Eine Themenbeilage der
Heise Medien GmbH & Co. KG

II
2019

SICHERHEIT & DATENSCHUTZ

Industrial Security, E-Government und Zugriffskontrolle

Security Management:
Wie sich Synergieeffekte nutzen lassen

Cloud Security:
Was E-Government vor Cyberangriffen schützt

E-Signatur:
Wer digitale Unterschriften verifiziert

BEG III:
Was vom Bürokratie-entlastungsgesetz zu halten ist

Industrial Security:
Wie ein optimales Sicherheitsdesign aussieht

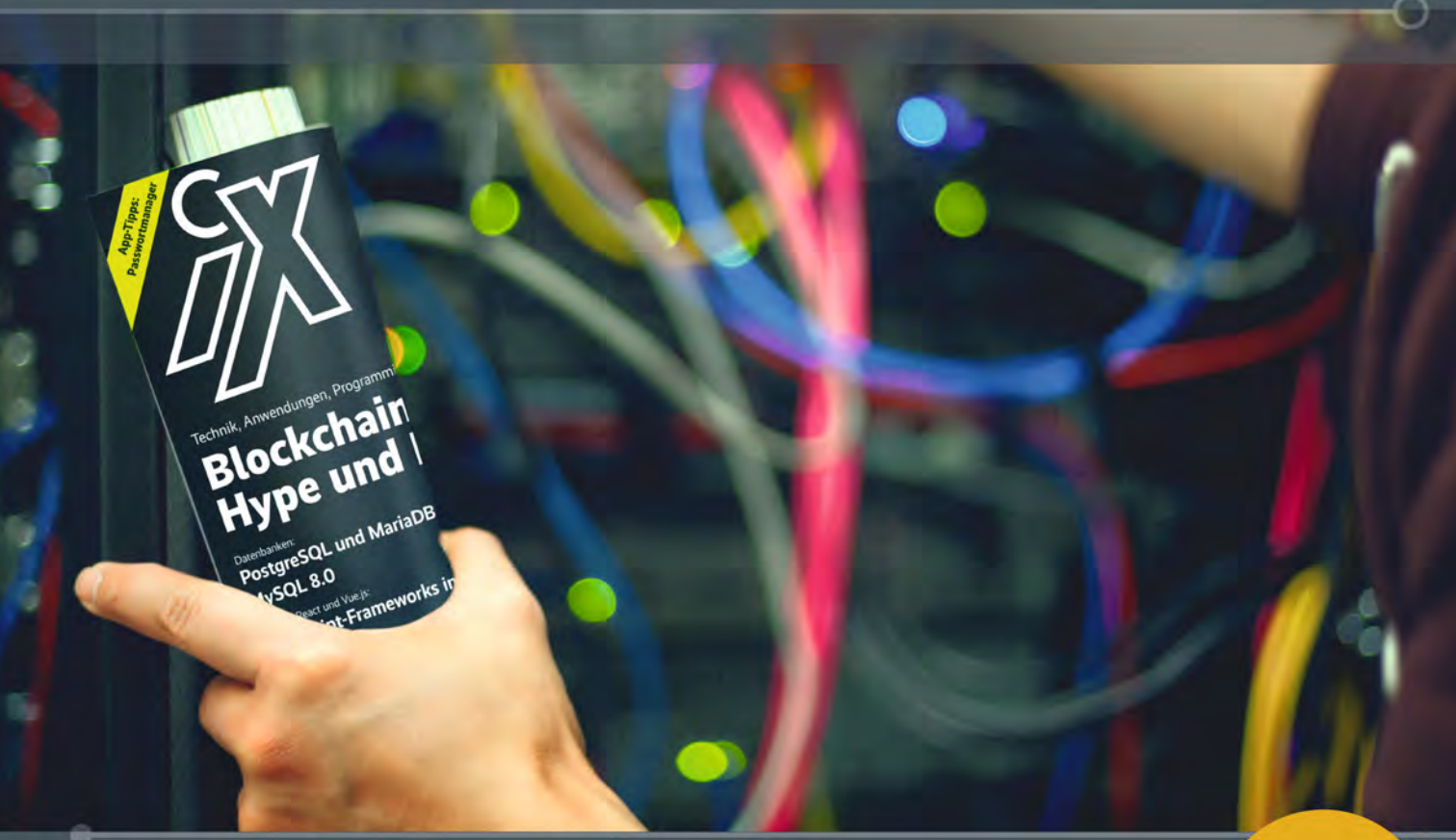
Sealed Computing:
Warum Admins draußen bleiben müssen

www.it-security-und-management.de

powered by: TeleTrusT Pioneers in IT security. iX

Es gibt 10 Arten von Menschen.

iX-Leser und die anderen.



Jetzt Mini-Abo testen:
3 Hefte + Leiterplatten-Untersetzer
nur 16,50 €

www.iX.de/testen

www.iX.de/testen 49 (0)541 800 09 120 leserservice@heise.de

iX MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

IT-Sicherheit in unsicheren Zeiten

Liebe Leserinnen und Leser,

die EU muss ein gesamteuropäisches Vorgehen im Kampf gegen Cybergefahren sicherstellen, nationale Alleingänge vermeiden und auch die Bürgerinnen und Bürger einbinden.

Mit der zunehmenden Vernetzung und Digitalisierung verändern sich die Bedrohungen für Bürgerinnen und Bürger, Unternehmen und Staaten.

Die Angriffe werden verteilter, raffinierter und professioneller und richten Milliardenschäden an. Die IT-Kriminalität erfährt eine zunehmende Industrialisierung und damit eine nicht zu unterschätzende und nie dagewesene Professionalisierung.

Dieser Gefahr und den sich daraus entwickelnden Herausforderungen müssen nicht nur die Mitgliedstaaten gerecht werden; auch die EU steht hier in einer besonderen Verantwortung.

Die aktuelle IT-Sicherheitssituation ist für eine moderne Informations- und Wissensgesellschaft wie Deutschland nicht angemessen sicher und vertrauenswürdig genug.

Im Dialog mit allen Verantwortlichen sollten deshalb Lösungsansätze zur Verbesserung aufzeigt werden. Dabei müssen die Kompetenzen der Akteure bestmöglich gebündelt werden. Hierfür hat TeleTrusT ein umfangreiches Konzeptpapier erstellt und zeigt darin die Stärken der IT-Sicherheitsbranche in Deutschland auf.

Diese Sonderpublikation informiert Sie über generelle Lösungsvorschläge, die von deutschen IT-Sicherheitsunternehmen im Bereich der IT-Sicherheit entwickelt worden sind. Ebenso wird die 5G-Diskussion thematisiert, die weit über Deutschland hinaus eine große Rolle spielt.

Im Namen des Bundesverbandes IT-Sicherheit wünsche ich Ihnen eine spannende und informative Lektüre und eine besinnliche, sichere Weihnachtszeit.

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

Inhalt

Orientierungshilfe im Regulierungsdschungel

Zur Bewältigung regulatorischer Anforderungen lassen sich Synergieeffekte nutzen

Weil Anzahl und Umfang von IT-Sicherheitsvorgaben kontinuierlich ansteigen, verliert so manches Unternehmen schnell den Überblick im Dickicht der Verordnungen. Doch anstatt die Kompetenzen auf einzelne Fachabteilungen zu verteilen, sollte das Security Management einen integrativen Ansatz verfolgen.

In den letzten Jahren steigerte sich die Frequenz bei der Einführung neuer regulatorischer Anforderungen an die IT-Sicherheit und den Datenschutz mehr als in all den Jahren zuvor. Neben einer omnipräsenten Datenschutz-Grundverordnung (DSGVO), die dem Datenschutz in der gesamten EU eine höhere Relevanz verschafft, müssen Unternehmen sich auch immer intensiver mit dem Thema IT-Sicherheit beziehungsweise dem umfassenderen Bereich Informationssicherheit auseinandersetzen. Es gilt, eine ganze Reihe von Vorgaben zu beachten, so etwa das IT-Sicherheitsgesetz für KRITIS (Kritische Infrastrukturen), die Notwendigkeit der Implementierung von technischen und organisatorischen Maßnahmen (TOMs) – eben aufgrund der Datenschutz-Grundverordnung – oder Auflagen zum Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen durch das neue Geschäftsgeheimnisschutzgesetz (GeschGehG) diesen Jahres.

Dabei werden Verpflichtung und Vereinheitlichung von IT-Sicherheitsstandards nicht nur in Deutschland forciert. Auch die EU hat nicht zuletzt durch die NIS-Richtlinie einen Markstein gesetzt. Nun ist jeder Mitgliedsstaat verpflichtet, entsprechende nationale Gesetzgebungen durchzusetzen, die dem IT-Sicherheitsgesetz in Deutschland ähneln bzw. sehr ähnlich sein werden. Auch das Thema der einheitlichen Zertifizierungen im Bereich IT-Sicherheit wird durch die EU im Zuge des Cybersecurity Act dieses Jahr behandelt. Und 2020 steht vermutlich die ePrivacy-Verordnung (ePVO) vor der Tür.

