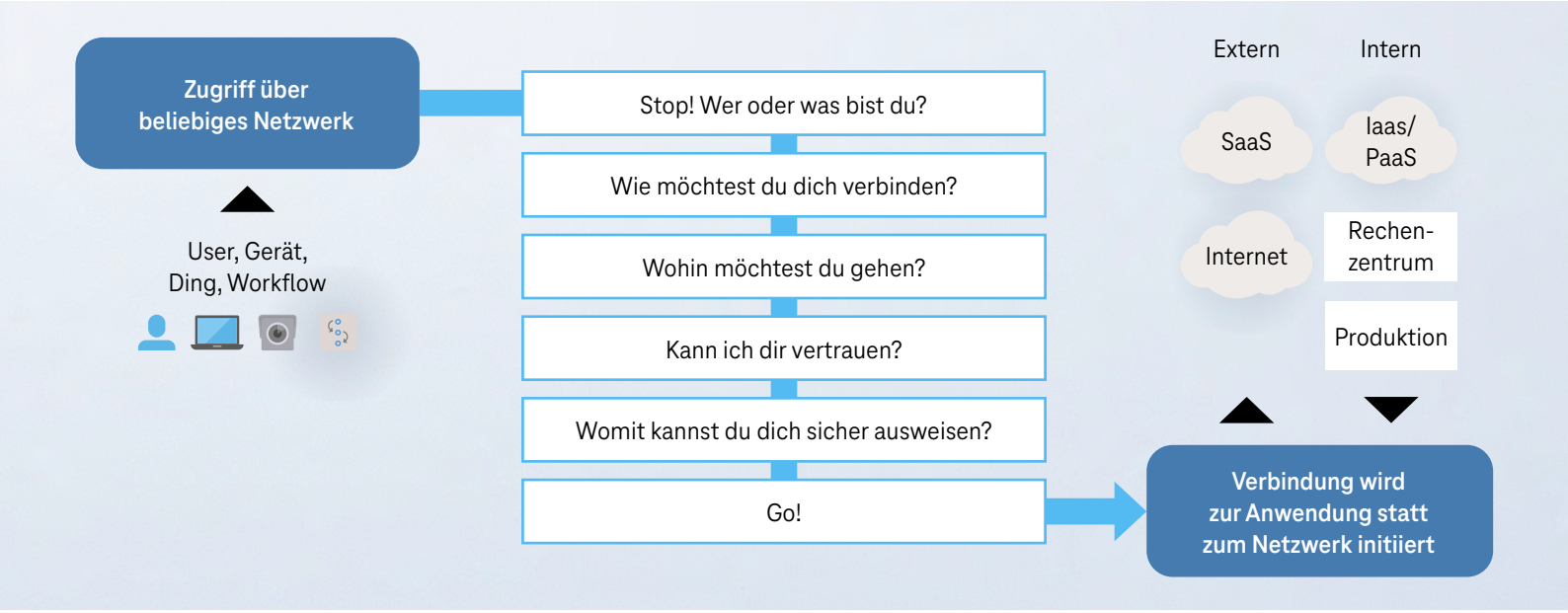
Unternehmen, die sich nicht an die Vorschriften des Cyber Resilience Act halten, drohen Bußgelder von bis zu 15 Millionen Euro oder 2,5 Prozent ihres Jahresumsatzes. Hinzu kommen mögliche Schäden in Bezug auf die CE-Sicherheitszertifizierung sowie mögliche Rückrufaktionen und deren Folgen, welche Unternehmen existenziell bedrohen können.

Moderne Sicherheitsmodelle

Ein weiterer Grund, weshalb Identity Security in den Fokus rückt: Bei Zero Trust (ZT) und Secure Access Service Edge (SASE) spielen starke digitale Identitäten eine zentrale Rolle. Durchgesetzt werden sie durch eine moderne und sichere Zugriffssteuerung.

Zero Trust

Zero Trust stellt das traditionelle, perimeterbasierte Sicherheitsmodell in Frage. Der perimeterbasierte Ansatz von früher schützte die Grenzen des Netzwerks und stufte alles, was innerhalb des Netzwerks passierte, als vertrauenswürdig ein. Bei Zero Trust hingegen wird davon ausgegangen, dass kein Benutzer oder Gerät von Natur aus vertrauenswürdig ist. Zugriffsanforderungen werden vielmehr auf der Grundlage mehrerer Identitäts-Faktoren wie Benutzer- und Computeridentität, Gerätezustand, Standort und Verhalten ausgewertet.



