Eine Themenbeilage der
Heise Medien GmbH & Co. KG

I
2017

SICHERHEIT & DATENSCHUTZ

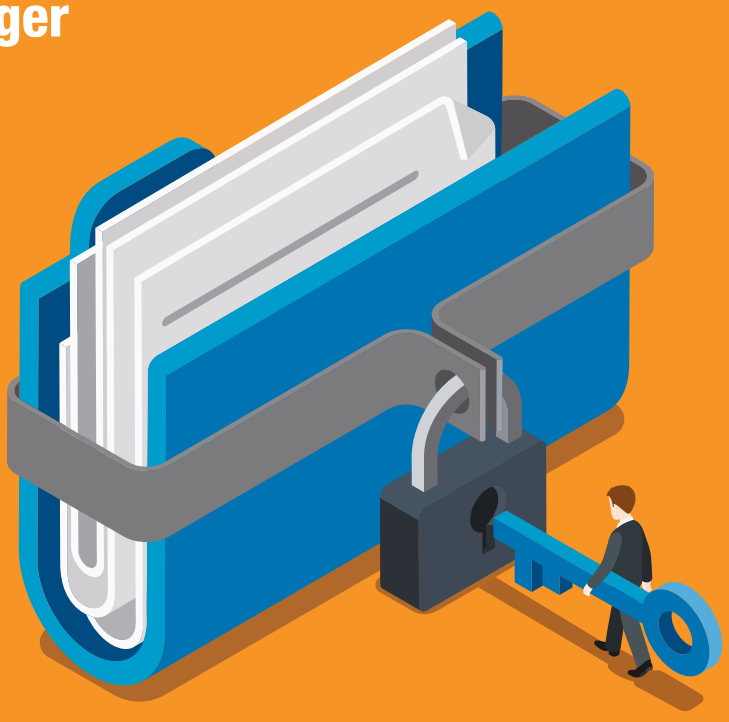
Blockchain, Kryptografie und Quantencomputer

Cybersecurity & Innovation:
Worauf Entscheidungsträger achten sollten

Identity Management:
Wie ein IAM in der Blockchain funktioniert

Post-Quantum-Kryptografie:
Was Alice und Bob im Quantenland suchen

Connected Cars:
Wer im Auto der Zukunft das Sagen hat



Gesundheitssektor:
Wann Patientendaten in der Cloud geschützt sind

Verschlüsselung:
Wie man mit PAKEs Passwörter sicher macht

www.it-security-und-management.de

powered by: TeleTrusT Pioneers in IT security. iX

WIR TRINKEN DEN KAFFEE #000000.

iX. WIR VERSTEHEN UNS.

Jetzt Mini-Abo testen:
3 Hefte + iX-Kaffeebecher nur 13,50 €
www.iX.de/test

Sie mögen Ihren Kaffee wie Ihr IT-Magazin: stark, gehaltvoll und schwarz auf weiß!
Die iX liefert Ihnen die Informationen, die Sie brauchen: fundiert, praxisnah und unabhängig.
Testen Sie 3 Ausgaben iX im Mini-Abo + iX-Kaffeebecher für 13,50 Euro und erfahren Sie, wie es ist, der Entwicklung einen Schritt voraus zu sein.
Bestellen Sie online oder telefonisch unter +49 (0)541 800 09 120.

Wer die Wahl hat …

Liebe Leserinnen und Leser,

werden wir noch in diesem Jahr erleben, wie die Blockchain ihren großen Siegeszug antritt? Sind verschlüsselte Daten und Kommunikation noch sicher, wenn Quantencomputer Realität werden? Wie bewältigen Entscheidungsträger den Spagat zwischen notwendigen Investitionen in Cybersecurity und der Umsetzung innovativer Geschäftsmodelle? Und wie steht es mit der Politik – wird die IT-Sicherheit ein prägendes Wahlkampfthema sein?

Im laufenden Jahr 2017 werden uns diese und viele andere Themen mit Bezug zur IT-Sicherheit beschäftigen. Ein besonderes Augenmerk verbleibt auf rechtlichen Fragen, wie etwa dem „Stand der Technik", wenn es um das IT-Sicherheitsgesetz geht. Hier gilt es, die Fortentwicklung der europäischen und deutschen Rechtsetzung zu beobachten.

Die jüngste Vergangenheit hat eindrucksvoll gezeigt, dass Bedrohungen der IT-Sicherheit äußerst real sind. Hackerangriffe auf Krankenhäuser, kritische Infrastrukturen, politische Parteien, Unternehmen und Institutionen sind allemal zur Regel geworden. Die Organisationsentwicklung und die Anpassung der Prozesse hält damit vielerorts nicht Schritt. Auch wiegen sich Verantwortliche immer noch in falscher Sicherheit. Kriminelle Strukturen haben sich professionalisiert und Schattenmärkte entwickelt, die für jedermann eine Gefahr darstellen können. Durch den Einzug von vernetzten Geräten in Produktion, Haushalt oder Fahrzeug ist die Digitalisierung in viele alltägliche Lebensbereiche vorgedrungen. Doch die IT-Sicherheit im Sinne von „Security by Design" wird leider vielerorts immer noch nicht ausreichend berücksichtigt. Und auch der Datenschutz bleibt weiterhin ein kontroverses Thema.

Die vorliegende Beilage „Sicherheit & Datenschutz" vermittelt Einblicke in ausgewählte Themen, die uns als Bundesverband IT-Sicherheit derzeit beschäftigen. Die Beiträge zielen dabei auf grundsätzliche Fragen ab, mit denen Sie sich als IT-Verantwortliche befassen sollten: Neben Praxisartikeln zu IT-Recht und Cybersecurity (S. 4), Identitätsmanagement in der Blockchain (S. 6) sowie eHealth & Cloudsecurity (S. 10) wird auch das Thema Automotive (S. 16) eingehender beleuchtet. Darüber hinaus widmen sich zwei technische Beiträge aktuellen Entwicklungen in der Quantentechnologie (S. 14) und bei der kryptografischen Schlüsselaushandlung (S. 12).

Als Bundesverband IT-Sicherheit wünschen wir uns entsprechende Schwerpunktsetzungen der Parteien im laufenden Wahljahr und werden weiterhin Wirtschaft, Verwaltung, Politik und Gesellschaft mit der Kompetenz eines nun fast 300 Mitglieder starken, aus Unternehmen und Organisationen bestehenden Expertennetzwerkes mit Rat und Tat zur Seite stehen, um die bestmöglichen Technologien voranzubringen. Die Herausforderungen nehmen zu. Aber die mittelständisch geprägte deutsche IT-Sicherheitsbranche ist sehr gut aufgestellt und durch innovative Produkte, gepaart mit der starken deutschen Datenschutzgesetzgebung, international wettbewerbsfähig. „IT Security made in Germany" wird auch über das Jahr 2017 hinaus eine gute Wahl bleiben.

Dr. Holger Mühlbauer
TeleTrusT – Bundesverband IT-Sicherheit e.V.
(Geschäftsführer)

Inhalt

Das Dilemma der Entscheider

Wie lassen sich IT-Sicherheit und Innovationen unter einen Hut bringen?

Digitaler Fortschritt bei gleichzeitiger Erhöhung der Cybersecurity-Anforderungen – viele Entscheidungsträger geraten hier immer häufiger in die Zwickmühle. Doch auch neue gesetzliche Vorgaben bieten noch genügend Spielraum, um Sicherheit und neue Geschäftsmodelle zu vereinbaren.

Digitalisierung und Cybersecurity – selten waren zwei Themen so eng miteinander verbunden und boten zugleich so viel Konfliktpotenzial. Zum einen öffnet die Digitalisierung den Unternehmen die Chance, innovative Geschäftsmodelle und -produkte zu entwickeln. Geschäftsführer und Vorstände sind deshalb gehalten, zum Wohle des Unternehmens zukünftige Trends möglichst vor der Konkurrenz zu erkennen und umzusetzen. Gleichzeitig werden die Unternehmen vermehrt rechtlich dazu verpflichtet, wirksame Cybersecurity zu implementieren. Auch diese Pflicht obliegt den Firmenchefs, die sich deshalb zunehmend verunsichert fühlen und mitunter auf zukunftsträchtige Projekte verzichten.

Kein neues Thema

Obwohl Digitalisierung und Cybersecurity relativ neue Begriffe sind, lässt sich die Verpflichtung zu Maßnahmen für die IT-Sicherheit aus altbekannten gesetzlichen Regelungen herleiten. Der Leitbegriff des „Risikomanagements“ (§§ 91 Abs. 2, 111 AktG, § 43 Abs. 1 GmbHG, Gesetz zur Kontrolle und Transparenz im Unternehmensbereich „KonTraG“) verlangt die Einführung wirksamer Frühwarnsysteme, die Risiken im Vorfeld lokalisieren und einen Schadenseintritt verhindern.

Risikomanagement umfasst heute auch umfängliche Maßnahmen, die ein Eindringen in digitale Infrastrukturen des Unternehmens abwehren. Die bloße Ermittlung des Ist-Zustandes reicht nicht aus. Vielmehr ist es zwingend erforderlich, Sicherheitslücken zu schließen, getroffene Security-Maßnahmen stetig fortzuentwickeln und deren Einhaltung zu überwachen. Was mit der Einführung von Videokameras und Eingangskontrollen begann, hat sich längst schon zu professioneller Hackerabwehr entwickelt. Notfallpläne, Mitarbeiterschulungen und Eskalationsmechanismen sind ebenso Teil einer zeitgemäßen Cybersecurity-Strategie.

Hohe Sicherheitshürden

Laut der Studie „Security Bilanz Deutschland 2016“ steigt dennoch der Gefährdungsindex weiter an, während der Sicherheitsindex kontinuierlich sinkt. Als Reaktion auf die steigende Bedrohung durch Cyberkriminalität versucht der Gesetzgeber durch diverse Gesetzesinitiativen wie dem IT-Sicherheitsgesetz, etablierte Standards wie die internationale Norm ISO 27001 oder den deutschen BSI-IT-Grundschutz für bestimmte Branchen verbindlich zu machen und regelmäßige Kontrollen einzuführen. Eine weitere Verschärfung sieht die EU-Datenschutzgrundverordnung vor, die alle Unternehmen zur Implementierung von Cybersecurity-Maßnahmen zum Schutz personenbezogener Daten verpflichtet. Anderenfalls drohen Bußgelder bis zu zehn Millionen Euro oder 2 % des gesamten weltweit erzielten Jahresumsatzes einer Unternehmensgruppe.

Bei einer Veracode-Umfrage im Jahr 2017 gaben immerhin 40 % der Unternehmen in Deutschland an, schon bei der Entwicklung der Software auf Sicherheitstests zu setzen. Zudem betonten 38,6 % der Softwareentwickler, dass die Absicherung vor Cyberangriffen und Datenschutzverletzungen oberste Priorität genieße. Dennoch – Cybersecurity-Maßnahmen fordern erhebliche personelle und finanzielle Ressourcen. Es verwundert deshalb nicht, dass etwa 90 % aller IT-Sicherheitsbeauftragten (CISOs) nach einer 2016 durchgeführten Studie des britischen Consulting-Unternehmens Cebr davon überzeugt waren, dass ihre aktuellen Bemühungen um mehr Sicherheit Innovationen eher behindern.

Haftung der Chefetage

Nicht ausreichende Cybersecurity in alltäglichen Bereichen hat neben den schädlichen Auswirkungen für das Unternehmen vor allem auch Folgen für den Entscheidungsträger selbst. Denn das Unternehmen kann im Innenverhältnis Schadensersatz vom ihm verlangen (§ 93 Abs. 2 Satz 1 AktG, § 43 Abs. 2 GmbHG), wenn er es versäumt hat, erforderliche Sicherheitsmaßnahmen einzurichten und Prozesse zu schaffen, die sowohl eine Weiterentwicklung als auch eine Überwachung der Einhaltung ermöglichen. Dieser Sachverhalt wirkt umso schwerer, da Entscheidungsträger sogar durch den Abschluss einer D&O-Versicherung (Directors-and-Officers-Haftpflichtversicherung) die persönliche Haftung mit ihrem Privatvermögen nicht gänzlich ausschließen können (z. B. § 92 Abs. 2 Satz 3 AktG). Und neben dem Vorstand oder der Geschäftsführung ziehen laut der Cebr-Studie auch immer mehr deutsche Unternehmen – insgesamt 43 % – den CISO für eine wesentliche Verletzung der Cybersecurity zur Rechenschaft.