Regeln und Zuständigkeiten

Unternehmen jeder Branche und Größe, insbesondere aber kleine Mittelständler sind mit all diesen neuen Anforderungen meist überfordert. Dies zeigt eine Bitkom-Umfrage zur Umsetzung der Datenschutz-Grundverordnung in Deutschland, bei der von 503 befragten Unternehmen nur jedes vierte angegeben hat, alle Vorgaben der DSGVO bereits vollständig umgesetzt zu haben.

Dass Unternehmen bei all diesen regulatorischen Vorgaben schnell den Überblick verlieren, ist nicht verwunderlich. Betrachten wir beispielsweise die Anforderungen für Betreiber eines Online-Shops: Die Compliance- bzw. Rechtsabteilung muss sicherstellen, dass Anforderungen an AGBs, Widerrufsmöglichkeiten für Käufer, Lieferbedingungen und die Bestimmungen für das Impressum der Website umgesetzt sind. Der Datenschutz muss die Verarbeitungsprozesse des Online-Shops im Verzeichnis von Verarbeitungstätigkeiten dokumentieren, Informationspflichten nach Art. 13 DSGVO nachkommen und sicherstellen, dass entsprechende technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten implementiert sind. Die Security- und Risk-Abteilung kümmert sich – leider oft ohne Absprache mit dem Datenschutz – um Verschlüsselungsmaßnahmen, Maßnahmen gegen Angriffe auf die Website und eine Risikobetrachtung, um den Anforderungen an Diensteanbieter nach § 13 Telemediengesetz nachzukommen. Darüber hinaus gibt es oftmals noch Verantwortliche für das Business Continuity Management, die die Verfügbarkeit des Online-Shops sicherstellen und sich um Backups kümmern müssen.

Internationale Standards bieten Hilfestellung

Hier zeigt sich nun das grundsätzliche Problem: Unternehmen haben etliche Fachabteilungen, die verschiedene Teilbereiche von prinzipiell sehr ähnlichen Anforderungen betrachten und sich dabei viel zu oft nicht untereinander absprechen. Nicht nur der Datenschutz, sondern auch das Telemediengesetz, das Geschäftsgeheimnisschutzgesetz und, falls es sich um ein KRITIS-Unternehmen handelt, das IT-Sicherheitsgesetz verweisen auf die großen Schnittmengen einer notwendigen Risikobetrachtung und der angemessenen Implementierungen technischer und organisatorischer Maßnahmen.

Viele Unternehmen haben mittlerweile verstanden, dass international etablierte Best Practices, wie die ISO 27001 für Informationssicherheit, die ISO 22301 für Business Continuity Management oder die ISO 19600 für Compliance-Managementsysteme große Hilfestellungen bieten, um regulatorische Anforderungen der IT-Sicherheit und des Datenschutzes zu bewältigen. So können etwa ISO-27001-Maßnahmen helfen, Anforderungen an technische und organisatorische Maßnahmen nach dem Telemediengesetz oder der Datenschutz-Grundverordnung zu erfüllen. Die ISO 22301 hilft Unternehmen, die Verfügbarkeit von Systemen zu gewährleisten, und die ISO 19600 dabei, notwendige Compliance-Prozesse zu implementieren, wie z. B. die Gewährleistung von Meldepflichten nach DSGVO oder IT-Sicherheitsgesetz.

Best Practices lassen sich kombinieren

Leider ist das oben dargestellte Beispiel des Online-Shops kein Einzelfall. Auch die Umsetzung von ISO-Normen erfolgt oft entkoppelt getrennt für jeden Fachbereich und ohne Absprache, was redundante Implementierungen und Dokumentationen zur Folge hat. Dabei spielen die genannten ISO-Standards den Verantwortlichen eigentlich in die Karten, sollte eine einheitliche Betrachtung regulatorischer Anforderungen der IT-Compliance mit ISO-Best-Practices angestrebt werden: Managementsysteme der ISO werden nach der gleichen High Level Structure aufgebaut, was Unternehmen ermöglicht, verschiedene ISO-

Normen miteinander zu kombinieren, um ein integriertes Managementsystem zu implementieren.

Um beschriebene Anforderungen der IT-Compliance ganzheitlich zu betrachten und effizient zu erfüllen, ließe sich ein integriertes Managementsystem aus ISO 27001, ISO 19600, ISO 22301 und anderer datenschutzspezifischer ISO-Normen, wie etwa der ISO 27701 als „Datenschutz-Add-on" der ISO 27001, konzipieren und implementieren. Das könnte, vereinfacht dargestellt, folgendermaßen aussehen.

Im Anwendungsbereich wird definiert, dass im Rahmen des Managementsystems bestimmte Werte des Unternehmens an bestimmten Standorten betrachtet werden, so zum Beispiel der Online-Shop. Es werden technische und organisatorische Maßnahmen nach ISO 27001 in Verbindung mit ISO 27701 risikobasiert definiert und implementiert, wodurch Integrität, Vertraulichkeit und Verfügbarkeit gewährleistet werden. Dabei wird auf Anforderungen des Telemediengesetzes, der Datenschutz-Grundverordnung, des Geschäftsgeheimnisschutzgesetzes und bei Bedarf weiterer regulatorischer Anforderungen verwiesen, die technische und organisatorische Maßnahmen benötigen. Zur Stärkung der Verfügbarkeit wird das klassische Risikomanagement um eine Business-Impact-Analyse nach ISO 22301 erweitert, aus der sich Notfall- und Wiederherstellungspläne ableiten lassen. Rollen und Verantwortlichkeiten werden umfassend für alle Bereiche der IT-Compliance definiert und nicht nur für Teilaspekte aus Informationssicherheit oder Datenschutz. Leit- und Richtlinien werden nicht pro Themenfeld erstellt, sondern kombiniert, da etwa Richtlinien für den zulässigen Gebrauch von Geräten und Betriebsmitteln, Richtlinien für Kryptografie oder eine Ereignisprotokollierung relevant für alle genannten regulatorischen Anforderungen der IT-Compliance sein können.

Der Prozess steht im Mittelpunkt

Zusammengefasst lässt sich sagen: Mit der Nutzung eines integrierten Managementsystems zur Bewältigung einer Vielzahl von regulatorischen Anforderungen ist der Weg frei hin zu einem wert- bzw. prozessorientierten Ansatz und weg von einer rein fachrichtungsspezifischen Sicht. Im Beispiel des Online-Shops kümmern sich also nicht mehr die jeweiligen Fachabteilungen um ihre speziellen Anforderungen, sondern der gesamte Prozess steht im Mittelpunkt und Maßnahmen zur Erfüllung der Anforderungen werden zentral gesteuert.

Im Verzeichnis der Werte (Asset Repository) werden alle Werte, wie eben der Online-Shop, aufgenommen, mit wertebetreffenden regulatorischen Anforderungen verknüpft und im besten Fall mit notwendigen Informationen nach Art. 30 DSGVO erweitert, sodass eine weitere Dokumentation für ein Verzeichnis von Verarbeitungstätigkeiten gar nicht mehr nötig ist. Im Risikomanagement werden zentral Security-, Datenschutz- und sonstige Compliance-Risiken gesteuert. Dadurch können nicht nur risikobasierte TOMs definiert werden, eine Datenschutzfolgenabschätzung nach Art. 35 DSGVO könnte direkt aus der Risikobetrachtung exportiert und ein Notfallmanagement im Sinne der ISO 22301 aufgebaut werden. Im Rahmen des Compliance-Managements werden für alle zugrunde liegenden regulatorischen Anforderungen Maßnahmen bei der Identifizierung von Nichtkonformitäten definiert. Redundante Maßnahmen und Dokumentationen lassen sich dadurch vermeiden und regulatorische Anforderungen effizienter und gesamtheitlicher behandeln.

Fazit

Regulatorische Anforderungen des Datenschutzes, der IT-Sicherheit und der Informationssicherheit werden immer gewisse Schnittmengen aufweisen. Bei der Umsetzung der diskutierten Themen müssen im Rahmen der Gap-Analyse, die bei Implementierungsprojekten immer an erster Stelle stehen sollte, entsprechende Schnittstellen identifiziert werden, um Verbesserungen im Sinne aller notwendigen Anforderungen der IT-Compliance umzusetzen. Zudem sollten Dokumentationen auf alle Anforderungen ausgerichtet und kontinuierliche Verbesserungsprozesse für alle Anforderungen umgesetzt werden. Und das nicht separat von Fachbereich zu Fachbereich, sondern in Zusammenarbeit und mit dem betreffenden Prozess im Mittelpunkt, um eine effiziente und ganzheitliche IT-Compliance zu ermöglichen.

Tobias Theelen
esatus AG

E-Government in der Cloud

Ein datenzentrischer Ansatz bietet höhere Sicherheit beim Cloud-Computing

Die Cloud ist bei Behörden und Kommunalverwaltungen ein Treiber der digitalen Transformation. Herkömmliche Sicherheitskonzepte greifen für die Datensicherung in der Public Cloud aber zu kurz. Neue Ansätze und Lösungen können Daten selbst im Falle eines Angriffs effektiv schützen.