Zugriffskontrolle im Zero Trust Modell

Basierend auf den Prinzipien der kontinuierlichen Überprüfung und Steuerung von Zugriffen, der minimalen Rechtevergabe und der automatisierten Durchsetzung definierter Richtlinien schützt Zero Trust das Netzwerk sowohl vor externen als auch vor internen Gefahren durch fahrlässige oder böswillige Akteure. Die Implementierung granularer Zugriffskontrollen (Zero Trust Network Access) und die kontinuierliche Überwachung des Benutzerverhaltens ermöglichen es, Anomalien und potenzielle Bedrohungen frühzeitig zu erkennen.

Durch den Einsatz starker Authentifizierungsmechanismen und Verschlüsselungsprotokolle können Unternehmen darüber hinaus Zugriffsanfragen auch in nicht vertrauenswürdigen Umgebungen validieren und sichern. Das Zero-Trust-Modell bietet so einen widerstandsfähigen und sichereren Identifizierungs- und Validierungs-Rahmen mit unterschiedlichen Komponenten, die je nach Entwicklung der Bedrohungslandschaft anpasst werden können.

Zero-Trust-Sicherheitskomponenten: Authentifizierung und Autorisierung

Das Zero-Trust-Modell baut insbesondere auf starke Authentifizierung- und Autorisierungsmechanismen, um feiner abgestimmte Zugangskontrollen umsetzen zu können. Diese ermöglichen es Nutzern, auf bestimmte Anwendungen abhängig von ihrer Rolle nur mit bestimmten Berechtigungen zuzugreifen.

SASE

Secure Access Service Edge (SASE) ist ein mit Zero Trust korrespondierender weiterer Ansatz für mehr Sicherheit in Netzwerken und in der Cloud. Geprägt wurde das Akronym SASE im Jahr 2019 durch das globale Forschungs- und Beratungsunternehmen Gartner[4].

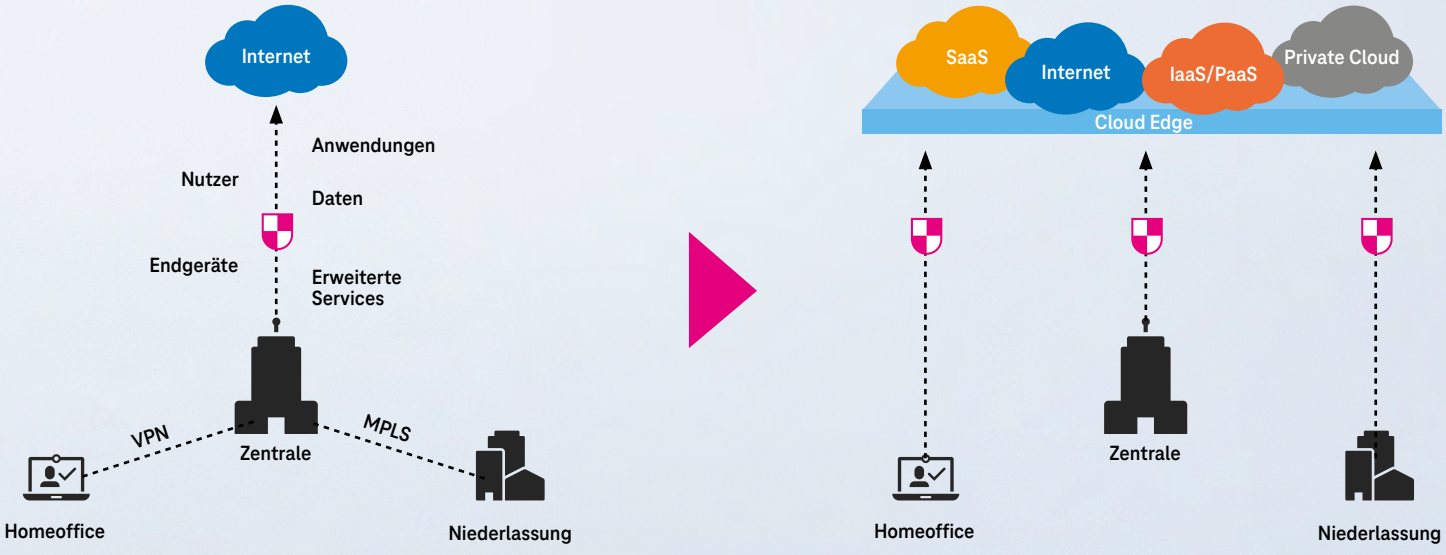
SASE zielt darauf ab, Nutzerinnen und Nutzer unabhängig von ihrem Standort einen sicheren und effizienten Zugriff auf Anwendungen und Daten zu ermöglichen, die über Clouds und Unternehmensdatenzentren verteilt sind. Damit reagiert es auf die neuen Sicherheitsanforderungen, die durch neuartige, dezentrale Unternehmensnetzwerke entstehen.