Um einen etwaigen Regressanspruch abwehren zu können, ist den Entscheidungsträgern eine hinreichende Dokumentation der getroffenen IT-Sicherheitsmaßnahmen anzuraten. So ist beispielsweise ein den Vorstand entlastender Hauptversammlungsbeschluss im Falle einer unzureichend dokumentierten Cybersecurity anfechtbar. Ferner drohen im Fall lückenhafter Nachweise ab 25. Mai 2018 auch durch die EU-Datenschutzgrundverordnung Bußgelder in Millionenhöhe.

Fazit

Entscheidungsträger sind im Rahmen des Risikomanagements verpflichtet, ihre IT-Systeme zu sichern und sich nicht nur vor Cyberattacken, sondern vor allem auch vor Cyberspionage zu schützen. Dies soll jedoch nicht dazu führen, dass Unternehmen förmlich erstarren. Vielmehr ist ein gesunder Umgang mit den Anforderungen der digitalen Welt gefordert. Das gilt sowohl bei der Digitalisierung der Geschäftsmodelle als auch bei der Etablierung von IT-Sicherheitsstandards. Dafür bieten die gesetzlichen Regelungen noch ausreichend Möglichkeiten.

Mareike Gehrmann
Rechtsanwältin, Taylor Wessing Partnerschaftsgesellschaft mbB

SCHON BALD VERNETZT – ENDSPURT FÜR DEN AUFBAU DER TELEMATIK-INFRASTRUKTUR

Der Rollout der Telematikinfrastruktur im deutschen Gesundheitswesen gilt als eines der größten IT-Projekte weltweit. Rund 167.000 Ärzte und Psychotherapeuten, ca. 2.000 Kliniken und 124 gesetzliche Krankenversicherungen (KVs) werden in den nächsten Jahren über digitale Netze und Anwendungen miteinander verknüpft. Ziel ist eine reibungslose Kommunikation und ein sicherer Datenaustausch zwischen allen Akteuren des deutschen Gesundheitswesens. Im Zuge des in der zweiten Jahreshälfte 2017 beginnenden Rollouts werden in den nächsten Jahren eine Vielzahl von Fachanwendungen für Wirtschaftlichkeit, Transparenz und Aktualität in allen Bereichen des Gesundheitswesens sorgen.

Bereit für die Installation vor Ort

Telekom Healthcare Solutions (THS) ist im Begriff, die letzten Entwicklungen umzusetzen und alle Zulassungen für den Rollout zu erhalten. Sobald die letzten Spezifikationen für alle notwendigen Komponenten und Dienste feststehen, kann in den nächsten Monaten der Aufbau von Test- und Referenzumgebungen für das Zusammenspiel der Systeme abgeschlossen werden. In enger Kooperation mit etablierten Praxis- und Kliniksoftwareherstellern erfolgt dann die Implementierung der IT-Setups vor Ort: Dazu gehört die Installation der Hardware und die Anbindung an die Praxissoftware ebenso wie die Einrichtung eines VPN-Zugangsdiensts und einer hochsicheren Internetverbindung. Zur Hardware zählen ein Konnektor und Kartenterminals der neuesten Generation. Sie dienen dem Auslesen der Institutionskarten (SMC-B), der elektronischen Heilberufsausweise (eHBA) und der elektronischen Gesundheitskarten (eGK). Die Installation erfolgt durch geschultes Personal und die anschließende Betreuung durch spezialisierte Supportteams.

Wir setzen auf starke Partner

Für eine erfolgreiche Umsetzung in den Arztpraxen und Kliniken suchen wir den Schulterschluss mit den Dienstleistern vor Ort. Die zukünftige Telematikinfrastruktur ist ein hochkomplexes System, das sowohl auf dem Know-how eines industriellen Kommunikationsdienstleisters als auch auf der Branchenerfahrung der Praxis- und Kliniksoftwarehersteller basiert.

Versichertenstammdaten online aktualisieren

Das Versichertenstammdatenmanagement (VSDM) ist die erste Fachanwendung im Rahmen der Einführung der Telematikinfrastruktur. Es ermöglicht den Praxen, die Versichertendaten nicht nur binnen Sekunden auszulesen, sondern indirekt über den Konnektor auch eine Onlineaktualisierung der Daten vorzunehmen. Das Praxispersonal steckt dazu die eGK in das nach SICCT-Standard LAN-fähige Kartenterminal, das an den Konnektor angeschlossen ist. Die verschlüsselte Kommunikation und Übertragung der Daten von der zentralen Telematikinfrastruktur der Betreiber (Krankenversicherungen) zur dezentralen Telematikinfrastruktur (Arztpraxen und Kliniken) erfolgt über den VSDM-Fachdienst der Betreiber, über den hochsicheren VPN-Zugangsdienst, den VSDM-Intermediär und den Konnektor. Im Mittelpunkt aller Praxisanwendungsszenarien steht also immer der Konnektor.

Nur wenige Zugangsvoraussetzungen

Für die Implementierung des Telematikinfrastruktur-Pakets müssen die SMC-B und der eHBA in der Praxis vorliegen. Nur mit ihnen kann sich eine Praxis als zugangsberechtigt verifizieren. Die SMC-B, auch Praxisausweis genannt, ist über die jeweilige Standesorganisation (Kassenärztliche Vereinigung, Kassenzahnärztliche Vereinigung etc.) erhältlich. Einmal installiert, lässt sich das System mithilfe optionaler Komponenten und Leistungen an alle Veränderungen der Praxisstruktur anpassen.

Digital, sicher, nachhaltig

Die Telematikinfrastruktur bringt das deutsche Gesundheitswesen viele Schritte nach vorne: Schon die automatisierte Datenaktualisierung reduziert den Verwaltungsaufwand beim Abrechnen der Leistungen. Es folgen Anwendungen wie die qualifizierte elektronische Signatur und der E-Arztbrief, die auch die Kommunikation von Ärzten untereinander erleichtern.

Für all das weben wir jetzt ein hochsicheres Netz: Mit uns und unseren Partnern sind sowohl Ärzte als auch Kliniken bei der Einführung der Telematikinfrastruktur gut beraten. Dafür spricht unsere jahrzehntelange Erfahrung in der Vernetzung komplexer Systeme und Anwendungen, sei es im privatwirtschaftlichen oder im öffentlichen Raum – und natürlich im Gesundheitswesen.

www.telekom-healthcare.com

T · ·

HEALTHCARE SOLUTIONS

Bring Your Own Identity

Die Blockchain-Technologie könnte das Identitätsmanagement revolutionieren

Das BYOI-Konzept stellt eine digitale Identität in den Mittelpunkt, die den Nutzer wieder zum Herrn über seine eigenen personenbezogenen Daten macht. Doch auch für Unternehmen und Organisationen bietet das Konzept einige klare Vorteile – nicht zuletzt bei der Realisierung rechtlicher Vorgaben.

Ob Logins bei Facebook, Amazon, Google oder jedem anderen Webservice: Digitale Identitäten sind in einer Vielzahl vorhanden. Bei jeder Registrierung muss eine E-Mail-Adresse zur Account-Eröffnung hinterlegt, durch Links in Bestätigungsmails validiert und der neue Account mit einem Passwort versehen werden. Als Konsequenz haben Nutzer solcher Webservices viele Konten mit – hoffentlich! – verschiedenen Passwörtern und müssen vermutlich öfter die Passwort-vergessen-Funktion nutzen, als ihnen lieb ist. Es findet ein regelrechter Spam an Identitäten statt. Dieses Problem wird heute durch Identity Federation und Anbieter von Identity as a Service (IDaaS) gelöst. Solche Dienste gibt es von diversen Softwareherstellern, jedoch bergen sie einige Risiken, die durch die Nutzung der Blockchain-Technologie eliminiert werden könnten, und das zugleich unter Berücksichtigung neuer regulatorischer Anforderungen wie etwa der EU-Datenschutz-Grundverordnung (EU-DSGVO).

Der Status Quo

Identity & Access Management (IAM) ist eine hochkomplexe Disziplin, vor allem für global agierende Unternehmen, die Tausende von Identitäten verwalten müssen. Die besondere Herausforderung liegt hierbei in der Vergabe von adäquaten Zugriffsberechtigungen. Mitarbeiter eines Unternehmens sollten dabei nur die Berechtigungen besitzen, die sie tatsächlich für ihr Tagesgeschäft benötigen, um das Risiko eines Verlustes von kritischen Daten durch Weitergabe der Mitarbeiter zu mindern, was als Prinzip des geringstmöglichen Privilegs (Principle of Least Privilege) bezeichnet wird. Wenn der Status einer Person sich ändert, z. B. durch erstmaligen Einritt in das Unternehmen, durch Beförderungen, Wechsel in eine andere Abteilung oder den Austritt aus dem Unternehmen, müssen Zugriffsrechte für die entsprechende digitale Identität ohne Zeitverzug angepasst werden. Dieser Prozess ist im IAM als Joiner-Mover-Leaver (JML) bekannt, er wird heute durch verschiedenste Softwarelösungen unterstützt.

IdaaS: Gut, aber nicht perfekt

Zahlreiche Serviceprovider bieten die Möglichkeit, Identitäten cloudbasiert zu verwalten und dadurch eine effiziente Authentifizierungsinfrastruktur zu bieten. Mit der Nutzung solcher IdaaS-Lösungen geht die Möglichkeit für ein Single-Sign-On (SSO) einher. Jeder Mitarbeiter eines Unternehmens benötigt damit nur noch eine Identität, die mit allen Applikationen und Fileshares verbunden ist, auf die er Zugriff haben soll. Dies setzt eine entsprechende Integration aller relevanten Systeme voraus. Die Vorteile liegen klar auf der Hand: Es ist nur noch eine Identität im Unternehmen pro Mitarbeiter zu verwalten, die an das Berechtigungsmanagement gekoppelt ist.

IDaaS kann das Problem des Identitätsspams lindern. Jedoch setzt dies das Vertrauen in den entsprechenden Provider voraus, der als zentrale Instanz alle Identitäten außerhalb des Unternehmens verwaltet. Weiterhin hat der Nutzer selbst keine Hoheit über die ihm zugeordneten Daten, da er nicht im Mittelpunkt steht, sondern vielmehr ein zu verwaltendes Objekt darstellt. Vorteilhafter wäre eine einzige digitale Identität, die der Nutzer vollständig unter Kontrolle hat – universell einsetzbar bei Google, Amazon oder sonstigen Webservices, für Behörden und auch den Einsatz beim Arbeitgeber. Die eine digitale Identität, ganz im Besitz des Nutzers, die echtes „Bring Your Own Identity“ (BYOI) ermöglicht. Diese Idee wirft einige Fragen auf: Wer verwaltet die digitale Identität und die verknüpften Informationen? Wie erhalten die jeweiligen Institutionen Zugriff auf die Daten und wo liegen diese? Und wie kann eine Berechtigungsstruktur an die eine digitale Identität sicher verknüpft werden?

Die Blockchain-ID

Die Blockchain-Technologie, oder auch Distributed-Ledger-Technologie (DLT), ist allgemein formuliert eine dezentrale Datenbank, die bei allen aktiven Teilnehmern der Blockchain verteilt liegt. Sie basiert auf einem Peer-to-Peer-Netzwerk (P2P) aus sogenannten Nodes, die individuell die vollständigen Informationen der Blockchain speichern. Werden Informationen ausgetauscht, d. h. Transaktionen ausgeführt, so müssen alle Teilnehmer Konsens über die Transaktionen erzielen. Dies geschieht über einen kryptografischen konsensbildenden Algorithmus (bei Bitcoin z. B. „Proof-of-Work“). Eine Manipulation der Transaktionen ist nicht möglich, da Prüfinformationen der vorangegangen Transaktion im nächsten Block gesichert werden. Durch die Dezentralität besteht keine Notwendigkeit für eine zentrale kontrollierende Instanz, wie sie derzeit in vielen Netzwerken üblich ist.

Ein Anwendungsfall, der noch nicht intensiv erforscht wurde, aber die Probleme des Identitätsspams lösen könnte, ist die Speicherung von digitalen Identitäten in der Blockchain. Eine solche Blockchain-ID bietet die Vorteile, dass sie unanfechtbar ist und keine zentralen Validierungsverfahren benötigt. Alle persönlichen Informationen können mit der Blockchain-ID verknüpft und dort auch abgelegt werden. Dies könnte im einfachsten Fall etwa eine Postadresse sein, aber auch Bankverbindungs- oder Führerscheindaten sind denkbar; weiterhin können Zugriffsberechtigungen hinterlegt werden – ein flexibles Datenmodell basierend auf JSON-Objekten lässt vielfältige Nutzungen zu. Die Blockchain-ID könnte sowohl mit allen persönlichen Services, die genutzt werden, als auch mit Applikationen des Arbeitgebers verknüpft werden (BYOI). Der größte Vorteil einer Blockchain-basierten Lösung besteht darin, dass der Nutzer selbst die Verwaltungs- und Freigabe-

macht innehat. So würde er wieder Herr seiner eigenen Daten und wäre nicht mehr auf eine zentrale Instanz angewiesen. Eine echte souveräne digitale Identität wäre geschaffen, die auch für andere Arten von Entitäten erstellt werden könnte, z. B. für Organisationen oder Applikationen. Durch das Knüpfen von Beziehungen zwischen den IDs ließe sich ein Vertrauensnetzwerk (Web of Trust) aufbauen, das die Glaubwürdigkeit der Identitäten untermauert. So könnten personenbezogene Identitäten de facto durch vertrauenswürdige Organisationen, z. B. behördliche Stellen, validiert werden.