E-Government vereinfacht die Arbeit, hilft beim Abbau von überbordender Bürokratie und schafft mehr Bürgernähe. Die Menge personenbezogener und sensibler Daten wächst allerdings aufgrund der wachsenden Digitalisierung kontinuierlich. Der Einsatz von Cloud-Computing und die Nutzung von Public Clouds können dabei helfen, diese Datenflut zu bewältigen. Angebote wie Dropbox, iCloud oder Google Drive werden deshalb auch von Behörden heute zunehmend genutzt. Im Umfeld öffentlicher Verwaltungen und Behörden wird jedoch mit besonders vielen sensiblen Daten der Bürger gearbeitet, die keinesfalls in die Hände von Hackern gelangen dürfen. Der Schaden für den Einzelnen und die Gesellschaft wäre immens. Zudem unterliegen im Zuge der europäischen Datenschutz-Grundverordnung (DSGVO) sicherheitsrelevante und personenbezogene Daten strengeren Datenschutzvorgaben. Das Thema nimmt also auf der Tagesordnung staatlicher und kommunaler Entscheidungsgremien mittlerweile einen festen Platz ein.

Verständliche Skepsis

Beim Thema IT-Sicherheit scheint es jedoch – ebenso wie in vielen Unternehmen – noch viel Nachholbedarf bei den Behörden zu geben. Das stellte u. a. das „Zukunftspanel Staat & Verwaltung 2017“ fest, Teil einer Studie zu Verwaltungsmodernisierung und Digital Government, die von der Wegweiser GmbH Berlin Research & Strategy in Kooperation mit der Hertie School of Governance seit 2013 jährlich durchgeführt wird. 336 Verantwortliche aus allen Behördenebenen gaben Auskunft zum aktuellen Stand der Digitalisierung, ihren Umsetzungserfahrungen sowie zukünftigen Herausforderungen bei der Einführung von E-Government in der deutschen Verwaltung. Das Ergebnis ist eindeutig: 83,5 Prozent sehen mögliche Cyberangriffe als starke Bedrohung für die eigene Behörde an.

Hoch ist die Skepsis der Behörden bei der Einführung von Cloud-Computing und Big-Data-Anwendungen, die demzufolge auch bei einer Mehrheit der befragten Behörden nicht geplant sind. Diese Skepsis ist durchaus begründet: Denn während viele Behörden und Verwaltungen in den vergangenen Jahren Schutzwälle und Sicherheitsschleusen gezogen haben, um die eigene Infrastruktur und IT-Systeme vor äußeren Einflüssen zu schützen, geben sie mit der Nutzung von Cloud-Diensten ihre sensiblen Daten in fremde Hände. Mit diesem Schritt befürchten zahlreiche Behörden einen unberechtigten Zugriff durch Hacker auf sensible und personenbezogene Daten.

Datenzentrischer Ansatz

Das Problem: Herkömmliche Sicherheitskonzepte unterscheiden zwischen öffentlichen und internen Netzwerken. Eine solche Perimetersicherheit reicht bei der Nutzung von Cloud-Diensten aber nicht mehr aus. Die Verarbeitung und Speicherung der Daten verlagert sich durch die Cloud ja gerade auf externe Systeme. Cloud-Provider oder Cyberkriminelle könnten sich somit Zugriff verschaffen. IT-Sicherheitslösungen für die Cloud müssen deshalb in der Lage sein, die Daten unabhängig von ihrem Speicherort vor dem Zugriff (unberechtigter) Dritter zu schützen.

Die Lösung: Technisch umsetzen lässt sich die Absicherung der Daten mit einem datenzentrischen Sicherheitsansatz. Es spielt dann keine Rolle mehr, ob die Daten in einem Behördennetzwerk oder in einer Cloud abgelegt werden, die Sicherheit ist direkt in die Daten eingeschrieben und ermöglicht maximale Flexibilität. Denn allein die Metadaten eines Dokuments werden als Platzhalter in die Cloud geladen. Das Originaldokument selbst wird hingegen in einem sogenannten Streaming-Verfahren verschlüsselt. Die Fragmentierung der Dokumente in mehrere kleine Teile – sogenannte Chunks – bietet weiteren Schutz. Die Chunks können durch einen Software Defined Storage Layer in konfigurierbaren Speicherorten abgelegt werden. Dadurch kann der Nutzer unabhängig von der benutzten Cloud-Lösung autonom entscheiden, wo er seine Daten speichert, und sicherstellen, dass die Originaldokumente und Daten beispielsweise in Europa verbleiben.

Daten, die Europa nicht verlassen dürfen, werden logisch-rechtlich in verschiedenen europäischen Rechenzentren sicher verschlüsselt und verteilt abgelegt. In der globalen Cloud liegen ausschließlich virtuelle Dateien ohne sensiblen Dateninhalt, die aber dafür sorgen, dass von allen autorisierten Nutzern alltägliche Arbeitsabläufe in der Cloud wie gewohnt genutzt werden können. Diese Art der Speicherung ist nicht nur besonders sicher, sie entspricht auch den strengen Datenschutz- und Sicherheitsvorgaben der EU-DSGVO.

Fragmentierte Daten in der Cloud

Ein Anmeldesystem regelt über verschiedene Sicherheitsabfragen den Zugriff und überprüft den Benutzer. Nur Mitarbeiter mit autorisierten Zugriffsrechten können das komplette Dokument herunterladen. Beim Download wird das Dokument aus seinen Einzelteilen wieder zusammengesetzt und entschlüsselt. Auf diese Weise können die Mitarbeiter das Dokument trotz Verschlüsselung und Fragmentierung von verschiedenen Standorten aus öffnen und gemeinsam daran arbeiten.

Die physikalische Fragmentierung in mehrere kleine Teile schützt die Daten besonders stark vor Angriffen und fremden Zugriffen. Das Originaldokument ist nie vollständig einsehbar und nur in Form von Fragmenten hinterlegt. Selbst bei einem Angriff auf die Cloud oder wenn Hacker in ein System eindringen, bleiben die vertraulichen Inhalte für Angreifer oder nicht befugte Personen unlesbar.

Mit einer solchen Lösung können Public Clouds sicher genutzt werden, ohne dass Unternehmen den Verlust ihrer Daten befürchten

müssen. R&SÆTrusted Gate von Rohde & Schwarz Cybersecurity ist beispielsweise eine solche Cloud-Security-Lösung, die den datenzentrischen Ansatz umsetzt. Sie lässt sich nahtlos in gängige Public Clouds wie Microsoft Azure, Google, AWS und Collaboration-Tools wie Microsoft Office 365 und SharePoint einbinden, sodass eine gewohnte Nutzung möglich ist. Besonders für weltweit tätige Unternehmen und für Behörden mit mehreren Standorten ist der datenzentrische Ansatz hilfreich, da er flexibles und kollaboratives Arbeiten auf sichere Weise ermöglicht.

Skalierbare Sicherheit

Eine solche Lösung eignet sich somit perfekt für global agierende Teams, die Dokumente untereinander austauschen und gemeinsam bearbeiten müssen. Die Lösung läuft transparent in bestehenden Anwendungen, sodass Arbeitsabläufe weitgehend unverändert bleiben. Eine spezielle Suchfunktion ermöglicht eine sichere Volltextsuche selbst in verschlüsselten Dokumenten.

Weitere entscheidende Vorteile für die IT-Sicherheit in der Cloud bieten skalierbare Sicherheitssysteme. Sie bieten die Möglichkeit, Elemente einer IT-Sicherheitslösung abhängig von deren Sicherheitsbedarf entweder on-premises oder in der Cloud abzulegen. Auf diese Weise lassen sich die Vorteile der Cloud nutzen, ohne auf die notwendige Sicherheit verzichten zu müssen. Eine solche Skalierung der Sicherheit wird möglich durch ein sogenanntes „Containering“. Bei diesem Architekturmodell kommen kleinste Softwareeinheiten – sogenannte Microservices – zum Einsatz, die sich unabhängig voneinander steuern lassen.

Microservices für sensible Elemente, wie etwa den Key- und Administrationsserver, können dann zum Beispiel auf der eigenen Hardware abgelegt werden. Falls eine solche nicht vorhanden oder unzureichend ist, kann auch eine Cloud mit einem höheren Sicherheitsniveau genutzt werden. Kryptografisch weniger kritische Abläufe lassen sich dann auf andere Clouds auslagern. Sicherheitslösungen, die mit Microservices arbeiten, eignen sich auch für global agierende Firmen mit komplexen Strukturen. Die Software lässt sich flexibel an die unterschiedlichsten Bedingungen anpassen, beispielsweise an die Betriebsgröße oder im internationalen Geschäft auftretende Zeitverschiebungen.

Fazit

Die datenzentrische Sicherheit ist so ausgelegt, dass sie jede Datei, egal wo sie abliegt, vor Missbrauch schützt und die Cloud damit zu einem sicheren Ort macht. Die Perimetersicherheit wird dadurch aber keineswegs abgelöst. Sie bleibt weiterhin ein wichtiger Schutzwall vor Angriffen von außen. Durch die Verbindung von beiden Absicherungsstrategien erreichen Unternehmen ebenso wie Behörden den bestmöglichen Schutz und können die Chancen der Digitalisierung nutzen, ohne ihre Daten zu gefährden.