In sogenannten Software-Defined Networks (SDN) verbinden sich sämtliche Endgeräte direkt mit der Cloud (Local Internet Breakout). SASE schließt dabei eine Sicherheitslücke, die dadurch entsteht, dass eine Vielzahl verteilter Endpunkte wie z. B. Mitarbeiter aus dem Homeoffice und Zweigstellen sich direkt mit dem Internet verbinden.

Dabei kombiniert der Ansatz Funktionen wie SD-WAN (Software-Defined Wide Area Network) und verschiedene identitätsgesteuerte Netzwerksicherheitsdienste in einer einheitlichen, cloud-nativen Service-Plattform. Das erklärte Ziel von SASE ist, diese Technologien zu einem einheitlichen Framework zusammenzufügen. So entsteht ein auf der Cloud aufsetzendes sicheres Netzwerk, das auf die speziellen Bedürfnisse dieser komplexen Anwendungsumgebungen ausgerichtet ist.

Identitäts-gesteuerte Zugriffe

SASE-Services werden basierend auf der Identität der Nutzerinnen und Nutzer eingesetzt. Unabhängig von Ort oder Endgerät können Zugangs- und Sicherheitsberechtigungen so auf einzelne User zugeschnitten werden.



Von zentraler zu dezentraler Netzwerkarchitektur

[4] Gartner Research: Invest Implications: The Future of Network Security is in the cloud | gartner.com

Sicherheitsbausteine für Identity Security

Zero Trust und SASE sind in erster Linie keine Sicherheitsprodukte, sondern umfassende Ansätze, um Sicherheit auch in verteilten und über das Internet angebundenen Infrastrukturen zu gewährleisten. Verschiedene Dienste und Anwendungen werden benötigt, um diese Konzepte umzusetzen. Anbei ein Überblick über solche Sicherheitsbausteine, die im Kontext digitalen Identitäts-managements eine Rolle spielen.

Ein wichtiger Schwerpunkt von Sicherheitslösungen liegt in der Vereinfachung der sicheren Ausstellung, des Besitzes und der Nutzung digitaler Identitäten und einem effizienten Lebenszyklus-Management. Dies schließt ein Vorhandensein von nicht dokumentierten oder nicht genehmigten digitalen Identitäten mit schwachen Sicherheitsstandards aus.

Moderne Konzepte wie das IT-unterstützte Delegieren administrativer Aufgaben und die vollständige oder teilweise Automation von Prozessen für die Verwaltung digitaler Identitäten (z. B. über Sicherheitstoken, eWallets, Zertifikate und Schlüssel) befördern nicht nur deren Akzeptanz, sondern auch die Wirtschaftlichkeit entscheidend.

Public Key Infrastruktur (PKI)

Eine Public Key Infrastruktur ermöglicht den sicheren und vertraulichen Austausch von Daten über digitale Zertifikate und kryptographische Schlüssel. Public Key Infrastrukturen gewährleisten, Identitäten sicher festzustellen und die Kommunikation für digitalisierte Abläufe und Transaktionen der unterschiedlichsten Art gegen Manipulation, Abhören und Fälschung mittels Authentifizierung und Verschlüsselung zu schützen.

Unser Angebot:

Magenta Security Enterprise.ID
Mit Magenta Security Enterprise.ID erhalten Sie Ihre individuelle Public Key Infrastruktur mit hohem Automatisierungsgrad als Dienstleistung. Dabei werden ausschließlich Ihre eigenen Zertifizierungsstellen (Root CA und CA) genutzt. Die Lösung kann über Microsoft AutoEnrollment in Ihre Active-Directory-Landschaft eingebunden werden.

Magenta Security Business.ID
Mit Magenta Security Business.ID stellt die Telekom Ihnen eine Public Key Infrastructure (PKI) als Dienstleistung bereit. Dabei werden anerkannte, öffentliche Zertifizierungsstellen (Root CA, CA) der Telekom genutzt. Sie erhalten einen Mandanten und haben damit direkt nach der Beauftragung Zugriff auf die Lösung.