Auflagen der EU-DSGVO

Seit einigen Jahren wird auf EU-Ebene diskutiert, wie das Thema Datenschutz und -sicherheit in den Mitgliedsstaaten standardisiert werden könnte. Das Ergebnis der Diskussionen ist die im April 2016 verabschiedete EU-DSGVO, die die bisherige EU-Datenschutzrichtlinie ablöst und in Deutschland das Bundesdatenschutzgesetz (BDSG) weitgehend ersetzen wird. Die wichtigsten neuen Anforderungen der Verordnung und ihre Auswirkungen lassen sich in drei Oberthemen zusammenfassen.

Technikgestaltung: Technologien, die personenbezogene Daten verarbeiten, müssen zukünftig, beispielsweise durch Zertifizierungen, in ihren technischen und organisatorischen Maßnahmen sowohl in Gestaltung als auch in den Voreinstellungen dem Stand der Technik entsprechen, sofern dies in einem angemessenen Verhältnis mit den Implementierungskosten und dem Zweck der Verarbeitung steht. Der „Stand der Technik“ ist dabei ein weit diskutierter juristischer Begriff, der bewusst offen definiert wurde. Eine Zertifizierung nach ISO 27001 könnte beispielsweise ein guter Indikator sein, dass der Stand der Technik berücksichtigt wird. Für IDaaS bedeutet dies insbesondere, dass eine sichere Verbindung (beispielsweise durch Layer3-VPN) zum Cloud-Service bestehen muss und der Cloud-Server mit entsprechenden Prozessen zu Data Leakage Prevention (DLP) ausgestattet ist. Weiterhin müssen die Voreinstellungen für ein Benutzerprofil so gesetzt sein, dass möglichst wenige personenbezogene Daten gesammelt werden. So wird sichergestellt, dass nur die tatsächlich für den Service benötigten Daten erhoben und gespeichert werden.

Auskunfts- und Löschprozesse: Die EU-DSGVO gibt betroffenen Personen, deren personenbezogene Daten verarbeitet werden, neue Rechte im Umgang mit diesen. So haben sie das Recht, alle personenbezogenen Daten in strukturierter Form anzufordern, wenn beispielsweise ein Anbieter gewechselt werden soll (Recht auf Datenübertragbarkeit). Ein anderer Aspekt ist das „Recht auf Vergessenwerden“: Betroffene Personen haben durch die EU-DSGVO nun das Recht, eine Löschung aller ihrer personenbezogenen Daten anzuordnen. Das Unternehmen hat auch hier einen erheblichen Mehraufwand, da alle Daten in jeder Datenbank zur Verarbeitung unbrauchbar gemacht werden müssen.

Datenschutzfolgenabschätzung ist eine weitere neue Anforderung für das Risikomanagement in Unternehmen. Unternehmen müssen nun Risikobewertungen für Technologien anfertigen, die personenbezogene Daten verarbeiten. Werden personenbezogene Daten besonderer Kategorien verarbeitet (z. B. politische Einstellung oder religiöse Überzeugung), so muss ein Bericht über die Folgen der Datenverarbeitung erstellt werden. Eine große Herausforderung hierbei stellt bereits die Feststellung dar, ob die personenbezogenen Daten als besondere Kategorie klassifiziert werden können.

All diese Anforderungen der EU-DSGVO haben einen hohen Mehraufwand für Unternehmen im Umgang mit digitalen Identitäten und der

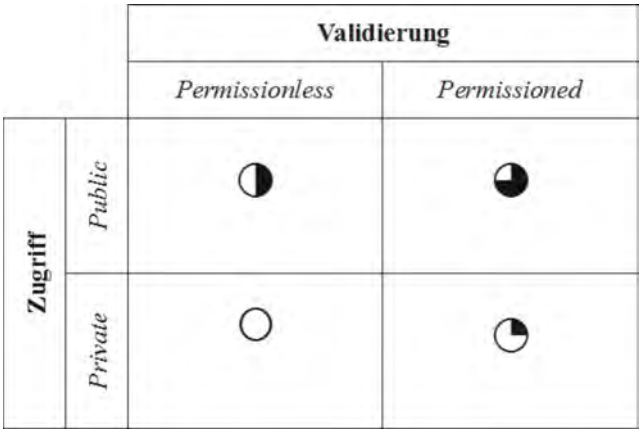
Verknüpfung von personenbezogenen Daten zur Folge. Die Blockchain-Technologie und der Einsatz eines BYOI-Konzeptes könnten also nicht nur zahlreiche Vorteile für den Nutzer bieten, sondern gleichzeitig die Anforderungen der EU-DSGVO in der Praxis realisieren und die Einführungsaufwände reduzieren.

Flexibles IAM mit BYOI

Mit der Nutzung einer Blockchain-ID ließen sich die Schutzziele der EU-DSGVO effizient umsetzen und zugleich Einsparungen in Unternehmen erzielen. So sind z. B. einige Punkte, die den erforderlichen Stand der Technik betreffen, durch den Einsatz der Blockchain-Technologie per se abgebildet. Der Anspruch der sicheren Authentifizierung ist einer der Hauptaspekte zur Nutzung der Blockchain für das IAM. Daneben ist eine kryptografische Speicherung aller Daten inhärent gegeben. Mögliche Datenverluste sind durch die dezentrale mehrfache Speicherung nahezu ausgeschlossen und datenschutzfreundliche Voreinstellungen durch den Nutzer selbst prüf- und beeinflussbar. Ein relativierender Faktor ist allerdings der zukünftige Einsatz von Quantencomputern, mit denen die kryptografische Datenverschlüsselung auflösbar wäre.

Das Recht auf Datenübertragbarkeit lässt sich durch die Nutzung einer Blockchain-ID für Unternehmen sehr effizient gestalten. Sie sind dadurch nicht mehr in der Bringschuld, personenbezogene Daten in strukturierter Form an die betroffene Person zu übermitteln, falls beispielsweise ein Anbieterwechsel angestrebt ist. Da der Nutzer selbst wieder die Hoheit über seine Daten hat, muss bei diesem Anwendungsbeispiel lediglich die Berechtigung der Nutzung für das Unternehmen A entzogen und für das Unternehmen B freigegeben werden. Genau durch diese freie Ausgestaltung ist auch der Löschprozess nicht mehr mit hohem Aufwand verbunden – unter der Voraussetzung, dass das Unternehmen die Daten lediglich aus der Blockchain-Datenbank genutzt und nicht unternehmensintern in eigene Datenbanken abgelegt hat.

Die größte Herausforderung bei der Datenschutzfolgenabschätzung ist für Unternehmen, alle personenbezogenen Daten bis auf Datenbank- bzw. Feldebene hinunter zu identifizieren. Nur so kann festgestellt werden, für welche Technologien eine Folgenabschätzung angestrebt werden muss. Da in dem beschriebenen Konzept des BYOI alle Daten aus einem Datenpool gezogen werden, müssten nur die Verknüpfungen aller Technologien mit den entsprechenden Daten der Blockchain-ID überprüft werden. So ließe sich die Datenklassifizierung mit den Daten der Nutzer, die den Unternehmen zur Verfügung gestellt werden, abgleichen und auf diese Weise relativ schnell erörtern, welche Technologien ein hohes Risiko bergen.



Quelle: esatus AG

Architektur-Bewertungsmatrix

Anwendungsszenarien

Eine einmal etablierte digitale Blockchain-Identität kann für zahlreiche Anwendungsfälle eingesetzt werden. So lässt sich etwa die Adresse einer Person als ein Datensatz hinterlegen. Die zuständige Einwohnermeldebehörde attestiert diese Adresse dann, d. h. sie bestätigt sie als gültige Meldeadresse. Da die digitale Identität samt zugehöriger Daten, abgespeichert in der Blockchain, unanfechtbar ist, kann sie auch für Anwendungsfälle freigegeben werden, die besondere Sicherheitsanforderungen mit sich bringen. Der Inhaber der digitalen Identität hat z. B. die Möglichkeit, in den Fällen, in denen eine behördlich bestätigte Meldeadresse übermittelt werden muss, dem Empfänger die Adresse samt offizieller Bestätigung bekanntzugeben.

Ein weiterer praktischer Anwendungsfall ist die Nutzung der eigenen digitalen Identität im Rahmen eines Arbeitsverhältnisses. Beim Beginn an der Arbeitsstelle werden für den neuen Mitarbeiter alle Berechtigungen, die er für die Ausübung seiner Tätigkeit benötigt, mit dessen Blockchain-ID verknüpft. Verlässt er das Unternehmen wieder, so werden die bestätigten Berechtigungen an der Blockchain-ID wieder aufgelöst. Nicht nur für das Arbeitsverhältnis, auch für privat genutzte Online-Services von Anbietern wie Facebook und Google, wären dadurch in Zukunft keine weiteren Accounts nötig. Die Anwendung der Blockchain-ID ermöglicht dem Inhaber einen effizienten Authentifizierungsprozess und die Entscheidungshoheit darüber, welche persönlichen Daten dem entsprechenden Service zur Verfügung gestellt werden sollen. Diese Entscheidung ist via Blockchain-ID zu einem späteren Zeitpunkt wieder revidierbar. Das Recht auf Vergessenwerden könnte so eigenständig durch den ID-Inhaber selbst ausgeübt werden.

Architekturen

Beim Aufbau einer Blockchain-IAM-Lösung sind insbesondere zwei Dimensionen zu betrachten: Zugriff und Validierung. Die Dimension des Zugriffes definiert, ob es Zugriffsbeschränkungen für das Lesen der Daten gibt (private) oder nicht (public). Die Dimension der Validierung unterscheidet, welche Clients die Transaktionen verarbeiten, d. h. neue Blöcke bilden und der Blockchain hinzufügen dürfen. Bei „permissionless“ Blockchains hat jeder Client dieselben Rechte, neue Blöcke zu schaffen; bei „permissioned“ Blockchains gibt es eine beschränkte Liste von Clients mit Schreibberechtigung (vgl. Abbildung).

Als besonders beachtenswert hat sich die Dimensionskombination der Public Permissioned Blockchains herauskristallisiert. Bei diesem Konstrukt wird von einer vertrauenswürdigen Gruppe – einem Konsortium – ausgegangen, die die Validierung der Transaktionen übernimmt. Die Möglichkeit des lesenden Zugriffs wird jedoch public gewährt, was sie für eine breite Population nutzbar macht. So wird eine souveräne digitale Identität ermöglicht: Das Betreiberkonsortium könnte ein übergreifendes, globales IAM etablieren. Identitätssilos können abgeschafft werden, da der Nutzer BYOI real praktizieren kann. Wesentlicher Erfolgsfaktor sind allerdings umfassende Diversität und Vielfalt im Konsortium, um Glaubwürdigkeit zu schaffen und einen großen Anwenderkreis zu überzeugen.

Risiken

Bei dem dargestellten Anwendungsfall handelt es sich derzeit um ein theoretisches Konzept, das bislang noch keine praktische Realisierung gefunden hat. Die Blockchain-Technologie wird derzeit intensiv erforscht und aktuell primär für den Anwendungsfall finanzieller Transaktionen genutzt. Zahlreiche Punkte stehen in der öffentlichen Kritik,

diese bedürfen noch der Klärung und weiteren Erforschung – so bislang auch der Ansatz des BYOI. Die größten Hemmnisse eines Blockchain-IAM werden im Folgenden dargestellt.

Die 51 %-Attacke birgt bei der Blockchain-Technologie das größte Risiko. Bei diesem Angriff wird vorausgesetzt, dass ein Teilnehmer des Netzwerkes über 50 % der Transaktionsrechenkapazität stellt. Dadurch könnte ein Angreifer Transaktionen in der Blockchain beliebig manipulieren, in dem dargestellten Anwendungsfall also etwa die Bereitstellung personenbezogener Daten einer Blockchain-ID. In diesem Fall wäre der Einsatz der Blockchain für das Konzept des BYOI mehr als ungeeignet. Der Lösungsansatz besteht aktuell darin, eine große Grundgesamtheit von Nodes sicherzustellen. Dieses Angriffsszenario betrifft besonders alle Public Permissionless Blockchains.