Dr. Falk Herrmann
Rohde & Schwarz Cybersecurity

Unterschrift aus einer Hand

Vereinfachte Identifikationsverfahren wirken als Katalysator der E-Signatur

Die Zeit, da jedes Dokument persönlich und handschriftlich unterzeichnet werden muss, neigt sich allmählich ihrem Ende zu. Identifikation, Registrierung und Signatur lassen sich heute mittels geeigneter Applikationen in einen geschlossenen digitalen Gesamtprozess integrieren.

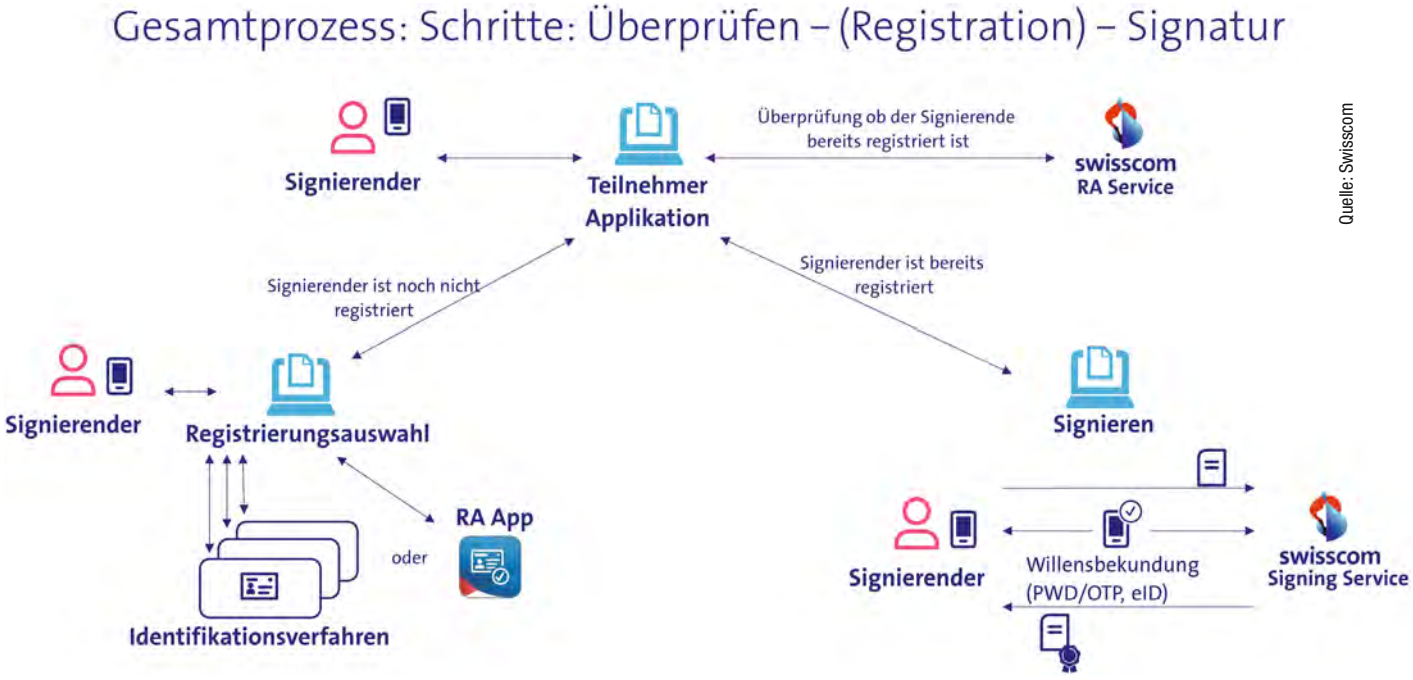
Als Charley Kline am Vormittag des 29. Oktobers 1969 die erste Nachricht zwischen zwei Computersystemen über den Vorläufer des heutigen Internets versandte, war nicht abschätzbar, welche fundamentalen Auswirkungen die Weiterentwicklung dieser Technologie haben würde. Der erste Versuch dieser Übertragung scheiterte, da eines der Systeme nach der Übertragung der zwei Buchstaben „l“ und „o“ abstürzte. Die Techniker der beiden involvierten Universitäten mussten sich damals noch mittels einer parallel dazu laufenden, analogen Telefonverbindung abstimmen und darüber melden und verifizieren, was gesandt beziehungsweise was empfangen wurde.

Seit diesem Ereignis vor 50 Jahren ist viel passiert und das Internet hat zur Entstehung einiger der wertvollsten Unternehmen überhaupt beigetragen. Dennoch muss auch heute noch allzu oft auf analoge Mittel zurückgegriffen werden, um Business-Transaktionen abzuwickeln – ähnlich wie die Techniker damals mit der Telefonleitung. Verträge müssen ausgedruckt, von Hand unterzeichnet und versandt werden und oftmals müssen Menschen zwecks Identifizierung persönlich vorstellig werden. Technisch und gesetzlich besteht seit längerer Zeit die Möglichkeit, diese Prozesse vollständig digital mittels qualifizierter elektronischer Signatur durchzuführen. In der Realität existiert aber eine Reihe von Hürden, die sich schleppend auf die Verbreitung ausgewirkt haben.

Notwendige Hürde

Die elektronische Signatur wird über kurz oder lang die händische Unterschrift als bevorzugte Form der Beglaubigung einer Willenserklärung ablösen. Die Abwicklung von geschäftlichen Transaktionen mittels elektronischer Signatur bringt dabei einen deutlichen Sicherheitsgewinn, denn die händische Unterschrift ist in puncto Sicherheit kein harter Konkurrent, sie kann mit einfachsten Mitteln kompromittiert werden. Der Sicherheitsgewinn wird durch die Implementierung von standardisierten Sicherheitskomponenten erreicht, aber zu einem großen Teil auch aufgrund von strengen Richtlinien und Kontrollen, insbesondere für das Level der qualifizierten elektronischen Signatur.

Damit ein Nutzer eine qualifizierte elektronische Signatur auslösen kann, muss er eindeutig identifiziert werden. Die eindeutige Identifikation stellt derzeit in vielen Prozessen eine (notwendige) Hürde dar. Wenn die Identifizierung nicht durch persönliches Erscheinen von Angesicht zu Angesicht möglich ist, müssen weitere Verfahren gefunden und integriert werden. Für den Identitätsabgleich gibt es verschiedene Ver-



Der kurze Weg von der Identifikation bis zur Signatur.

fahren zahlreicher Anbieter wie BankIdent, Videoident bis hin zur persönlichen Erfassung via Smartphone-App. Mit dem Verfahren zur Identifikation per Smartphone-App beispielsweise kann eine Person innerhalb von wenigen Minuten für die qualifizierte elektronische Signatur identifiziert und registriert werden, unter Einhaltung der eIDAS-Vorgaben. Eine solche Lösung verhilft Unternehmen und Organisationen, ihre Belegschaft schnell für die elektronische Signatur zu befähigen und beschreibt damit einen sehr effektiven Anwendungsfall.

Der Markt unterliegt aber einer starken Weiterentwicklung. Dies macht es für Unternehmen heute schwierig, einen Partner oder ein Verfahren auszuwählen, welches langfristig alle Anwendungsfälle abdeckt. Doch mehrere Verfahren von verschiedenen Anbietern selbst zu integrieren, ist für Unternehmen selten praktikabel und erhöht die Komplexität der Umsetzung bezüglich rechtlicher Freigabe sowie auch aus technischer Perspektive.

Zentraler Integrationspunkt

Aus diesem Grund bietet es sich an, auf einen Anbieter zu vertrauen, der es ermöglicht, verschiedene Identifikationsverfahren aus einer Hand zu nutzen. Die Teilnehmerapplikationen können eine Auswahl mehrerer Identifikationsverfahren nutzen, die Integration findet direkt beim Anbieter statt. Der Ablauf für den Nutzer stellt sich wie folgt dar: Der Signierende befindet sich in einem Prozess, bei welchem er elektronisch unterschreiben muss. Die Teilnehmerapplikation prüft, ob der Signierende für das geforderte Signaturlevel, wie zum Beispiel die qualifizierte elektronische Signatur nach eIDAS, bereits registriert ist. Trifft dies zu, wird der Prozess der Signaturerstellung ausgelöst und abgeschlossen. Trifft dies nicht zu und der Signierende ist noch nicht registriert, hat die Teilnehmerapplikation die Möglichkeit, verschiedene Identifikationsmethoden anzusteuern.

Muss eine Identifikation erfolgen, kann das passende, verfügbare Verfahren ausgewählt werden. Nach der erfolgreichen Identifikation wird die Identifikationsevidenz für künftige weitere Signaturen im RA Service abgelegt. Daraufhin kann der eigentliche Signaturprozess durchlaufen werden. Auf diese Weise können Identifikationsanbieter und Signaturapplikationen in einem kohärenten Ökosystem entsprechend den eIDAS-Vorgaben zusammengeführt werden.

Fazit

Die geringeren Hürden im Identifikationsprozess erleichtern es Unternehmen, komplett digitale Prozesse basierend auf der elektronischen Signatur anzubieten. Damit wird es deutlich wahrscheinlicher, schon sehr bald sämtliche Transaktionen komplett auf diese Art abwickeln zu können. Der analoge Kanal via Papier wird schließlich ähnlich weit in der Vergangenheit zurückliegend erscheinen wie der erste Versand einer Nachricht zwischen zwei Computersystemen 1969.