Magenta Security Qualified.ID
Magenta Security Qualified.ID ist ein Vertrauensdienst, der nach der europäischen eIDAS Verordnung akkreditiert ist, mit dem wir die besonderen Anforderungen des öffentlichen Sektors erfüllen. Die hierfür verfügbaren Signaturkarten ermöglichen es, elektronische Dokumente mit qualifizierten elektronischen Signaturen eIDAS-konform zu unterzeichnen.

Identitätsmanagement für IoT / Industrie 4.0

Für die Sicherung von Maschinenidentitäten bieten digitale Zertifikate aus einer Public Key Infrastruktur (PKI) in Verbindung mit Automatisierungsprotokollen wie ACME, EST, SCEP und CMP, einschlägigen Sicherheitsstandards wie HTTPS, TLS und SSH sowie Schnittstellen für Web-Anwendungen auf Grundlage des REST Standards effektive Sicherheit.

Unser Angebot: Magenta Security IoTm2m.ID

Der IoTm2m.ID PKI-Service ist eine der aktuellsten PKI-Service-Implementierungen im Telekom Trust Center. Der Service fokussiert die automatisierte Ausgabe von Maschinenzertifikaten für Computer, Server, VoIP-Systemen, Containerlandschaften für IT-Applikationen, Drucker und IoT/M2M-Devices und ermöglicht so eine sehr effiziente Zertifikatsverteilung an Endsysteme.

Key Management

Kryptographische Schlüssel dienen der Signatur und Verschlüsselung von Informationen. In Firmennetzwerken müssen kryptographische Schlüssel nicht in jedem Fall in Verbindung mit digitalen Zertifikaten eingesetzt werden. Ein besonders abgesichertes Schlüsselmanagement stellt sicher, dass der Schlüssel echt ist und geheim gehalten wird. Dieses kann eine große Anzahl von Schlüsseln generieren, aufbewahren, bereitstellen, austauschen und schützen.

Besonders in Cloud-Umgebungen sollten die für den Schutz der Daten benötigten kryptographischen Schlüssel aus Sicherheitsgründen getrennt von den schützenswerten Daten extern mit besonderen Sicherheitsvorkehrungen gespeichert werden. Hierfür bieten Cloud-Anbieter eine sogenannte Bring-Your-Own-Key-Option (BYOK) oder eine Doppelschlüssel-Verschlüsselung (DKE) an, die üblicherweise unter Verwendung separat betriebener Hardware-Sicherheits-Module zur sicheren Erzeugung, Aufbewahrung und Verwendung von Krypto-Schlüsseln zum Einsatz kommt.

Unser Angebot: Magenta Security Key Management.ID

Magenta Security Key Management.ID ist ein externes Key Management System (eKMS), das Ihre kryptographischen Schlüssel sicher und DSGVO-konform verwaltet. So können Sie die Vorteile der Cloud-Services ausschöpfen, ohne die Sicherheit Ihrer Daten zu gefährden.

Identity and Access Management (IAM)

Identity und Access Management (IAM) stellt sicher, dass nur autorisierte Zugriffe auf sensible Informationen und Ressourcen möglich sind. Eine rollenbasierte Zugriffssteuerung schränkt den Zugriff jedes Benutzers auf die Ressourcen ein, die für seine Rolle erforderlich sind.

Die Überwachung und Protokollierung von Zugriffsaktivitäten gewährleistet darüber hinaus die Erkennung nichtautorisierter Aktivitäten, stellt Nachweispflichten sicher und mindert potenzielle Sicherheitsrisiken im Zusammenhang mit privilegierten Konten.

Unser Angebot:

IAM Lösungen
Magenta Security Identity Governance, Identity Lifecycle, Joiner-Mover-Leaver Prozesse (Lebenszyklus von Rollen- oder Mitarbeiteridentitäten), Segregation of Duties (Aufteilung/Minimierung von Befugnissen), Zertifizierung, Zero-Trust-konforme Zugriffssteuerung

Magenta Security Identity Analytics
Geschäftsrollenkonzept, Geschäftsrollendesign, Geschäftsrollenanalyse

Magenta Security Secure Access
Single Sign-On, Adaptive Multi-Faktor-Authentifizierung, Cloud Access, Zero-Trust-konforme Zugriffssteuerung

IAM Consulting
Portfolio-Beratung, Portfolioneutrale Beratung

Hardwaresicherheit: Smart Cards und Secure Elements

Hardwaresicherheit beschreibt Sicherheitsmaßnahmen, bei denen ein physisches Gerät dazu dient, eine IT-Infrastruktur zu schützen – im Gegensatz zur Sicherheitssoftware. Gängige Beispiele sind Smartcards und Hardware-Sicherheits-Module (HSM), die kryptografische Schlüssel für wichtige Funktionen wie Verschlüsselung, Entschlüsselung und Authentifizierung für IT-Systeme und Anwendungen bereitstellen.