Verlust der digitalen Identität: Eine Gefahr besteht für den Anwender darin, dass sein privater Schlüssel, mit dem er Zugriff auf seine digitale Identität erlangt, kompromittiert wird. Einerseits kann dies dadurch bedingt sein, dass der ID-Inhaber seinen privaten Schlüssel verliert. Dies kommt einem Vergessen des Passwortes gleich, allerdingst gibt es keine zentrale übergeordnete Instanz, die das Passwort zurücksetzen könnte. Für diese Problematik werden bereits verschiedene Lösungsansätze diskutiert: So können bei der Erstellung eines Profils mehrere vertrauenswürdige Personen bestimmt werden, die im Falle eines Schlüsselverlustes bestätigen müssen, ob der Wunsch zur Generierung eines neuen Schlüssels rechtmäßig ist. Dabei lassen sich Schwellenwerte hinterlegen, d. h. es kann ein Minimum von notwendigen zustimmenden Personen definiert werden. Mit dieser Prozedur lässt sich dann ein neuer privater Schlüssel für das Profil generieren. Schwerwiegender ist der Fall, dass der private Schlüssel in falsche Hände gerät. Dies entspricht einem vollständigen Verlust der digitalen Identität, mit der Folge, dass unerwünschte Aktivitäten im Namen des eigentlichen Eigentümers der ID initiiert werden können. Aber auch hier kann der private Schlüssel zurückgesetzt werden.

Kritische Masse: Wie jede innovative Idee, so muss auch die Blockchain-ID von einer ausreichenden Zahl an Teilnehmern akzeptiert und genutzt werden. Wenn nicht genügend Nutzer, Behörden und Unternehmen existieren, die ihr aktuelles IAM zukunftsweisend ändern möchten, so wird der Ansatz nicht bestehen können. Zum Start müsste ein Konsortium aus interessierten Unternehmen gebildet werden, das einerseits für die Validierung der Identitäten zuständig ist und das andererseits die Lösung im jeweiligen Unternehmen unmittelbar einsetzen möchte. Ein solcher Proof-of-Concept könnte ein Treiber für die weiterführende, generelle Akzeptanz des Ansatzes sein.

Rechtliche Unsicherheit: Grundsätzlich zu erwägen sind rechtliche Aspekte der Blockchain-Technologie, die derzeit noch weitgehend ungeklärt sind. So ist im Sinne der EU-DSGVO zu klären, inwiefern eine Blockchain-basierte digitale Datenhaltung und -verwaltung im Einklang mit dieser Gesetzgebung steht. Juristisch geprägte Grundsatzdiskussionen sind daher in diesem Kontext zu erwarten – und auch notwendig.

Ausblick

Ist 2017 das Jahr der Blockchain? Kann die Technologie jetzt einen echten Durchbruch erzielen? Zumindest wird dieses Jahr wegweisend für die Blockchain und darauf aufbauende technologische Ansätze sein. Welche Anwendungen davon profitieren können und für wen sie zur Verfügung stehen, wird derzeit in zahlreichen Forschungsgruppen untersucht. Identity & Access wurde vielerorts als ein äußerst erfolgsversprechender Bereich identifiziert, z. B. durch die Arbeitsgruppe „Blockchain“ des TeleTrusT Bundesverband IT-Sicherheit e.V.

Im Bereich des IAM sollte insbesondere die Durchsetzungsfähigkeit einer Public Permissioned Blockchain betrachtet werden: In diesem Szenario dürfen nur erlaubte Nodes Transaktionen validieren, Zugriff und Nutzung sind jedoch für eine breite Nutzergemeinschaft möglich. Dies spricht für die Schaffung eines entsprechenden Konsortiums von Organisationen, die das Netzwerk betreiben, die Nutzung aber für jedermann öffnen. Lösungsansätze, die konzeptionell auf dieser Grundlage aufbauen, sind besonders Erfolg versprechend – das Unternehmen oder Start-up, dem es gelingt, genügend Aufmerksamkeit zu generieren, um eine kritische Masse zu erreichen, wird den Wettlauf um die Blockchain-basierten digitalen Identitäten für sich entscheiden.

Dr. André Kudra
Vorstand (CIO), esatus AG

Patientendaten in der Cloud

Die Realisierung der elektronischen Patientenakte erfordert neue Lösungsmodelle

Ärzte und Krankenhäuser scheuen bislang weitgehend vor der Nutzung von Cloud-Diensten zurück, denn im Gesundheitssektor gelten besonders hohe datenschutzrechtliche Standards. Mithilfe geeigneter Verschlüsselungstechniken könnten aber einige Hürden überwunden werden.

Die Verlagerung von IT-Infrastrukturen in die Cloud ist mittlerweile zum Mainstream geworden. Nur im Gesundheitssystem ticken die Uhren anders: Arztpraxen und Krankenhäuser betreiben eigene IT-Systeme, obwohl ihre Personaldecken und technischen Kenntnisse dafür oft gar nicht ausreichen. Die Folgen können gravierend sein: Im vergangenen Jahr mussten erstmals etliche Arztpraxen und Krankenhäuser infolge von Cyberangriffen oder Krypto-Trojanern ihren Betrieb – zumindest zeitweise – einstellen.

Rechtliche Beschränkungen

Der wichtigste Grund für den lokalen Betrieb der IT-Systeme im Gesundheitsbereich ist der Schutz der sensiblen Patientendaten, deren Erhebung, Verarbeitung und Nutzung nach dem Bundesdatenschutzgesetz (§ 4 BDSG) grundsätzlich verboten ist. Erlaubt ist dies nur ausnahmsweise dann, wenn eine klare Rechtsgrundlage vorliegt oder die betroffene Person ausdrücklich ihre Zustimmung gegeben hat. Noch strengere Maßstäbe legt der § 203 StGB an, nach dem Ärztinnen und Ärzte, die fremde, ihnen in ihrer Funktion anvertraute Geheimnisse offenbaren, mit empfindlichen Freiheits- oder Geldstrafen belegt werden können. Als Geheimnis gelten im medizinischen Bereich sämtliche personenbezogenen Daten und Tatsachen – ja bereits schon der Umstand, dass überhaupt ein Behandlungsverhältnis besteht – sowie alle übrigen Informationen, die während der Behandlung bekannt werden (z. B. Wohn- und Lebenssituation, Suchterkrankungen, sexuelle Orientierung, Vermögenslage, körperliche Hygienesituation usw.).

Der Schutz dieser persönlichen Daten hat einen sehr hohen rechtlichen Stellenwert, sodass deren Offenbarung nur in einigen Sonderfällen gerechtfertigt ist. Doch mithilfe dieser gesetzlichen Rechtfertigungsgründe kann ein regulärer Rechenzentrumsbetrieb von Arzt- oder Krankenhaussoftware nicht realisiert werden. Als Lösung ebenfalls nicht ausreichend sind Hilfskonstruktionen wie die Verpflichtung des Auftragnehmers auf Schweigepflicht oder die Einstufung des externen Dienstleisters als Gehilfen. Auch die aktuellen Vorstöße der Regierung, das Arztgeheimnis zugunsten Dritter aufzuweichen, entbinden Ärzte nicht von ihrer Sorgfaltspflicht zum bestmöglichen Schutz der Patientendaten und zur Überwachung der beauftragten Dienstleister.

Technischer Datenschutz durch Verschlüsselung

Es gibt allerdings eine Möglichkeit, den Schutz der persönlichen Patientendaten zu wahren und diese trotzdem in ein Rechenzentrum auszulagern. Durch den Einsatz geeigneter Verschlüsselungstechniken verlieren Daten dann ihren Personenbezug, wenn der Dienstleister keine Möglichkeit hat, die Daten selbst zu entschlüsseln. Diese Auffassung wird auch von deutschen Datenschutzbehörden vertreten, die mit einem starken kryptografischen Verfahren nach dem aktuellen Stand der Technik sicher verschlüsselte Daten für nicht mehr personenbezogen halten. Daher muss auch ein Verlust von Daten, die nach dem Stand der Technik verschlüsselt wurden, nicht nach § 42a BDSG gemeldet werden. Durch kryptografische Verschlüsselung personenbezogener Daten wird es daher möglich, Patientendaten in einem Cloud-System zu speichern, ohne gegen die Vorschriften des Datenschutzes und des Strafgesetzbuches zu verstoßen. In der IT-Welt haben diese Konzepte bereits verschiedenen Namen. Man spricht unter anderem von „Security by Design“ oder auch von „Host-proof Hosting“.

Entscheidend in einem solchen System ist, dass die kryptografischen Schlüssel, die zur Ver- und Entschlüsselung der Daten verwendet werden, den Administratoren des Rechenzentrums nicht bekannt sind. Möchte eine Arztpraxis oder ein Krankenhaus das System nutzen, müssen die benötigten Schlüssel daher auf der Client-Seite erzeugt werden und dürfen diese niemals im Klartext verlassen. Um ein unbefugtes Auslesen zu verhindern, dürfen die Schlüssel aber nicht auf den Clients, sondern mit einem weiteren Geheimnis des Benutzers verschlüsselt auf dem Server abgelegt werden.

Zur Speicherung der Daten im Rechenzentrum reicht es auch nicht aus, die Datenbank als Ganzes zu verschlüsseln, da in diesem Fall der Schlüssel selbst im Zugriff ihres Administrators wäre. Die Verschlüsselung der zu speichernden Patientendaten muss vielmehr auf der Client-Seite durch eine Ende-zu-Ende-Verschlüsselung mit dem Schlüssel des Benutzers erfolgen, bevor die Daten seinen Rechner verlassen. So geschützt werden die Daten zum Rechenzentrum transportiert.

Suche auf verschlüsselten Daten

Es gibt aber noch weitere technische Herausforderungen zu meistern. Ein clientseitiges Ver- und Entschlüsseln der Daten ist nichts Neues und wird heutzutage auch von jedem gängigen Cloud-Backup-System beherrscht. Für eine komplexe, von mehreren Benutzern verwendete Full-Business-Application ist es aber nicht darstellbar, jedes Mal den gesamten Datenbestand herunterzuladen, zu bearbeiten und später wieder hochzuladen. Tatsächlich ist es zwingend notwendig, dass auf den verschlüsselten Daten Suchoperationen durchgeführt werden können, um nur die Datensätze zu laden, die man aktuell benötigt.

Selbstverständlich können diese Anfragen nicht im Klartext zum Server gesendet werden, denn zum einen könnte auch schon die Suchanfrage selbst ein schützenswertes Geheimnis beinhalten, zum anderen kann der Server die entsprechenden Datensätze gar nicht identifizieren, denn sie sind ja verschlüsselt. Um dieses Problem zu bewältigen, ist es notwendig, auch die Suchanfrage zu verschlüsseln und mit dieser den Server dann in den verschlüsselten Daten suchen zu lassen. Etwas opportunistisch ausgedrückt, weiß der Server nicht,

wonach er sucht, und er weiß auch nicht, was er findet. Aber das, was er findet, sendet er zum Client zurück, und nachdem dieser es entschlüsselt hat, erhält er die angeforderten Daten.

Dezentralisierung und verteilte Datendepots

Aber nicht nur in Arztpraxen und Krankenhäusern können Ende-zu-Ende-verschlüsselte Cloud-Systeme Effizienz und Kollaboration verbessern. In elektronischen Patientenakten können die Patienten selbst die Daten verschiedener Ärzte und Krankenhäuser sammeln und diesen eigene, etwa durch Wearables erzeugte Daten selektiv zur Verfügung stellen. Im europäischen Vergleich hinkt Deutschland hier hinterher, die Datenskandale der Vergangenheit zeigen aber auch, dass Datenhoheit und -sicherheit sowie Einflussmöglichkeiten von Patienten essenziell für ein funktionierendes System sein werden.

Die realistische Alternative ist ein dezentrales System mit verteilter Datenhaltung. Die Gesundheitsdaten jedes Patienten würden dabei durch kryptografische Verfahren geschützt redundant in verschiedenen Instanzen gespeichert. Die individuelle Verschlüsselung sorgt für die notwendige Datenhoheit und schützt wirksam vor dem Zugriff Unbefugter. Der Datenaustausch erfolgt mittels asymmetrischer Verschlüsselung, indem auszutauschende Daten in den Client geladen und dort mit dem öffentlichen Schlüssel des Empfängers verschlüsselt werden. So vor dem Zugriff Dritter geschützt können sie zentral abgelegt werden, bis der Empfänger die Daten abholt, mit seinem privaten Schlüssel entschlüsselt und wiederum für das Speichern in seiner eigenen Datenhaltung mit seinem eigenen Schlüssel verschlüsselt. Ärzte können über dieses Verfahren ihre Daten selektiv mit ihren Patienten teilen, ohne Praxisinterna preiszugeben oder die Behandlungshoheit zu verlieren; Patienten entscheiden selbst, welche Daten sie an ihre behandelnden Ärztinnen und Ärzte weitergeben.