Marco Schmid
Swisscom Trust Services

Entbürokratisierung treibt die Digitalisierung voran

Ein neues Gesetz soll für Unternehmen und Behörden vieles einfacher machen

Am 24.10.2019 hat der Deutsche Bundestag das dritte Bürokratieentlastungsgesetz (BEG III) verabschiedet. Bestandteile sind unter anderem ein elektronisches Meldeverfahren zur Einreichung von Krankenscheinen und die Einführung eines digitalen Meldescheins für die Hotellerie. Im Interview bezieht Jürgen Vogler, Geschäftsführer der procilon GROUP, Stellung zu diesen Themen.

Foto: procilon IT-Solutions GmbH

Jürgen Vogler, Geschäftsführer der procilon IT-Solutions GmbH

Herr Vogler, nach Ansicht der Bundesregierung können Unternehmen durch Digitalisierung erheblich Kosten sparen. Auf der anderen Seite häufen sich gerade die Meldungen von Trojanern, die ganze Unternehmen oder Gerichte außer Betrieb nehmen. Ist die Digitalisierung gescheitert bevor sie so richtig begonnen hat?
Die Liste der angegriffenen Unternehmen und Behörden ist inzwischen erschreckend groß. Aber das sollte uns alle nicht von weiteren Aktivitäten in Richtung moderner und effizienter Prozesse abhalten. Deshalb begrüßen wir als Unternehmen und auch ich als Bürger alle Initiativen, die dabei helfen, bürokratische Hürden digital umzustoßen. Allerdings können nach unserer Auffassung alle Bemühungen zur digitalen Transformation nur erfolgreich sein, wenn ein Kulturwandel hin zu einem größeren Sicherheitsbewusstsein damit einhergeht. Vertrauen allein wird hier nicht ausreichen. So haben wir schon in Bezug auf das Onlinezugangsgesetz darauf verwiesen, dass es nicht darum geht, das Rad digital neu zu erfinden, sondern durch die Anwendung bestätigter elektronischer Identitäten und vertrauenswürdiger, also verschlüsselter Kommunikation, völlig neue und benutzerfreundliche Lösungen zu schaffen. Damit wird dann nicht nur die erhoffte Kostenersparnis erreicht werden, sondern auch ein nachhaltiger Nutzen für Bürger und Unternehmen. Nur damit wird Akzeptanz erreicht.

Der Gesetzentwurf sieht vor, dass beim elektronischen Meldeverfahren im Beherbergungsgewerbe optional die eigenhändige Unterschrift auf dem Meldeschein durch sichere digitale Verfahren ersetzt werden kann. Was ist damit gemeint?
Abzuwarten bleibt hier, was der Gesetzgeber unter „andere sichere Verfahren“ versteht. Heute reden wir beim Ersatz der Unterschrift primär von der qualifizierten elektronischen Signatur (QES), also im übertragenen Sinn die Anwendung einer bestätigten elektronischen Identität. Für die QES haben wir zwar schon lange die juristische Klarheit darüber, dass sie den gleichen Wert wie die eigenhändige Unterschrift hat, aber die Anwendung ist in der Vergangenheit vorsichtig formuliert etwas sperrig gewesen, da sie an eine SmartCard gebunden war. Zu deren Anwendung benötigt man zusätzlich noch ein Lesegerät. Die Akzeptanz solcher Szenarien ist nicht sonderlich groß und lässt sich aus meiner Sicht durchaus im oben genannten Sinn verbessern. Ähnlich verhält es sich bei dem im Gesetzentwurf genannten digitalen Meldeschein. Die Möglichkeit, in diesem Zusammenhang die eID-Funktion des Personalausweises zu nutzen, ist begrüßenswert, aber könnte ebenfalls an den technischen Voraussetzungen scheitern. Wenn der Gesetzgeber den Mut hat, zum Beispiel das Potenzial der eIDAS-Verordnung voll auszuschöpfen, können hier durchaus interessante Lösungen entstehen.

Wollen Sie uns verraten, welche?
Das wird deutlich, wenn man wieder die Position des Nutzers einnimmt. Der will eine einfache Anwendung ohne allzu viel technischen Aufwand und nur eine elektronische Identität, mit der er alles erledigen kann. Der angestrebte Bürokratieabbau durch digitale Prozesse birgt aktuell die Gefahr, dass in den unterschiedlichen Anwendungsfeldern wie Online-Zugang zu Verwaltungen, Telematik-Infrastruktur im Gesundheitswesen, Kommunikation mit Finanzbehörden und der Justiz oder, wie im Gesetzentwurf vorgesehen, zur Übermittlung einer Arbeitsunfähigkeitsmeldung an den Arbeitgeber technisch in sich abgeschlossene Inseln entstehen, die zwar eine sichere Lösung anbieten, aber zum einen nicht kompatibel sind und zum anderen für Bürger oder Unternehmen jeweils eine eigene elektronische Identität voraussetzen. So etwas kann man auch in einer föderalen Staatsform anders standardisieren. In Europa haben wir das mit eIDAS ja auch geschafft. Nicht zuletzt haben wir auf dieser Grundlage unsere erst kürzlich vorgestellte proTECTr Embedded Service Architecture definiert, mit der sich Fachprozesse um elementare Sicherheitskomponenten ergänzen lassen.

Ein interessanter Blickwinkel. Aber wie kann so etwas funktionieren?
Dafür möchte ich als Beispiel den elektronischen Rechtsverkehr anführen. Zugegeben ein Themenfeld, in dem wir uns schon seit Jahren bewegen: Hier werden sichere Kommunikationsbeziehungen zwischen unterschiedlichsten Anwendergruppen hergestellt. Auch hier sind sichere Verfahren in Form von sogenannten sicheren Übertragungswegen definiert, die sich durchaus technisch stark unterscheiden. Zentrale Komponente ist aber ein Verzeichnisdienst, der eine übergreifende Gültigkeit von elektronischen Identitäten zulässt. Im jeweiligen Hoheitsgebiet werden diese Identitäten auf hohem Niveau bestätigt. Auf diese Weise ist nicht nur eine verschlüsselte Kommunikation, sondern auch der Zugriff auf Systeme und Anwendungen möglich. Solche Architekturen haben eine vertrauensstärkende Wirkung und lassen sich dazu noch stark automatisieren. Der Anwender hat einen einmaligen Implementierungsaufwand und keine weitere Behinderung in der täglichen Arbeit. Das ist die Vorstellung, die wir von nutzerfreundlicher IT-Sicherheit haben.

Hat die bewährte Signaturkarte damit ausgedient?
Das glaube ich nicht. Wenn ich denn doch eine Signaturkarte oder den Ausweis mit Leser benutzen muss, steigt die Akzeptanz umso deutlicher, desto mehr ich sie benutzen kann. Der Schlüssel hierzu sind sogenannte Mehrwertdienste.

Nehmen wir dazu ein Beispiel aus dem Gesundheitswesen. Hier kann ein Arzt mit seinem eArztausweis nicht nur Rezepte oder Arztbriefe elektronisch unterschreiben, sondern hat über diese bestätigte elektronische Identität auch Zugriff auf die abgesicherte Telematik-Infrastruktur und dort verfügbare Anwendungen. Zukünftig erhält er damit auch Zugriff auf die Patientendaten auf der eGK oder kann eRezepte ausstellen. Mit jeder weiteren Funktion wird die Karte für den Arzt wertvoller. Die elektronische Unterschrift auf dem Krankenschein ist ein weiterer Baustein dazu.

Herr Vogler, wenn aber bei der Digitalisierung das Risiko für Cyberangriffe immens steigt, ist es dann nicht besser, doch bei Papierakten und Briefpost zu verharren?
Wie das berühmte Kaninchen vor der Schlange, das dann doch gefressen wird? Nein, auf gar keinen Fall! Zum einen würde uns ein Scheitern der sicheren Digitalisierung die Geschäftsgrundlage entziehen und zum anderen will ich nicht ständig Estland, die Slowakei oder Österreich als Best Practice vorgesetzt bekommen. Wir, und damit meine ich die Gemeinschaft aus Behörden, Fachverfahrensherstellern und die IT-Sicherheitsfirmen im TeleTrusT e. V., können das mindestens genauso gut, wenn nicht sogar besser. Wir müssen nur mal loslegen.

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

Security by Design, by Obscurity oder by Forecast?

Die IoT-Sicherheit kämpft mit alten Problemen und fragwürdigen Prognosen

Sechs Jahre nach ihrer Proklamation ist bei der Industrie 4.0 noch immer kein einheitlicher Sicherheitsstandard in Sicht. Stattdessen dominieren angestaubte Lösungen und wir träumen von Blockchain und Quantencomputern. Eigentlich war aber die Blickrichtung mit „Security by Design“ schon vorgegeben – oder doch nicht?