Eine weitere Option sind sogenannte Secure Elements. Das sind fälschungssichere Mikrocontroller, die in steckbarer Form (z. B. als SIM-Karte) oder direkt als Mikrochips auf Motherboards montiert, genutzt werden können. Die Idee dabei ist, ein kleines, separates Stück Hardware einzusetzen, das Geheimnisse und deren Verwendung bei kryptografischen Operationen schützt und so als Sicherheitsanker für Authentifizierungsmechanismen und Anwendungen auf mobilen Geräten dient.

Unser Angebot:

Magenta Security Smartcards
Hardwarebasierte Sicherheitsanker mit TCOS-Betriebssystem, das höchsten Anforderungen an Funktionalität und Sicherheit entspricht. Magenta Security Smartcards verfügen über hochwertige Mechanismen zum Schutz der Daten und einer sicheren Zwei-Faktor-Authentifizierung.

Secure Elements & Services
Wir bieten Ihnen All-in-one Services und Lösungen für z. B. eHealth, Maut, IoT, Industrie 4.0, Automotive und im Behördenumfeld. Dabei übernehmen wir alles von der Konzeption über die Spezifikation und Entwicklung bis hin zum Rollout und Lifecycle Management von Hardware-Sicherheitsprodukten.

Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung (MFA) ist eine wesentliche Komponente des Identitätsmanagements, die eine höhere Sicherheitsebene als herkömmliche Verfahren wie Benutzername und Passwort bietet. Indem Nutzerinnen und Nutzer sich mit mehreren Faktoren wie Kennwörtern, Smart Cards oder mobilen Token authentifizieren müssen, können Unternehmen den Identitätsschutz erheblich verbessern. Selbst wenn Passwörter durch Techniken wie Phishing kompromittiert werden, verhindert die Multi-Faktor-Authentifizierung einen unbefugten Zugriff, da nur ein Faktor kompromittiert wurde.

Zusätzliche Sicherheit kann durch adaptive MFA erreicht werden. Diese evaluiert die Authentifizierungsanforderungen auf Basis von Risikofaktoren und Kontextinformationen wie z. B. Tageszeit oder Netzwekadressen, und legt den erforderlichen Authentifizierungsgrad in Abhängigkeit vom erkannten Risiko dynamisch fest.

Unser Angebot: Magenta Security OneTimePass.ID

Magenta Security OneTimePass.ID bietet eine starke Zwei-Faktor-Authentifizierung auf Basis eines dynamischen Einmalpasswortsystems. Die Cloud-basierte Authentifizierungslösung wird im im Telekom Trust Center betrieben.

Zusammenfassung: Sicherheit beginnt mit Identität

Identity Security ist eine grundlegende Notwendigkeit für Unternehmen und Organisationen aller Größenordnungen. Denn durch fortschreitende Digitalisierung wachsen die Angriffsflächen für die Korrumption digitaler Identitäten. Gleichzeitig steigt die Zahl der Angriffsversuche. Hierauf müssen Verantwortliche reagieren. Zudem gilt es, neue regulatorische Vorgaben zu erfüllen. Moderne Sicherheitsmodelle können helfen, diesen Anforderungen zu begegnen und digitale Identitäten erfolgreich zu schützen.

Digitale Identitäten bilden die Grundlage für elektronische Interaktionen, denn mit diesen Daten identifizieren Computersysteme Personen, Organisationen, Softwareanwendungen oder Geräte. Die Vertrauenswürdigkeit digitaler Identitäten ist daher von entscheidender Bedeutung. Nur so können sichere Interaktionen im Internet-Zeitalter stattfinden – egal in welchem Lebensbereich.