Ein weiter Weg

Im Gegensatz zu den Herausforderungen der Cloud-Speicherung von Patientendaten im Rahmen einer Arztpraxis, für die es bereits marktreife Lösungen gibt, sind die weiteren organisatorische Rahmenbedingungen einer ganzheitlichen Lösung und deren Finanzierung noch vollkommen ungelöst. Patientenfinanzierte Modelle sind wiederholt gescheitert, Finanzierung und Betrieb durch die Kostenträger werden von der Ärzteschaft abgelehnt und in einem Ende-zu-Ende-verschlüsselten System scheidet eine Drittverwertung der Daten als Finanzierungsquelle aus. Auch fehlt eine inhaltliche Definition standardisierter Datenstrukturen (Interoperabilität), die, wie die Erfahrungen aus den USA zeigen, für den Datenaustausch zwischen verschiedenen Systemen unabdingbar ist. Der Einsatz von Cloud-Software ist in einer Reihe von Arztpraxen zwar heute bereits Realität, doch die elektronische Patientenakte wird wohl noch eine Weile auf sich warten lassen.

Alexander Wilms und Jochen Brüggemann
Geschäftsführer RED Medical Systems GmbH

Schlüsselaushandlung per PAKE-Protokoll

Auch mit Passwörtern lässt sich noch ein hohes Maß an Sicherheit erreichen

Zur Authentifizierung werden nach wie vor einfache Passwortverfahren genutzt, die potenzielle Angreifer kaum abwehren können. Um dies dennoch zu erreichen, wurden sogenannte PAKE-Protokolle entwickelt, die das Aushandeln eines kryptografischen Schlüssels auf Basis eines geteilten Passworts erlauben.

Passwörter sind in der Regel leicht zu merken und schnell einzugeben. Infolgedessen werden sie auch im Internet sehr häufig zur Authentifizierung verwendet. Da die Nutzer ihre Kennwörter regelmäßig eingeben müssen, wählen sie oft einfache und einprägsame, also sehr schwache Zeichenfolgen. So sind laut einer Studie des Hasso-Plattner-Instituts von Ende 2016 die meistbenutzten Passwörter in Deutschland „hallo“, „passwort“ und „hallo123“. Dies zeigt eindrucksvoll, wie leicht es Angreifern oftmals gemacht wird, Passwörter durch simples Durchprobieren zu ermitteln.

Aber auch zufällig gewählte Passwörter können nicht den gleichen Schutz wie kryptografische Schlüssel bieten. Letztere sind allerdings nicht dafür geeignet, von einem Nutzer eingetippt zu werden. Um dieses Spannungsfeld – einfach zu merkende und einzugebende Zugangsdaten vs. größtmögliche Sicherheit – aufzulösen, wurden bereits im Jahr 1992 von S. Bellovin und M. Merritt „Password-Authenticated-Key-Exchange-Protokolle“ (PAKEs) vorgestellt. Die grundlegende Idee hinter diesen Protokollen ist, dass beide Seiten den Besitz des Passworts beweisen, ohne es direkt auszutauschen. Damit ist das Verfahren gegen Offline-Angriffe abgesichert, denn ein Angreifer, der das Passwort nicht kennt, muss zur Verifikation jedes Versuches mit einer legitimen Partei interagieren und wird so schnell entdeckt.

Der Veröffentlichung des ersten PAKE-Protokolls – „Encrypted-Key-Exchange-Protokoll“ (EKE) – von Bellovin und Merritt folgten verschiedene andere Ideen und Standards. Allen bisher veröffentlichten PAKE-Protokollen ist jedoch gemein, dass sie asymmetrische Kryptografie verwenden. Wie die Parteien die öffentlichen Schlüssel austauschen und benutzen, um sich auf einen gemeinsamen symmetrischen Schlüssel zu einigen, variiert jedoch zwischen den Protokollen. Das Ziel, sicher gegen Offline-Angriffe auf das Passwort zu sein, wird dadurch erreicht, dass weder das Passwort selbst noch davon abgeleitete Daten zwischen den Kommunikationspartnern übertragen werden.

Schlüsselaustausch

Eine Möglichkeit, die z. B. vom EKE umgesetzt wird, besteht darin, eine symmetrische Verschlüsselung mit einem vom Passwort abgeleiteten Schlüssel zu nutzen, um einen ephemeren öffentlichen Schlüssel zu verschlüsseln und auszutauschen. Die erfolgreiche Entschlüsselung des asymmetrischen Schlüssels beweist, dass der Empfänger das Passwort kennt. Für einen Angreifer darf sich das Resultat jedoch nicht von einem Zufallswert unterscheiden, damit im Fall einer passiven Attacke jedes mögliche Passwort gleich wahrscheinlich bleibt.

Öffentliche Schlüssel können jedoch auch unverschlüsselt übertragen werden. Ein prominentes Beispiel eines solchen Protokolls ist „Password Authenticated Key Exchange by Juggling“ (J-PAKE). Hier werden verschiedene ephemere Schlüssel und andere Werte ausgetauscht, die teilweise vom gemeinsamen Passwort abhängen. Die Werte an sich werden jeweils mit zufälligen Zahlen versehen, sodass sie einem Angreifer keine Informationen preisgeben. Die legitimen Kommunikationspartner können jedoch unter Verwendung des Passworts

Alice Gemeinsames Passwort Π		Bob Gemeinsames Passwort Π
Wählt zufällige Nonce n		
Verschlüsselt n mit Π : $c=E_{\Pi}(n)$	--- c --->	Entschlüsselt c mit Π : $n=D_{\Pi}(c)$
Bildet n auf g ab: $g=M(n)$		Bildet n auf g ab: $g=M(n)$
Wählt zufälligen Wert x		Wählt zufälligen Wert y
Berechnet $X=g^x$	--- X ---> <--- Y ---	Berechnet $Y=g^y$
Berechnet $K=Y^x$		Berechnet $K=X^y$
Leitet aus K symmetrische Schlüssel für die weitere Kommunikation ab		Leitet aus K symmetrische Schlüssel für die weitere Kommunikation ab

Quelle: secunet

Exemplarischer Ablauf von PACE: Neben dem Passwort nutzen Alice und Bob ein symmetrisches Verschlüsslungsverfahren (E,D), eine geeignete Gruppe G und ein (ggf. interaktives) Mapping M, das eine zufällige Zahl auf einen Generator von G abbildet. (E,D), G und M müssen nicht geheim gehalten werden.

einen gemeinsamen kryptografischen Schlüssel berechnen. Ähnlich arbeitet auch das „Simple-Password-Exponential-Key-Exchange-Protokoll“ (SPEKE), bei dem das Passwort die Basis eines Diffie-Hellman-Schlüsselaustausches bestimmt. Im Gegensatz zu J-PAKE kommt SPEKE aber mit nur zwei wechselseitigen Nachrichten aus.

Eine Kombination der Methoden EKE und SPEKE wird beim „Password Authenticated Connection Establishment“ (PACE) verwendet. Praktische Anwendung findet PACE beispielsweise in internationalen Reisedokumenten. Im ersten Schritt des Protokolls wird eine zufällige Nonce symmetrisch mit einem auf dem Passwort basierten Schlüssel verschlüsselt, übertragen und vom Gegenüber entschlüsselt. Anschließend bilden beide Partien diese Nonce auf einen Generator für einen Diffie-Hellman-Schlüsselaustausch ab. Die Schlüsselaushandlung erfolgt nun wie bei SPEKE unter Verwendung des geheimen Generators (siehe Abbildung).

Passwortspeicherung

Die obigen Protokolle sind *balancierte* PAKEs. Balanciert bedeutet hierbei, dass beide Parteien die gleiche Repräsentation des Passworts verwenden. Dabei ist es ebenfalls möglich, dass eine Seite z. B. einen Hash des Passworts speichert und das Protokoll mit dem Hash ausgeführt wird. Bei balancierten PAKEs können beide Seiten die Kommunikation initiieren. Daher eignen sie sich auch für Peer-to-Peer-Netzwerke.

Es gibt allerdings noch eine zweite Gruppe von PAKE-Protokollen: Existiert eine klare Client-Server Architektur, können *augmented* PAKEs verwendet werden. Hier besitzt eine Seite ein mittels einer Einwegfunktion transformiertes Passwort und die andere Seite das Passwort als Klartext (oder eine Abwandlung davon wie im vorherigen Fall). Bei der Schlüsselaushandlung wird nun klar zwischen den beiden Parteien unterschieden. Der Vorteil dieser Unterscheidung wird evident, falls der Server kompromittiert wird: Im balancierten Fall könnte der Angreifer die erbeuteten Passwörter direkt für die Kommunikation mit anderen Servern verwenden und sich als legitimer Client ausgeben. Falls ein Angreifer Zugriff auf den Server erlangt, ist ein Offline-Angriff möglich. Der benötigte Aufwand, ein Passwort zu raten, hängt in diesem Fall nur von dessen Stärke ab. Im Fall von augmented PAKEs muss er erst das Passwort mittels einer Offline-Wörterbuchsuche erraten, da er die gewonnenen Informationen nicht direkt verwenden kann.

Ein Beispiel für ein augmented PAKE ist AugPAKE. Hier besitzt eine Kommunikationspartei, der Client, das Passwort, die andere, der Server, eine Art öffentlichen Schlüssel, der mithilfe des Passworts erstellt wurde. Damit und mit einem beim Austausch erzeugten geheimen Schlüssel berechnet der Server einen Wert, aus dem der Client mittels des Passworts ebenfalls den geheimen Schlüssel berechnen kann.

Sicherheitsbetrachtungen

Um die Sicherheit eines Protokolls nachzuweisen, wird meist ein möglichst starker Angreifer angenommen. Im Fall von PAKE-Protokollen ist das gängige Szenario, dass zwei legitime Parteien (Alice und Bob) ein Passwort teilen und einen kryptografischen Schlüssel über eine unsichere Leitung aushandeln wollen. Ein Angreifer (Eve) möchte diese Schlüsselaushandlung unterlaufen. Dabei wird angenommen, dass Eve in Besitz eines Wörterbuchs ist, das auch das Passwort von Alice und Bob enthält. Darüber hinaus ist Eve in der Lage, sämtliche Passwörter dieses Wörterbuchs in einem Bruteforce-Angriff durchzuprobieren.

Die Sicherheit des Protokolls hängt nun von der Wahrscheinlichkeit ab, dass Eve das Passwort korrekt errät und sich beispielsweise erfolgreich als Man-in-the-Middle in die Schlüsselaushandlung einklinken kann. Falls die Erfolgswahrscheinlichkeit von Eve eine Funktion in der Interaktion mit Alice oder Bob ist, kann das Protokoll in diesem Szenario als sicher betrachtet werden. Mit anderen Worten, Eve lernt durch Mithören eines Protokolldurchlaufs nichts über das Passwort. Bei einem aktiven Versuch lernt Eve nur, ob das eine ausprobierte Passwort korrekt war. Daher bleibt als einzige Angriffsmöglichkeit, für jedes mögliche Passwort eine Verbindung mit Alice oder Bob aufzubauen und zu testen, ob es korrekt ist. Da dies jedoch eine Interaktion mit einer legitimen Partei erfordert, wird der Angriff von Eve unweigerlich entdeckt. Folglich muss also die Anzahl der zugelassenen Versuche eine Balance zwischen einem möglichen Denial-of-Service auf der einen und einem erfolgreichen Angriff auf der anderen Seite herstellen.

Varianten und Anwendungsgebiete

Neben der bereits erwähnten Anwendung von PAKE in Reisepässen gibt es Vorschläge und Ideen, wie diese Protokolle beispielsweise in IKEv2 (Internet Key Exchange Protocol version 2) und TLS (Transport Layer Security) eingesetzt werden können. Allerdings können PAKEs nicht nur zur Aushandlung von Schlüsseln dienen, sondern auch um einen Schlüssel abzurufen, der entweder nur auf einem oder verteilt auf verschiedenen Servern abgelegt wurde. Dieses Problem wird als „Password Authenticated Key Retrieval“ bezeichnet. Eine weitere Möglichkeit besteht darin, PAKEs gemeinsam mit Zertifikaten zu nutzen. Durch die Verwendung eines privaten asymmetrischen Schlüssels kann ein Kommunikationspartner neben dem Besitz des gemeinsamen Passworts ebenso den Besitz des privaten Schlüssels nachweisen, für den ein öffentlicher getauscht wird. So wird durch das PAKE eine Vertrauensbeziehung zum Zertifikat hergestellt.