Beginnen wir mit einem motivierenden Aspekt – mit der Tatsache nämlich, dass Industrie 4.0 im Grunde eine deutsche Erfindung ist. An sich keine ungewöhnliche Beobachtung, dass Informations- und Netzwerktechnik seit den 1960er-Jahren immer mehr Anschluss suchen zu den traditionellen Disziplinen wie Mechanik oder Elektronik. Typisch für das Land der Dichter, Denker und DIN-Normen war es dann, eine von der Bundesregierung beauftragte Arbeitsgruppe ins Leben zu rufen, die 2013 ihren finalen Bericht veröffentlichte. Seitdem definieren wir die vierte industrielle Revolution auch über ihren neuartigen Sicherheitskern, der neben dem Grundprinzip des „Security by Design“ auch eine Reihe von modernen Begriffen prägte wie „Internet of Things“, „Internet of Systems“ oder „Cyber-Physical Systems“.

Was wir nun augenscheinlich begonnen haben, sollten wir getreu dem Motto „IT Security made in Germany“ auch zu Ende bringen – denn die internationale Konkurrenz schläft nicht, obgleich ihre proprietären Ideen nicht gerade neu sind und auch nicht unbedingt die noch älteren Probleme lösen, die nach wie vor die Sicherheitswelt dominieren. Dazu später mehr.

Security by Design

Auch wenn der berühmte Bericht der Arbeitsgruppe „Industrie 4.0“ nicht gerade ein Kochbuch voller Rezepte zum schnellen Nachkochen von breitflächigen Sicherheitslösungen ist, so stimmt er manch einen dennoch nachdenklich. Es werden tatsächlich sehr sinnvolle Designaspekte angesprochen, wie etwa die Motivation und gleichzeitige Mahnung, das Konzept „Security by Design“ nicht einfach nur an einzelne funktionale Komponenten zu binden, sondern dieses möglichst global auszulegen. Wenn man länger über diese globale Bedeutung nachdenkt, gelangt man zu Erkenntnissen wie dem Begriff der „symbiotischen Sicherheit“. Dieser findet heute bereits in wissenschaftlicher Literatur Verwendung (etwa in dem Beitrag „Reference Architecture for Secure Cloud Based Remote Automation – Zero-Knowledge Initial Enrolment of Resource-Constrained IoT with Symbiotic Security“, atp Magazin, Septemberausgabe 2019).

Demnach lässt sich eine höhere Form der architektonischen Sicherheit nur dann herbeiführen, wenn die wichtigsten Disziplinen wie Softwaretechnik, Hardware bzw. Elektronik, Netzwerk- sowie Prozesstechnik einen Schulterschluss bilden und sich dort gegenseitig ergänzen, wo die jeweils anderen ihre Grenzen haben. So lässt sich etwa die IoT-typische ressourcenbeschränkte Hardware hervorragend für starken Schutz der kryptografischen Schlüssel einsetzen. Sie kommt jedoch schnell an ihr Limit, wenn es darum geht, komplexe Sicherheitsprotokolle wie TLS rein in Hardware zu implementieren: Hier muss die Software aushelfen und gleichzeitig die Stärken der Hardware voll ausspielen. So entsteht am Ende eine symbiotische Beziehung zwischen den Architekturbausteinen, die das resultierende Sicherheitsniveau deutlich erhöhen kann.

Security by Obscurity

Soweit die Theorie von „Security by Design“. Doch was passiert eigentlich heutzutage in der Industrie, die sich selbst revolutionieren soll? Nun, die Gesetzgeber in Form von einschlägigen Regulierungsbehörden reagieren traditionell verhalten, indem sie bestenfalls Bestandsaufnahmen machen, die kaum über Empfehlungen hinausgehen. Die US-amerikanischen Vertreter wie NIST etwa veröffentlichen Berichtsentwürfe wie den „New NIST Report on Security of Consumer Home Internet of Things (IoT) Devices (NISTIR 8267)“ und bitten den interessierten Leser zur Stellungnahme in Form von öffentlichen Kommentaren. Die professionellere Ausrichtung in Form des „Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers 8259)“ sieht da auch nicht viel anders aus.

Die großen Technologiekonzerne wie Intel, Google oder Qualcomm wittern dagegen ihre Chance und nutzen ihre Vormachtstellung in weltweiten Allianzen wie FIDO, um das löbliche Konzept der passwortlosen Authentifizierung nunmehr auf nicht-interaktive Benutzer bzw. Maschinen auszuweiten. So wurde noch im Juni dieses Jahres eine neue Arbeitsgruppe unter dem Namen „FIDO IoT Technical Working Group“ ins Leben gerufen, die sich nun anschickt, eine neue Sicherheitsspezifikation für die Welt der IoT-Sicherheit zu etablieren. An sich kein schlechter Gedanke, doch das Erbe und damit die Vorgehensweise ist getrübt: die ursprüngliche und aktuelle FIDO-Spezifikation trifft einer gewissen Vorliebe für Bequemlichkeit geschuldet einige gefährliche Annahmen, die damit mehr Zugeständnisse einfordern, als die übliche Toleranzschwelle des modernen Sicherheitsverständnisses zulässt.

Die Rede ist von der Grundidee, die größtenteils schlecht gewählten Passwörter durch PKI (Public Key Infrastructure) zu ersetzen. PKI basiert auf asymmetrischen kryptografischen Verfahren, die von jeher jede praktische Umsetzung vor grundlegende Probleme gestellt haben: Wie etabliert man eine Vertrauensstruktur zwischen den Schlüsselträ-

gern, die ihre Schlüssel in digitale Zertifikate verpacken, und den Zertifizierungsstellen ohne Verlust der Datensicherheit und der Zuverlässigkeit der zwingend erforderlichen Beweisführung der eigenen Identität? Dieses Problem der Erstregistrierung (Initial Enrolment) ist im Grunde genauso alt wie die PKI selbst. Während nun die herkömmlichen Stammzertifizierungsstellen umständliche manuelle Prozesse aufrechterhalten, die von ihren jeweiligen Registrierungseinheiten (Registration Authorities) umgesetzt werden, nimmt FIDO an dieser Stelle eine fatale Abkürzung. Der FIDO-Registrierungsprozess geht von einem sog. Authenticator aus, der in Form einer mobilen App, einer PC-Anwendung oder eines USB-Dongles für die sitzungsbasierte Authentifizierung des Benutzers verantwortlich ist. Diese kann u. a. mithilfe von PIN-Eingaben oder biometrisch erfolgen. Im Grunde erzeugt der Authenticator während der Erstanmeldung ein Zertifikat (Attestation Certificate), dem zentral Vertrauen ausgesprochen und das dann in die entsprechenden Listen eingetragen wird, die wiederum von sog. Relying Parties zum Abgleich genutzt werden und so eine Authentifizierung gegenüber dem Zieldienst ermöglichen.

Dieses Grundvertrauen ist allerdings nur deshalb möglich, weil jeder Authenticator mit einem vorgefertigten Attestation Key (AK), also einem geheimen bzw. privaten Schlüssel ausgestattet ist, der ab Werk vorprogrammiert wird. Diese Praxis der vorgefertigten Geheimnisse, die logischerweise dem Hersteller bekannt sind, entspricht einem gängigen und gleichzeitig (zum Beispiel vom BSI) stark kritisierten Modell, das u. a. aus Trusted Platform Module (TPM) und damit nahezu jedem Laptop bekannt ist. Richtig gruselig wird es allerdings dann, wenn man erfährt, dass ein solcher AK nicht nur vorgefertigt, sondern vor allem quer über sämtliche Geräte einer Marke und Modellreihe wiederverwendet wird. Während die Hardware wie die USB-Dongles noch verhältnismäßig gut geschützt ist (aber dennoch keine vollständige Absicherung etwa gegen das Auslesen des Flash-Speichers oder des Datenbusses zwischen Speicher- und Mikrocontroller gewährleisten kann), sind Softwarepakete wesentlich einfacher zugänglich und bieten naturbedingt weniger Schutz gegen Reverse Engineering und das Auslesen von Geheimnissen.

Manche Hersteller machen sich an der Stelle noch erweiterte Konzepte wie die Whitebox-Kryptografie zunutze. Doch auch diese basiert letztlich auf einem geschickten Verstecken (Permutation) der Teilschlüssel (z. B. für AES-Verschlüsselung) innerhalb von großen Datentabellen im binären Programmcode. Diese Lösungen sind deshalb immer wieder erfolgreich angegriffen worden. Mobile Plattformen wie Google Android arbeiten dagegen im Grunde mit Java Bytecode, der als App zu einem Archiv verpackt und damit noch weniger gut vor Reverse Engineering geschützt ist. Das absolute KO-Argument in dem Zusammenhang ist jedoch die Tatsache, dass wenn ein AK auch nur von einem einzigen Gerät bzw. Authenticator erfolgreich extrahiert wird, die gesamte Modellreihe unwiederbringlich kompromittiert wird – ein Rückruf ist da kaum möglich, speziell in Hardware.