Die Bedrohungslage ist ernst – immer mehr kriminelle Akteure versuchen, digitale Identitäten zu stehlen. Sie verkaufen die erbeuteten Daten oder erpressen Lösegeld. Andere, staatlich gelenkte Akteure betreiben (Industrie-) Spionage, Desinformation oder Sabotage. Die Angriffsmethoden sind vielfältig und reichen von analogem Diebstahl und der Informationsbeschaffung über soziale Interaktionen bis hin zu Phishing-Methoden und dem Einsatz von Schadsoftware. Auch KI wird zunehmend zur Hilfe genommen.

Mit Regelungen wie der eIDAS-Verordnung, KRITIS, dem NIS-2-Abkommen und dem EU Cyber Resilience Act versuchen die gesetzgebenden Instanzen, auf die Bedrohungen zu reagieren und Rahmenbedingungen durchzusetzen, die sichere digitale Interaktionen ermöglichen und Datenmissbrauch verhindern. Aber nicht nur Betreiber kritischer Infrastrukturen stehen vor der Herausforderung, die immer strenger werdenden Vorgaben zu erfüllen.

Viele der neuen Richtlinien gehen Hand in Hand mit modernen IT-Sicherheitsansätzen wie Zero Trust und SASE. Digitale Identitäten und Zugriffsregelungen spielen in diesen Sicherheitsmodellen eine zentrale Rolle und werden sehr rigoros konzipiert und umgesetzt – die Devise lautet, nichts und niemandem zu vertrauen.

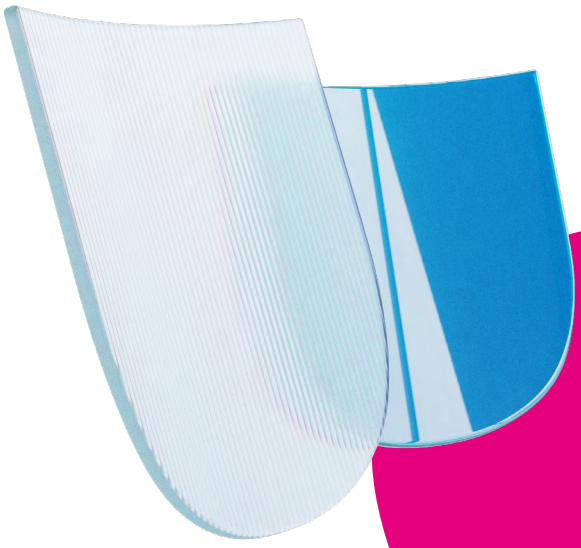
Zur Umsetzung dieser Ansätze sind verschiedene Dienste und Anwendungen notwendig. Diese reichen von Public Key Infrastrukturen über Key Management Systeme, Multifaktor-Authentifizierung, Identitäts- und Zugriffsmanagement bis zu Lösungen zur Hardware-Sicherheit.

Wir sorgen für sichere Identitäten!

Unternehmen stehen vor der Aufgabe, sich und ihre Kunden in einem digitalen Ökosystem zu schützen, das ständigen Veränderungen unterworfen ist. Dies erfordert nicht nur ein tiefes Verständnis der aktuellen Bedrohungslandschaft, sondern auch die Fähigkeit, proaktiv auf neue Herausforderungen zu reagieren. Angesichts der technischen Komplexität, der Notwendigkeit kontinuierlicher Anpassung und der sich wandelnden regulatorischen Anforderungen ist dies eine ernstzunehmende Herausforderung.

Die Telekom Security bietet als Managed Security Provider hochwirksame und professionelle Sicherheitsmaßnahmen für den Schutz vor Cyberangriffen. Mit über 25 Jahren Erfahrung ist die eigenständige Gesellschaft unter dem Dach der Deutschen Telekom AG Marktführer in DACH und einer der europäischen Leader in der Cyber Security Branche. Für das breite Portfolio – von Cyber Defense über Cloud Security bis zu OT Security – kooperiert die Telekom Security mit weltweit führenden Unternehmen und bietet so digitale Sicherheit aus einer Hand – von der Beratung über individuelles Design bis zur Implementierung.

Wir unterstützen Sie dabei, maßgeschneiderte Sicherheitslösungen für Ihr Business zu entwickeln und zu implementieren.



Deutsche Telekom Security GmbH | 04/2024

Kontakt
security.dialog@telekom.de
security.telekom.de

Herausgeber
Deutsche Telekom Security GmbH
Office Port 1
Friedrich-Ebert-Allee 71–77
53113 Bonn

Connecting your world.