Wie in diesen Beispielen sind die meisten PAKE-Protokolle für eine Kommunikation zwischen zwei Parteien gedacht. Dennoch existieren Vorschläge, wie auch Gruppen sich auf Basis eines Passworts auf einen gemeinsamen Schlüssel einigen können. Diese Verfahren werden Group PAKEs oder GPAKEs genannt. Neben eigens entwickelten Protokollen existieren auch generische Konstruktionen, die beliebige Zwei-Parteien-PAKEs in GPAKEs transformieren können. Eine weitere Idee ist die Verwendung einer vertrauenswürdigen dritten Partei, die mit jedem Teilnehmer ein Passwort teilt. So können mehrere Parteien einen gemeinsamen Schlüssel aushandeln, ohne untereinander im Vorfeld ein Geheimnis auszutauschen oder sich das Passwort, das sie mit dem Server teilen, gegenseitig verraten zu müssen.

Fazit

PAKE-Protokolle schlagen die Brücke zwischen einfach zu merkenden Passwörtern und sicheren kryptografischen Schlüsseln. Unterschiedlichste Designentscheidungen und Optimierungen liefern praxistaugliche Verfahren für vielerlei Anwendungen. Weitere Felder, in denen PAKEs in Zukunft Verbreitung finden könnten, sind das Internet der Dinge, um beispielsweise ein neues Gerät einfach in einen Pool bereits bestehender hinzuzufügen, ohne komplexe Netzwerkschlüssel einzugeben, und Industrie 4.0, etwa um mithilfe von aufgedruckten Passwörtern sichere Diagnoseverbindungen herzustellen.

Dr. Jörn-Marc Schmidt
Senior Consultant,
Division Homeland Security,
secunet Security Networks AG

Die Qubits kommen

Heute noch sichere Verschlüsselungsverfahren sind bald schon von gestern

Mit Hinblick auf die mögliche Entwicklung eines universellen Quantencomputers muss die gegenwärtig gängige Public-Key-Kryptografie möglichst bald durch Verfahren ersetzt oder ergänzt werden, die auch gegen Angriffe mit Quantencomputern resistent sind.

Seit in den 70er-Jahren Richard Feynman die Idee eines Computers präsentierte, der quantenmechanische Effekte wie Verschränkung und Superposition ausnutzt, stellt sich die Frage nach der Realisierbarkeit eines solchen Computers. Was vielen ehemals als vages Hirngespinst erschien, wird heute als durchaus möglich angesehen und ist vielleicht schon in wenigen Jahren Realität.

Unternehmen wie Google, IBM und Microsoft investieren große Summen in die Realisierung von Quantencomputern. Google hofft noch 2017 mit einem Quantensimulator ein Problem zu lösen, das mit herkömmlichen Rechnern nicht angreifbar ist und damit die „Quantum Supremacy“ nachzuweisen. Die EU startet gerade ein „Flagship Project“ zu „Quantum Technologies“, das neben Quantencomputern auch andere Anwendungen quantenmechanischer Effekte – die im „Quantum Manifesto“ beschrieben sind – im Blick hat.

Post-Quantum ante portas

Bei klassischen Computern treten zwar quantenphysikalische Effekte auf, werden aber nicht direkt ausgenutzt, um die Leistungsfähigkeit der Rechner zu erhöhen. Quantencomputer dagegen verwenden Superposition und Verschränkung von Zuständen direkt. Sie erlauben damit einen effizienten (polynomial-time, polynomial-space) Zugang zu Problemen, die mit den heute bekannten Methoden und herkömmlichen Computern nur mit exponentiellem Aufwand lösbar sind. Dazu gehören gerade auch diejenigen Probleme, auf denen die heute verwendete Public-Key-Kryptografie beruht. So könnten mit einem von Peter Shor 1994 veröffentlichten Algorithmus sowohl große Zahlen schnell faktorisiert als auch diskrete Logarithmen leicht berechnet werden. Damit wären Verfahren wie RSA und Diffie-Hellman-Schlüsselaustausch (in endlichen Körpern oder über elliptischen Kurven) unsicher. Symmetrische Algorithmen wie der AES könnten mit einem Algorithmus von Lov Grover (1996) zur Suche in unstrukturierten Datenbanken angegriffen werden. Als Faustregel müssen die Schlüssellängen symmetrischer Algorithmen verdoppelt werden, wenn man dasselbe Quantensicherheitsniveau wie zuvor das klassische Sicherheitsniveau erreichen möchte. Dies bedeutet, dass der AES-128 nicht als uneingeschränkt sicher gegen Quantenangriffe gelten kann.

Diese Situation hat dazu geführt, dass die NSA schon 2015 vor Quantencomputern gewarnt hat, und einen Wechsel zu quantensicheren kryptografischen Algorithmen (Post-Quantum-Kryptografie) eingeleitet hat. Für Informationen mit langer Lebensdauer ist dies auch notwendig, wenn man Schätzungen wie der von Michele Mosca, einem Mitbegründer des Institutes für Quantum Computing an der Universität Waterloo, vertraut: „I estimate a 1/7 chance of breaking RSA-2048 by 2026 and a 1/2 chance by 2031.“ Man könnte nämlich bereits heute Kommunikationen aufzeichnen, die mit Public-Key-Verfahren gesichert sind und sie dann in einigen Jahren entschlüsseln.

Krypto-Agilität

Was aber dringend benötigt wird, sind quantencomputerresistente Signaturverfahren für Software-Updates. Das BSI empfiehlt grundsätzlich kryptografische Produkte so zu gestalten, dass Krypto-Agilität erreicht wird. Dies bedeutet, dass veraltete Verfahren oder Parameter leicht durch neue ersetzt werden können. Die dafür nötigen Updates müssen authentisiert und entsprechend muss ein geeigneter Mechanismus schon heute in Produkte integriert werden. Dafür verwendet man in der Regel Signaturverfahren.

Es gibt bislang noch keine ausgereifte Möglichkeit eine beliebige Anzahl von Datensätzen quantencomputerresistent zu signieren. Bei einer vorab festgelegten Höchstzahl von Signaturen hingegen gelten die hashbasierten Merkle-Signaturen als geeignetes Verfahren. Diese verwenden Einmal-Signaturen und Hashbäume, mit denen die Signaturschlüssel verwaltet werden. Verschiedene Varianten (LMS, XMSS) befinden sich zurzeit in der Standardisierung durch die IETF. Wesentlicher Nachteil ist ihre Zustandsbehaftung: Der Signierer muss fehlerfrei kontrollieren, welche Einmal-Signaturschlüssel schon verbraucht sind, um die Sicherheit des Systems zu garantieren.

Dies macht Merkle-Signaturen ungeeignet für den Ersatz von Signaturverfahren wie dem ECDSA. Für quantensichere Updates von kryptografischen Mechanismen sind sie aber gut geeignet, da hierfür nur eine geringe Zahl von Signaturen erforderlich ist. Der Einsatz von Merkle-Signaturen wird schon heute vom BSI empfohlen – beispielsweise in den Technischen Richtlinien TR-02102 und TR-03140. Als zustandslose Variante wurde das Signaturverfahren SPHINCS entwickelt, welches jedoch starke Effizienznachteile gegenüber den zustandsbehafteten Verfahren zeigt.

Alice und Bob im Quantenland

Zur Schlüsseleinigung gibt es einige Kandidaten, die derzeit intensiv diskutiert werden. Diese basieren auf der Schwierigkeit, allgemeine fehlerkorrigierende Codes effizient zu dekodieren („codebasierte Verfahren“, z. B. McEliece mit binären Goppa-Codes), multivariate Gleichungssysteme zu lösen („multivariate Verfahren“), Isogenien zwischen elliptischen Kurven zu berechnen („isogeniebasierte Verfahren“) oder auf der Schwierigkeit von bestimmten Problemen in mathematischen Gittern („gitterbasierte Verfahren“). Von den genannten Kandidaten existieren die codebasierten Verfahren am längsten und sind am besten verstanden, in der aktuellen Diskussion stehen jedoch die gitterbasierten Verfahren im Vordergrund (siehe Kasten).

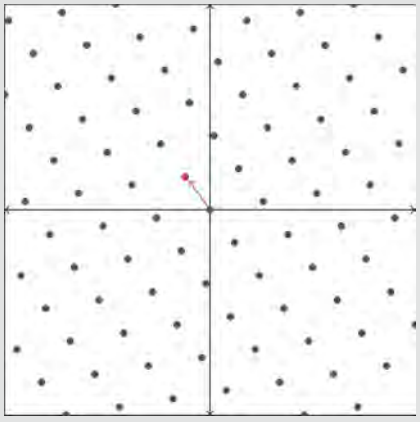
Standardisierungsorganisationen wie NIST, ETSI oder IETF haben mit der Standardisierung von quantensicheren Algorithmen und deren Einbettung in Protokolle begonnen. Ergebnisse sind allerdings erst in

GITTERBASIERTE KRYPTOGRAFISCHE VERFAHREN – A NEW HOPE?

In der Mathematik bezeichnet ein Gitter „eine diskrete Untergruppe eines n-dimensionalen reellen Vektorraums“. Grob gesagt bedeutet das, dass die Summe zweier Gitterpunkte wieder im Gitter liegt und es in einer „kleinen“ Umgebung um einen Gitterpunkt keinen weiteren Gitterpunkt gibt. Im zweidimensionalen Beispiel unten wird klar, warum ein solches Konstrukt als Gitter bezeichnet wird.

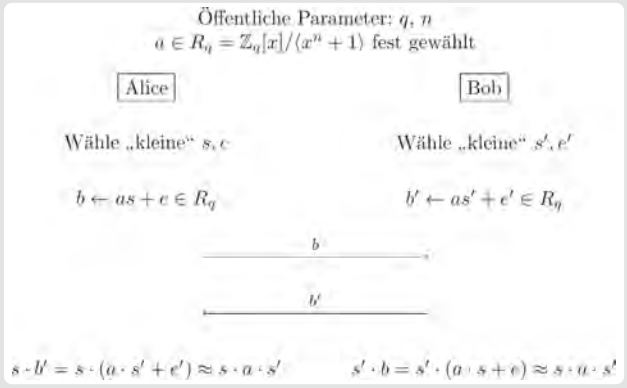
In einem Gitter lassen sich viele Probleme formulieren, die schwer zu lösen sind. Ein Beispiel ist das Finden eines kürzesten Vektors. Im zweidimensionalen Beispiel ist diese Aufgabe offensichtlich durch bloßes Hinschauen zu lösen (roter Pfeil). Der Rechenaufwand wächst aber exponentiell mit der Dimension des Gitters. Gitterbasierte kryptografische Verfahren beruhen nicht direkt auf solchen Gitterproblemen, sondern auf Problemen, die sich auf diese reduzieren lassen – z. B. auf dem LWE-Problem („Learning with Errors“). Dies lässt sich grob zusammenfassen als die Schwierigkeit, ein lineares Gleichungssystem, das mit einem „kleinen“ Fehler gestört wurde, zu lösen.

Eine LWE-Instanz ist somit gegeben durch eine Matrix und einen Vektor. Auch hier muss die Dimension ausreichend groß sein, damit sich das Gleichungssystem nicht „durch bloßes Hinschauen“ lösen lässt. Eine entsprechende Matrix ist dann leicht mehrere Kilobytes groß. Daher wird in vielen gitterbasierten kryptografischen Verfahren hierfür eine zyklische Matrix verwendet. Dann reicht es, nur die erste Zeile der Matrix zu speichern bzw. zu übertragen, alle anderen Zeilen lassen sich aus ihr berechnen. Das zugrunde liegende Problem wird Ring-LWE genannt.



Quelle: BSI

Zweidimensionale Darstellung eines Gitters



Quelle: BSI

New-Hope-Ansatz

Ein Beispiel ist das Schlüsseleinigungsverfahren „New Hope“, das testweise in Googles Browser Chrome eingebaut wurde. Es beruht auf einer Reihe von Arbeiten verschiedener Forscher. Die Idee dahinter ist, den bekannten Diffie-Hellman-Schlüsselaustausch, der zurzeit etwa unter Verwendung von elliptischen Kurven implementiert wird, in eine Post-Quantum-Welt zu retten.