Komfortgetriebener proprietärer Ansatz

Neben der FIDO Basic Attestation wurde von der Allianz – ausgehend von der Beobachtung, dass ein oftmals wiederverwendeter Gruppenschlüssel wesentlich verwundbarer ist als ein individueller Schlüssel – ein weiteres verbessertes Schema ins Leben gerufen, das auf Direct Anonymous Attestation (DAA) der Trusted Computing Group für den TPM-v1.2-Standard basiert. Es nutzt zudem elliptische Kurven, um den Rechendurchsatz zu steigern bei gleichzeitigem Erhalt der Sicherheit zwecks besserer Effizienz. Das ECDAA, wie es auch genannt wird, geht zudem innerhalb der Web Authentication API (WebAuthn) auf, die gemeinsam vom World Wide Web Consortium (W3C) und FIDO veröffentlicht wird. WebAuthn soll insbesondere im Zusammenhang mit hardware-basierten Zweifaktor-Authentifizierungsgeräten zum Einsatz kommen, um Einmalpasswortmechanismen wie HOTP bzw. TOTP oder aber SMS 2FA (two-factor authentication) deutlich zu verbessern.

Es ist allerdings bemerkenswert, dass unabhängige Experten im Bereich der Kryptografie noch im selben Jahr 2018, in dem auch der finale Implementierungsentwurf verabschiedet wurde, eine ganze Reihe von vermeidbaren Designunzulänglichkeiten identifizierten, die nach aktuellem Kenntnis- und Erfahrungsstand bei vergleichbaren Verfahren und den dort bekannt gewordenen Angriffen im frühen Entwurfsstadium hätten auffallen müssen. Hier wurden u. a. typische Protokolldefinitionsfehler begangen in Hinblick auf die Zurückhaltung in der Dokumentation von essenziellem Basiswissen. Diese führt meist dazu, dass die Entwickler, die konkrete Lösungen ausgehend von solchen Spezifikationen umsetzen, interpretativ arbeiten müssen und auf diese Weise unbewusst nicht nur Inkompatibilitäten einbauen, sondern auch unnötige Angriffsflächen. Auch bei ECDAA hätte man beispielsweise die ansonsten zwingende Maßnahme der Punktvalidierung auf der jeweiligen elliptischen Kurve klar und deutlich festhalten müssen.

Viel gravierender ist da allerdings die Feststellung, dass seit Jahrzehnten bekannte Schwachstellen wie „Bleichenbachers Padding Oracle“ nahezu unverändert wiederverwendet werden – so auch in WebAuthn. Der fast 20 Jahre alte Angriff basiert auf der Beobachtung, dass das für RSA erforderliche PKCS#1 v1.5 Padding (eine Randomisierung der Klartextnachricht, um die Verschlüsselung widerstandsfähiger zu machen u. a. gegen Mehrfachverschlüsselung der gleichen Nachricht mit dem gleichen oder verschiedenen Schlüsseln) den Klartext zu sehr zufällig verwürfelt, sodass geschickt gewählte Chiffrate (Adaptive Chosen Ciphertext) auf der entschlüsselnden Serverseite (Oracle) mehr oder weniger spät im Protokollverlauf als Fehler auffallen und dem Angreifer als solche entsprechend signalisiert werden. Aus diesen Seitenkanälen ist es deshalb möglich, mit der Zeit bzw. ausreichender Anzahl von Fehlversuchen den geheimen Schlüssel vollständig zu rekonstruieren.

Protokolle wie TLS reagierten mit Gegenmaßnahmen, die mit den Jahren immer komplexer wurden, was bei den bereits erwähnten Entwicklern zu Fehlinterpretationen und damit erneuten Anfälligkeiten führte. Diese wurden insbesondere im letzten Jahr wieder einer Vielzahl der TLS-Anwendungen zum Verhängnis im Kontext der sog. ROBOT-Attacke (die bezeichnenderweise für „Return Of Bleichenbacher’s Oracle Threat“ steht). Dabei wären wirkungsvollere Maßnahmen wie die Nutzung eines besseren Paddings (OAEP), das mehr Struktur in die Verwürfelung der Klartextnachrichten einbringt, deutlich einfacher gewesen als das Beibehalten von Lücken, die mehr und mehr gestopft wurden. Selbst das Aufgeben von RSA als Verschlüsselungs- und gleichermaßen betroffenes Signaturverfahren ist immer noch deutlich effektiver, was diese Maßnahme auch als Bestandteil von TLS 1.3 erklärt.

Elliptische Kurven

Was nun die elliptischen Kurven angeht, die insbesondere in ECDAA zum Einsatz kommen, so gibt es allein beim Thema Auswahl der passenden bzw. stabilen Kurven viele Stolperfallen. Ausgewiesene Experten auf dem Gebiet unterhalten deshalb eine dedizierte Anlaufstelle für Entwickler, um sie bei der Auswahl möglichst gezielt zu unterstützen. Neben der fehlerbehafteten Punktverifikation (Liegt ein Punkt auf der jeweiligen elliptischen Kurve oder nicht?) gibt es verlässliche Verfahren wie Punktkompression, die von ECDAA explizit ausgeschlossen

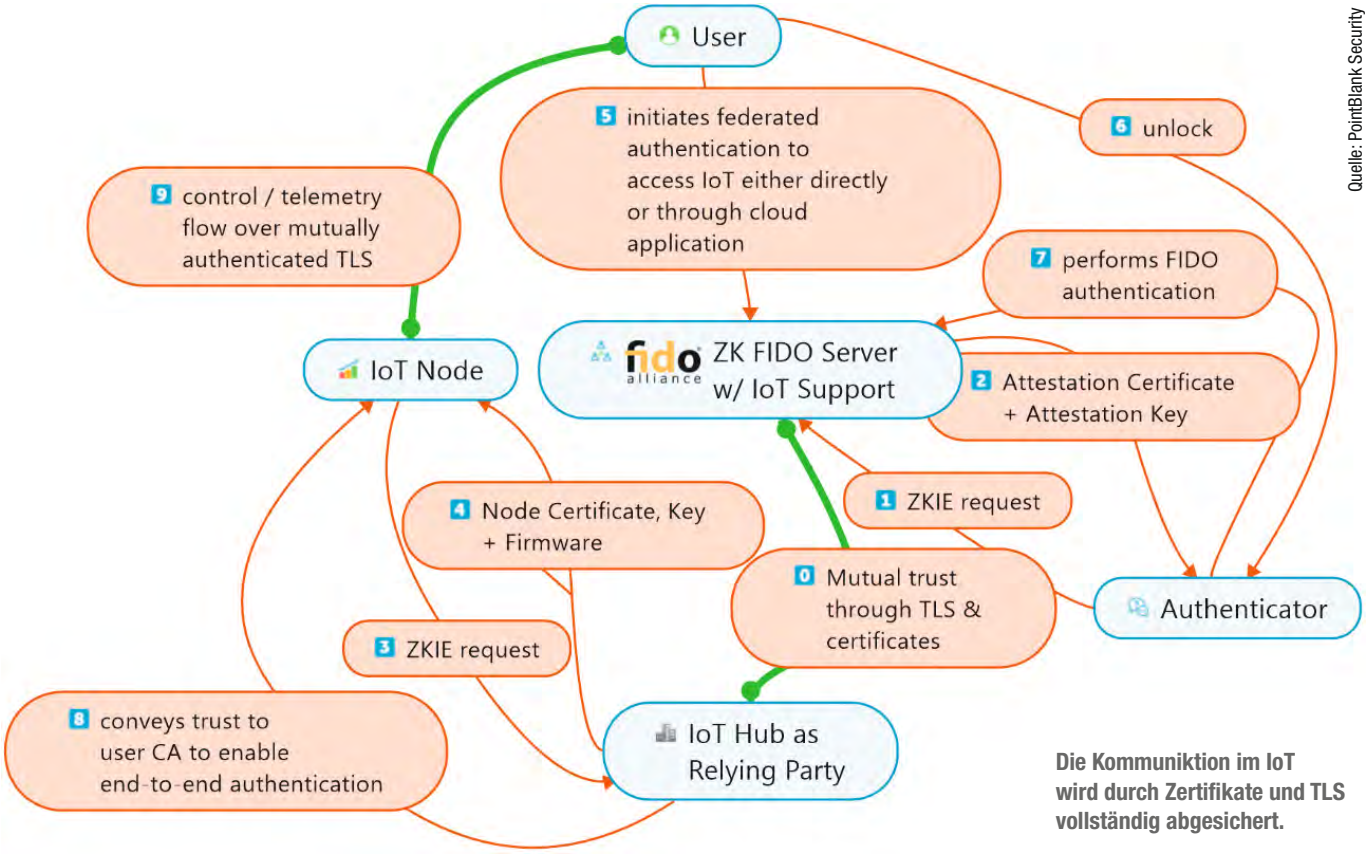
werden. Weiterhin hatte man eigentlich schon frühzeitig (2013) gelernt, dass bei digitalen Signaturen (mit oder ohne elliptische Kurven) zufällige Verwürfelung der Ausgangsnachricht (durch sog. k-Werte) ähnlich dem PKCS#1 v1.5 Padding zu Problemen führen kann. Hinzu kommt, dass der Umgang mit (pseudo-)zufälligen Zahlen für Entwickler auf diversen Plattformen nicht selbstverständlich oder selbsterklärend ist. Schlecht erzeugte Zufallszahlen können fatale Folgen haben, weshalb auch hier u. a. durch den RFC 6979 ein deterministisches und damit weniger anfälliges System für die Klartextverwürfelung eingeführt wurde.