Der erste wesentliche Unterschied zum klassischen Diffie-Hellman-Verfahren ist, dass Alice und Bob zunächst nur „ungefähr“ den gleichen Schlüssel erhalten. Es ist noch ein Mechanismus („Reconciliation“, oben nicht dargestellt) nötig, um ein gemeinsames Geheimnis zu errechnen. Dadurch ergibt sich der zweite große Unterschied: Das Verfahren ist nicht mehr symmetrisch, d. h. der Schlüssel hängt davon ab, welcher der beiden Kommunikationspartner der Initiator ist.

New Hope stützt seine Sicherheit auf das Ring-LWE-Problem, lässt sich aber auch als Variante formulieren, die auf LWE basiert („Frodo: Take off the ring!“). Generell ist bei der gitterbasierten Kryptografie abzuwägen zwischen Verfahren, die auf Problemen in Standard-Gittern (wie LWE) beruhen und eine höhere Sicherheit bieten, und Verfahren, die auf Problemen in Ideal-Gittern (wie Ring-LWE) beruhen und eine höhere Effizienz haben.

einigen Jahren zu erwarten. Dank der zunehmenden Forschung zu quantencomputerresistenten Algorithmen kann es durchaus noch zu unvorhersehbaren Fortschritten in der Analyse der derzeitigen Kandidaten kommen. Daher mag es verfrüht sein, sich jetzt schon auf einen Kandidaten oder auf Parameterlängen festzulegen. Auch Methoden zur Schlüsselvereinbarung, die auf physikalischen Prinzipien beruhen (QKD) bieten Alternativen. Jedoch sind in diesem Bereich noch viele Probleme zu lösen. Dazu gehört die Entwicklung von Quanten-Repeatern genauso wie die sichere Implementierung der Verfahren und die gegenseitige Authentisierung der Kommunikationspartner.

Fazit

Derzeit befinden wir uns in der Situation, dass wir den hergebrachten Verfahren zur Schlüsseleinigung nicht langfristig vertrauen können, andererseits aber noch kein standardisierter und langjährig untersuchter Ersatz zur Verfügung steht, der gleichzeitig einfach zu implementieren und effizient ist. Daher strebt das BSI hybride Lösungen an, die eine traditionelle Schlüsseleinigung mit einer als quantensicher vermuteten Schlüsseleinigung koppeln. Als Übergangslösung können zudem bereits heute verfügbare Ad-hoc-Lösungen genutzt werden, die Angriffe mit Quantencomputern erschweren. Dazu zählt etwa die Verwendung von zusätzlichen symmetrischen Schlüsseln, um die Public-Key-Schlüsseleinigung zu schützen, oder die Verwendung von privaten elliptischen Kurven. Solche Lösungen sind natürlich nur in einem Umfeld möglich, in dem die zusätzlichen Geheimnisse zuverlässig geschützt werden können.

Dr. Heike Hagemeier und Dr. Manfred Lochter
Bundesamt für Sicherheit in der Informationstechnik (BSI), Referat KT13

Security im Auto der Zukunft

Vernetzte Fahrzeuge müssen vor Datenmissbrauch und Cyberangriffen geschützt werden

Zunehmend entwickeln sich Fahrzeuge zu potenziell angreifbaren Komponenten im weltumspannenden IoT. Deshalb muss die zuverlässige Abwehr von Cyberangriffen ebenso wie der Schutz der Daten des Fahrzeugnutzers durch eine einheitliche Sicherheitsarchitektur rechtlich und technisch gewährleistet werden.

Seit über 100 Jahren ist die Straßenverkehrssicherheit und seit über zwei Jahrzehnten auch der Umweltschutz Antreiber für mehr Innovation, Investition, Wachstum und Beschäftigung im Automobilbau. Die stärksten Innovationsmotoren für mehr Sicherheit im Straßenverkehr und effiziente Nutzung der Verkehrsmittel sind heute die Vernetzung der Fahrzeuge mit dem Internet sowie die modernen Informationstechnologien. Big Data ist der Rohstoff dieser digitalen Revolution im Automobilbau, der das traditionelle Verständnis vom Auto als klassisches Transportmittel grundlegend ändert: Individuelle Infotainmentangebote für den Fahrzeugnutzer, hochentwickelte Fahrerassistenzsysteme bis hin zu autonomen Chauffeurdiensten und cloudbasierte Funktionalitäten im Fahrzeug bestimmen zukünftig die Kaufentscheidung.

Moderne Automobile kommunizieren mit der Infrastruktur und anderen Fahrzeugen (V2X Communications), verfügen über digitale Telematikschnittstellen zu Serviceanbietern (eCall etc.), fahrzeugseitige Vernetzungsschnittstellen (In-Vehicle Networking), drahtlose Technologien für den Fahrzeugzugriff (Dongles auf dem OBD-Port) und kabellose Nahbereichskommunikation (Smartphones via NFC und Bluetooth). Hierbei ergeben sich neue Herausforderungen sowohl für die Sicherheit der Fahrzeuge und ihrer Netzwerke gegen Hackerangriffe und Virenbefall als auch für den Datenschutz, da alle Daten, die in einem Fahrzeug anfallen, als personenbezogen gelten, sobald sie mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen verknüpft sind (vgl. § 3 Abs. 1 BDSG).

Bedrohungsszenarien

Digital vernetzte Fahrzeuge sind schon heute ebenso Realität wie gefährliche Angriffe von Cyberkriminellen. Die Bandbreite der Cyberattacken auf Connected Cars ist vielfältig und komplex. Sie reicht von relativ einfachen Angriffen wie dem Einschleusen von Schadnachrichten bis hin zum Einbruch in elektronische Steuergeräte des Fahrzeugs, um Fahrzeugsoftware und Mikrocontroller zu manipulieren. In allen Fällen wird das Vertrauen auf Seiten der Nutzer in die neue Technologie, trotz ihrer Komfortvorteile und Safety-Features, nachhaltig geschädigt.

So erlangte unlängst in der Automobilbranche das Bekanntwerden eines Cyberangriffs auf einen Jeep Cherokee große Aufmerksamkeit. Sicherheitsingenieure in den USA übernahmen ohne physischen Zugang unautorisiert Kontrolle über den fahrenden SUV, nachdem sie zuvor mittels Reverse Engineering über den OBD-II-Port die Schwachstellen im elektronischen Fahrzeugsystem ausspioniert hatten. Wahrscheinlich fanden die Hacker eine Lücke im Infotainmentsystem des Fahrzeuges, in dem auch GSM- und WLAN-Funktionen sitzen. In einem zweiten Schritt gelang es ihnen offenbar, das systeminterne Motorsteuer-Gateway zu durchbrechen und einen Trägervirus in das Fahrzeug einzuschleusen. Dieser Virus gaukelt dem Fahrzeugsystem vor, dass alles in Ordnung sei, während Angreifer unautorisiert die Steuerung über das Fahrzeug übernehmen. Fiat Chrysler reagierte entsprechend mit dem Rückruf von weltweit 1,4 Mio. betroffenen Fahrzeugen.

Gefährliche Manipulationen

Die Nutzung falscher bzw. gestohlener Identitäten zur illegalen Beschaffung von Fahrzeugen steht bei Kriminellen hoch im Kurs. Typische Sicherheitsschwachstellen befinden sich heute beispielsweise in Keyless-Go-Systemen, bei denen Scannerboxen Daten vom elektronischen Originalfahrzeugschlüssel abgreifen. Diebe verschaffen sich so recht einfach Zugang zum Fahrzeug und der Motorzündung. Angreifer können autonome Bremsassistenzsysteme der Fahrzeuge durch gefälschte V2X-Nachrichten an das CAN-BUS-System aktivieren oder die sicherheitsrelevante Kommunikation innerhalb des Fahrzeugs manipulieren.

Durch das sogenannte Flooding können einzelne CAN-BUS-Systeme, die simple Funktionen des Fahrzeugs wie den Scheibenwischer ansteuern, überlastet werden. Wenn dann bei Regen und Tempo 120 der Scheibenwischer nicht mehr funktioniert, kann das fatale Auswirkungen auf die Fahrzeuginsassen haben (klassische Denial-of-Service-Attacke). Security wird damit zur Voraussetzung für die Sicherheit (Safety) von Menschenleben.

Bei dem ab 2018 gesetzlich vorgeschriebenen eCall-System, mit dem zügig Hilfe bei einem Unfall geordert werden kann, zeichnen sich schon jetzt Datenschutzprobleme ab. Hier gilt es zu verhindern, dass Dritte unautorisierten Zugang auf persönliche Daten durch gefälschte Zertifikate erlangen. Die gleiche Anforderung an den Datenschutz besteht auch bei sogenannten Pay-as-you-drive-Versicherungstarifen. Relevante Daten für die Berechnung der monatlichen Versicherungsprämien sollten nur dem Versicherungsanbieter zur Verfügung stehen, nicht unautorisierten Dritten, die Daten über die Nutzungsgewohnheiten des Fahrzeughalters illegal abfangen.

Schon diese kleine Auswahl an Bedrohungsszenarien beweist, dass Security und Privacy zukünftig integraler Bestandteil der Fahrzeugkonstruktion (Security- bzw. Privacy-by-design) werden müssen und über den gesamten Lebenszyklus des Fahrzeugs entsprechend des aktuellen Stands der Technik gesichert werden sollten. Die dazu notwendige Sicherheitsarchitektur muss so angelegt sein, dass sie sich jederzeit auch an neue Gefährdungen anpassen lässt.

Anforderungsprofile

Zwar erfüllt die heutige Fahrzeugkonstruktion höchste Ansprüche an die funktionale Sicherheit (ABS, ESP, ACSF etc.) und den Schutz der physischen Kommunikationseinheit (OBD-II-Port). Im Gegensatz dazu steht jedoch eine eher schwache IT-Security-Absicherung des Fahr-

zeugs. Potenzielle Sicherheitsbedrohungen sind äußert volatil und nicht vorhersehbar – und daher auch nicht in einem eher deterministisch geprägten und risikobasierten Standardisierungsrahmen der funktionalen Sicherheit wie beim ISO-Standard 26262 abbildbar. Nach wie vor sind solche Bedrohungen weitgehend Neuland für die Automobilindustrie.

Security genießt bei den Fahrzeugherstellern heute nicht den gleichen Stellenwert wie die Umsetzung eines neuen cloudbasierten Geschäftsmodells im vernetzten Fahrzeug. Häufig erarbeiten die OEMs eigene IT-Security-Systeme, die nicht unbedingt interoperabel sind, Interdependenzen zur funktionalen Sicherheit des Fahrzeugs und zu Funktionalitäten in der Cloud bzw. im Backend-Server nicht berücksichtigen und daher nur unzureichend vor Missbrauch, Manipulation und Datendiebstahl schützen. Bereits standardisierte, generische Security-Rahmenwerke, wie etwa die Common-Criteria-Anforderungen in anderen Industriesektoren, könnten hier analog für fahrzeugspezifische Anforderungen zur Anwendung kommen.

Als eine der weltweit ersten Nationen diskutieren die Vereinigten Staaten seit Ende März 2017 angesichts der zunehmenden Bedrohungen einen Gesetzesvorschlag der Senatoren Edward Markey (D-MA) und Richard Blumenthal (D-CT). Danach sollen die Automobilhersteller zukünftig verpflichtet werden, in digital vernetzten Fahrzeugen Cybersecurity- und Datenschutzstandards zu etablieren und ein entsprechendes Bewertungssystem einzuführen. Einheitliche und verbindliche Vorgaben und Normen zur zukünftigen Gestaltung des Datenaustausches über die Drahtlosschnittstellen des Fahrzeuges und die Implementierung eines gemeinsamen IT-Security-Standards können tatsächlich helfen, bestehende Lücken zu reduzieren. Dazu bedarf es allerdings einer Sicherheitsarchitektur im vernetzten Fahrzeug, die den Schutz vor Cyberangriffen erhöht, den Datenschutz verbessert, und letztlich auch gleiche Wettbewerbsbedingungen für alle Marktteilnehmer cloudbasierter Servicedienstleistungen schafft.

Die IT-Security-Architektur des Fahrzeugs muss bereits bei der Fahrzeugtypgenehmigung entsprechend international verankerter Standards geprüft und nach dem jeweiligen Stand der Technik über den gesamten Lebenszyklus auf aktuellem Niveau gehalten werden. Hierfür sind Penetrationstests und Zertifizierungen als Voraussetzung für die Typgenehmigung anzuwenden. Cloudbasierte Servicedienstleister im Fahrzeug sollten ebenfalls mittels qualifizierter und unabhängiger Audits und Zertifizierungen ihre Datenschutzanstrengungen und die Vertrauenswürdigkeit ihrer Dienstleistungen nachweisen. Zudem bedarf es Sicherheitsmaßnahmen für die Zeit nach dem Verkauf des Fahrzeugs (Operational Time) im Rahmen der periodischen technischen Überwachung, die nicht durch die Typzulassung abgedeckt sind.

Wie kommt Security ins Fahrzeug?

Zukünftig könnte eine hochsichere und in allen Fahrzeugen einheitlich verbaute Kommunikationsplattform (Automotive Platform) implementiert werden, um den Anforderungen an Datenschutz und Security neuer Technologien und Geschäftsmodelle gerecht zu werden. Diese technische Konzeption soll Vertrauenswürdigkeit und beweisbare Sicherheit für alle am Connected Car beteiligten Akteure generieren. Die Plattform als zentrale Sicherheitsarchitektur im Fahrzeug verbindet alle elektrischen Steuergeräte (ECUs) der verschiedenen Fahrzeugdomänen. Zu diesen Steuergeräten zählen der Antriebsstrang, Brems- und Fahrerassistenzsysteme, Infotainmentangebote oder auch die Fahrwerk- und Komfortelektronik. Zudem ist die Plattform der zentrale Zugang, um Software-Updates, Diagnose- und Wartungsaufgaben via On-Board-Diagnose (OBD) und/oder Telematikschnittstelle (TCU) durchzuführen.

Gleichzeitig nimmt die Plattform eine sichere Separierung zwischen Servicediensten (externe Telematikschnittstellen des Fahrzeuges) von den für den Fahrer relevanten Informationssystemen (Comfort Domain) und zusätzlich von den Safety-relevanten Komponenten (Safety Domain) vor. Informationen, die das Fahrzeug verlassen, werden hierbei vorab von der zentralen Plattform nach bestimmten Nutzungsprofilen aufbereitet. Gleiches gilt für Informationsflüsse in das und innerhalb des Fahrzeugs, etwa bei Over-the-Air-Updates für elektronische Steuergeräte. Diese Kommunikationsplattform würde somit einen einheitlich-zentralen und interoperablen Sicherheitsstandard bezüglich Security und Safety im Fahrzeug schaffen, der u. a. folgende Security-Funktionalitäten (Security by Design) vorsieht: Informationsflusskontrolle (Firewall) – Fahrzeug-Domain-Separierung – sichere M2M-Identifizierung/-Authentisierung – Zugangskontrolle zu Fahrzeugschnittstellen und Einbruchserkennung (IDS) – Auditierung – Zufallsgenerator – Verschlüsselung (Kryptoverfahren zur Signierung).

Für diese Security-Funktionalitäten sollte ein Secure Element an der Kommunikationsplattform verwendet werden. Solche Mikrocontroller verfügen über hoch entwickelte Verschlüsselungsfunktionen sowie geprüfte physische und elektrische Widerstandsfähigkeit, wie sie auch im elektronischen Reisepass, in Geldkarten und in Smartphones Verwendung finden. Secure Elements etablieren eine sichere Ende-zu-Ende-Datenübertragung im Internet über ein hybrides Verschlüsselungsprotokoll. Zudem können sie auch als Tresor für notwendige Sicherheitsschlüssel und Zertifikate sowohl für die ECUs im Fahrzeug als auch für externe Kommunikationspartner, wie etwa Ampeln oder Drittanbieter, dienen.

Wie kommt Privacy ins Fahrzeug?

Digitale Steuergeräte und Sensoren generieren – oftmals intransparent für den Fahrzeughalter – selbsttätig große Mengen an Daten und Informationen zur aktuellen Position und Umgebung, zur Fahrweise, aber auch direkt zum Zustand der Fahrenden. So wird beispielsweise die Atemluft kontrolliert, Herz- und Pupillenschlag überwacht oder der psychische Zustand per Sprachanalyse verfolgt. Die erreichte Maximaldrehzahl des Motors mit dem jeweiligen Kilometerstand erlaubt Rückschlüsse auf den Fahrstil – genauso wie die Zahl der elektromotorischen Gurtstraffungen, etwa aufgrund starken Bremsens. Die Häufigkeit der Einstellvorgänge des elektrischen Fahrersitzes wiederum gibt Hinweise auf mehrfache Fahrerwechsel.

Die Herausforderung liegt also darin, entsprechend den Datenschutzbestimmungen die Verbraucher angemessen zu informieren, sodass diese in der Lage sind, den Datenfluss nachvollziehen zu können bzw. eine bewusste Entscheidung darüber zu treffen, welche Daten sie wann, zu welchem Zweck und zu welchen Bedingungen für welches Unternehmen zur Nutzung bzw. Verarbeitung zugänglich machen möchten. Der einzelne Fahrzeugnutzer darf nicht zum reinen Objekt der Technik werden, sondern sollte die Souveränität über seine Daten behalten. Die zukünftige Datenverarbeitung im Fahrzeug muss also bereits bei Konstruktion und Herstellung die Grundsätze Privacy-by-Design und Privacy-by-Default berücksichtigen. So sollten personenbezogene Daten prinzipiell im Auto selbst verbleiben und nur anonymisiert oder pseudonymisiert in einem externen Server der Hersteller oder Dienstanbieter verarbeitet werden.

Die Automotive Platform bereitet vorausschauend die zu kommunizierenden Informationen gemäß vorab definierter Fahrzeugprofile und Datenkategorien auf und versendet sie signiert und verschlüsselt über eine Telematikschnittstelle an unterschiedliche Serviceanbieter (OEMs, Zulieferer, Versicherung, Halter, Flottenmanagement, Notdienst, Smart

City Services, Parkhäuser, Warndienste, Prüfinstitute etc.). Diese Profile können im Betrieb durch einen Administrator geändert werden, der aber selbst weder Schreib- noch Lesezugriff auf die Fahrzeugdaten hat. Hierbei wird ein Privacy-by-Design-Ansatz verfolgt: Nur Daten, die im Sinne des Datenschutzgesetzes zu einem bestimmten Zweck abgerufen werden dürfen, werden auch versendet. Im Auslieferungszustand des Fahrzeuges ist die Plattform in der höchsten Datenschutzstufe konfiguriert (Privacy-by-Default). Falls der Nutzer bzw. Halter des Fahrzeugs zustimmt, können personenbezogene Daten für weitere Verwendungszwecke übermittelt werden; dies wird dann in den Nutzerprofilen abgebildet. Ein vertrauenswürdiger Zugriff auf die Fahrzeugdaten für Servicedienstleister im Automotive-Sektor muss somit weder aus Security- noch aus Privacy-Gesichtspunkten über die IT-Zentralen der Hersteller (Backend-Server) erfolgen, sondern kann unmittelbar vom Fahrzeug direkt übernommen werden.

Durch die Möglichkeit des Monitoring sicherheits- und emissionsrelevanter Systeme und einen sicheren, vorab geprüften und autorisierten OTA-Software-Update-Prozess elektronischer Steuergeräte im Fahrzeug lässt sich mit der Automotive Platform überdies die Verkehrssicherheit erhöhen. Bereits von der Automobilindustrie definierte Kommunikationsprotokolle und Dienste werden weiterhin berücksichtigt und genutzt, sofern sie nicht im Widerspruch zu dieser Security/Privacy-Architektur stehen. Eine europäische Gesetzesinitiative könnte strenge Datenschutzbestimmungen durchsetzen und durch einheitliche Standards die Kompatibilität vernetzter Fahrzeuge im europäischen Binnenmarkt voranbringen. Entsprechende Serviceanbieter erhalten somit die Möglichkeit, unter gleichen Bedingungen wie die Automobilindustrie intelligente datenbasierte Geschäftsmodelle für die Fahrzeugnutzer anzubieten. Die Automotive Platform schafft damit auch einen transparenten Wettbewerb, in dem die Verbraucher die Wahl zwischen mehreren Anbietern haben und bequem wechseln können.

Mit dem Einzug des Internet of Things (IoT) in den Fahrzeugbau befindet sich die Automobilbranche mitten in einer technologischen Revolution. Mobilitätsdienste und Funktionalitäten auf Grundlage von Big Data in der Cloud werden weiter zunehmen. Das Automobil als IoT-Produkt macht den Schutz gegen Cyberangriffe von außen notwendig. Die Kunden cloudbasierter Dienstleistungen müssen ganz bewusst entscheiden können, welche Daten sie preisgeben und was damit passiert. Es muss ihnen möglich sein, die Datenübermittlung zu erkennen, zu kontrollieren und ggf. auch zu stoppen. Entscheidend bleibt, dass der Nutzer am Ende selbst die Wahl hat, wie er mit seinen Daten umgehen möchte.

Fazit

Die Automotive Platform schafft hierfür einen einheitlich-zentralen und interoperablen Standard bezüglich IT-Security und funktionaler Sicherheit im Fahrzeug, schützt das Fahrzeug vor unbefugten Zugriffen von außen und kann die datenschutzrechtlichen Anforderungen abbilden. Durch ein hochsicheres Secure Element in der Plattform ist dieser Technologieansatz gegen Manipulationen gesichert. Die vertrauenswürdige Verwaltung der Daten setzt Maßstäbe für einen möglichst großen und wettbewerbsoffenen Mobility-Markt, der alle Dienstleister und Drittanbieter in eine gleichwertige, faire, angemessene und diskriminierungsfreie Position versetzt, den jeweiligen Dateneignern ihre digitalen Dienste im Fahrzeug anzubieten. So kann sowohl eine hohe Innovationskraft als auch wirksamer Verbraucherschutz in den Bereichen Automotive und Mobility gewährleistet werden.

Markus Bartsch
Business Development IT Security, TÜV Informationstechnik GmbH
Richard Goebelt
Director Automotive and Mobility, Verband der TÜV e.V.

Impressum
Themenbeilage Sicherheit & Datenschutz

Redaktion just 4 business GmbH
Telefon: 08061 34811100, Fax: 08061 34811109,
E-Mail: tj@just4business.de

Verantwortliche Redakteure:
Thomas Jannot (v.i.S.d.P.), Ralph Novak, Martin Fuhrmann (Redaktion), Rudolph Schuster (Lektorat)

Autoren dieser Ausgabe:
Markus Bartsch, Jochen Brüggemann, Mareike Gehrmann, Richard Goebelt, Dr. Heike Hagemeier, Dr. André Kudra, Dr. Manfred Lochter, Dr. Holger Mühlbauer, Dr. Jörn-Marc Schmidt, Alexander Wilms

DTP-Produktion:
Enrico Eisert, Matthias Timm, Hinstorff Media, Rostock

Korrektorat:
Ninett Wagner, Hinstorff Media, Rostock

Titelbild:
© shutterstock, Sentavio

Verlag
Heise Medien GmbH & Co. KG,
Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover;
Telefon: 0511 5352-0, Telefax: 0511 5352-129

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Mitglieder der Geschäftsleitung:
Beate Gerold, Jörg Mühle

Verlagsleiter:
Dr. Alfons Schräder

Anzeigenleitung (verantwortlich für den Anzeigenteil):
Michael Hanke (-167), E-Mail: michael.hanke@heise.de, www.heise.de/mediadaten/ix

Leiter Vetrieb und Marketing:
André Lux

Druck:
Dierichs Druck + Media GmbH & Co. KG, Frankfurter Straße 168, 34121 Kassel

Die Inserenten

NO ROCKET SCIENCE

Jetzt für 12,90 € bestellen!

shop.heise.de/ix-cloud16 service@shop.heise.de
Auch als eMagazin erhältlich unter: shop.heise.de/ix-cloud16-pdf

heise shop
shop.heise.de

Generell **portofreie Lieferung** für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 15 €

NEUHEIT

ID.logon
Smart Authentication

MADA ID.logon Smart Authentication:
Noch einfacher und sicherer kann eine Windows-Anmeldung nicht sein!

RFID-basierter Windows-Login:
Schnelle und einfache Windows-Anmeldung für alle gängigen **125 kHz** und **13,56 MHz** RFID-Transponder

- RFID-Medium als Logon-Key
  Die sichere Windows-Anmeldung
- Keine neuen RFID-Medien nötig
  Nutzen Sie Ihre Bestandsausweise
- Zentrale Schlüssel- & Userverwaltung
  Sichern Sie Ihr gesamtes Netzwerk
- 2-Faktor Authentifizierung mit PIN
  Identitätsnachweis nach Maß: PIN Code Eingabe + RFID

MADA Marx Datentechnik GmbH
Hinterhofen 4 – 78052 Villingen-Schwenningen
www.id-logon.de – info@id-logon.de

ID.logon sichert schnell und einfach den Zugang zu:
- Personal Computern mit Windows 7, 8 & 10
- Windows Server: Windows 2003, 2008, 2012. Active Directory
- Novell e-Directory: Voll kompatibel mit Novell Client 4.81 (oder höher)
- Windows Remote Desktop