ECDAA greift weder dieses Verfahren auf, noch liefert es Instruktionen hinsichtlich der Erwartung an die Zufälligkeit der eingesetzten k-Werte. Darüber hinaus setzt ECDAA auf elliptische Kurven, die das heute gesetzte Sicherheitsminimum um ganze 32 äquivalente (etwa 96 gegenüber den geforderten 128) Sicherheitsbits verfehlt, was einer Komplexitätsreduktion von ca. 4 Milliarden möglichen Kombinationen im Schlüsselraum entspricht. Gekrönt wird die Liste der Kritikpunkte mit der Feststellung, dass FIDO nicht einfach nur bestehende Standards wie (EC)DSA wiederverwendet. Vielmehr verabschiedet die Allianz mit ECDAA einen ungetesteten kryptografischen Ansatz (Pairing-basierte Authentifizierung), welcher der Effizienz halber auf elliptischen Kurven aufbaut mit allen erwähnten Parametrisierungsdefiziten.

Security by (Optimised) Design

FIDOs Vorgehensweise fällt nach reiflicher Überlegung nicht zwingend in die Kategorie „Security by Obscurity“, da sämtliche Spezifikationen öffentlich sind. Ein „Security by Design“-Kern ist hier allerdings auch nicht ganz zu erkennen, weil zu einem ernstzunehmenden Entwurf wesentlich mehr gehört als ein Griff in die Mottenkiste, der angestaubte Verfahren mit schlecht verstandenen Einflussgrößen zu Tage fördert. Die Mehrfachnutzung von vorgenerierten, dem jeweiligen Hersteller bekannten Geheimnissen (Basic Attestation) ist dagegen schlichtweg indiskutabel. Eine mögliche Erklärung lässt sich auch hier von der Dominanz der Technologieriesen ableiten: Intel etwa flutet seit 2008 den Markt mit seinem Secure Device Onboarding (SDO), das neben den ab Werk fest eingelassenen Schlüsseln unter anderem auch das (EC)DAA-Verfahren nutzt. Eine (Re-)Standardisierung als FIDO IoT-Spezifikation würde Unternehmen wie Intel natürlich sehr gelegen kommen. Ob Intel sich damit tatsächlich in diesem globalen Kontext der FIDO-Allianz durchsetzen wird oder ob möglicherweise progressivere Verfahren zum Tragen kommen, wird sich angesichts des sehr frühen Entwicklungsstadiums noch zeigen.

Genug progressive Alternativen gäbe es ja, wie etwa das bereits erwähnte Zero-Knowledge Initial Enrolment, das sich mit „sichere kenntnisfreie Erstanmeldung [von IoT-Geräten]“ übersetzen ließe. Kenntnisfrei bzw. Zero-Knowledge bezieht sich dabei auf die Tatsache, dass es durchaus möglich ist, eine vollständig (beidseitig) authentifizierte sowie dynamisch verschlüsselte (abgeleiteter Sitzungsschlüssel mit Vorwärtssicherheit bzw. Forward Secrecy) Sitzung mit einer IoT-Infrastruktur in der Cloud zu etablieren. Die zugrunde liegende Idee nutzt teilweise seit mehreren Jahrzehnten bekannte und bewährte Verfahren mit einer besonderen Fähigkeit: Sie sind in der Lage, eine kryptografisch verlässliche Beweisführung für den Besitz eines Geheimnisses als Authentifizierungsfaktor zu erbringen. Passender zu der Problemstellung der stark kritisierten vom Hersteller vorgegebenen festen Geheimnisse kann die Wahl kaum fallen. Ein weiterer entscheidender Unterschied zu der komfortorientierten Vorgehensweise von FIDO ist der, dass in diesem Fall ein grundsolides kryptografisches Protokoll (Secure Remo-



Quelle: PointBlank Security

Die Kommuniktion im IoT wird durch Zertifikate und TLS vollständig abgesichert.

te Password Protocol, kurz: SRP) gewählt wurde aus einer Familie von starken Verfahren (Password Authenticated Key Exchange bzw. PAKE), sodass ein nachträglicher Austausch gegen einen besseren oder effizienteren Kandidaten möglich ist. Im Übrigen stammt die passwortbezogene Namensgebung aus einer Zeit, in der Passwörter noch das Maß aller Dinge waren. Tatsächlich lassen sich einfache Passwörter (für die solche Verfahren überhaupt entwickelt wurden – um also auch mit schwachen Passwörtern eine hohe Stärke zu erzielen) gegen die zweifelsohne besseren zufällig gewählten kryptografischen Schlüssel austauschen.

Trotz der magisch anmutenden Natur von Zero-Knowledge haben auch diese Protokolle ihre Grenzen. Dem Konzept der symbiotischen Sicherheit folgend können diese allerdings mit anderen Mitteln, zum Beispiel auf der Prozessebene, abgefangen werden. Die modernen Cloud-Computing-Umgebungen bieten eine Vielzahl von starken Diensten, wozu auch Identity Provider (IdP) gehören. Eine ganzheitliche Lösung mithilfe solcher IdP könnte dann so aussehen, dass ein dazu berechtigter Mensch eine automatisierte Verarbeitung von Maschine-zu-Maschine-Kommunikation im Sinne der Erstanmeldung in der Cloud initial autorisiert – ganz ohne die für das Etablieren der sicheren Leitung notwendigen Parameter, geschweige denn Geheimnisse einsehen zu können, da dieser Vorgang sowieso auf einer niedrigeren Ebene stattfindet.

Verlässliche Verfahren

Das Zero-Knowledge-Protokoll liefert mindestens noch einen weiteren Vorteil: Der gesamte Datenaustausch findet in reinem TCP/IP statt. Da zum Zeitpunkt der Erstanmeldung von IoT-Knoten diese noch gar keine TLS-Verbindung aufbauen können (ihnen fehlen die erforderlichen Zertifikate), kommt diese Tatsache gerade recht: Die Anfangsverbindung findet authentifiziert und verschlüsselt statt (ohne TLS, aber mit vergleichbarer Sicherheit, die durch SRP erzielt wird), um über diese Brücke dynamisch erzeugte Knotenzertifikate aus der sicheren Cloud direkt (optional samt Firmware) an die IoT-Geräte auszuliefern. Die zweite, produktive Verbindung findet dann über TLS statt mit Zertifikaten, denen vollständig vertraut wird. Auch hier zeigt sich das symbiotische Denken: Wenn mit einem soliden Sicherheitsprotokoll wie TLS zunächst gewisse Grenzen erreicht werden (etwa weil es zu einem frühen Zeitpunkt noch gar nicht zur Verfügung steht), dann muss ein äquivalentes Verfahren (Zero-Knowledge bzw. SRP) geschickt eingesetzt werden, um gewissermaßen die Durststrecke zu überbrücken.

Für FIDO-IoT ließe sich diese Vorgehensweise im Übrigen auch gut einsetzen, um zu vermeiden, dass die Allianz das Rad neu erfindet, aber (wie schon am Beispiel der Basic Attestation bzw. ECDAA gesehen) nicht als einen „Run Flat Tyre“. Die Rede ist hier von dem Zurückbesinnen auf verlässliche Verfahren wie TLS, die zwar seit Jahrzehnten Wind und Wetter in Form von teilweise äußerst ausgeklügelten Angriffen ausgesetzt sind, aber dennoch im Kern nach wie vor wie ein Fels in der Brandung stehen (siehe Abbildung).

Die Abbildung auf Seite 14 zeigt verschiedene Schritte, wobei ZK für Zero-Knowledge bzw. ZKIE für Zero-Knowledge Initial Enrolment steht. Ausgehend von der Beobachtung, dass ein Attestation Certificate das Wort Zertifikat schon im Namen trägt und dass den Authenticator-Schlüsseln serverseitig ganz wie bei einer Stammzertifizierungsstelle das Vertrauen ausgesprochen wird (diesmal allerdings dynamisch und nicht über die vorgefertigten Schlüssel), ergeben sich die grün markierten Pfade: Die jeweiligen Knoten verfügen bis dahin über gegenseitiges Vertrauen mit Zertifikaten und können es folgerichtig im Zusammenhang mit TLS nutzen, um die Kommunikation vollständig abzusichern. Da bekanntlich mehrere Wege nach Rom führen, ist es dann denkbar, dass Benutzer entweder direkt IoT-Geräte nach vorhergehender verbesserter FIDO-Authentifizierung steuern, oder aber sie gehen den bereits bestehenden Umweg über die Cloud. Dort stehen klassische IoT-Komponenten wie der IoT Hub bereit, um letztlich nur noch die Steuerdaten an die angeschlossenen Knoten zu vermitteln.

Zwar ist ein solcher Ansatz für die Cloud-Umgebungen minimalinvasiv, doch auch er erfordert zwingend eine solide PKI bzw. Stammzertifizierungsstelle, die zudem multimandantenfähig sein sowie über den branchenüblichen Hardwareschlüsselschutz (z.B. Azure Key Vault) verfügen sollte. Eine solche Komponente lässt zumindest Microsoft bislang noch vermissen, was aber nicht bedeutet, dass es mit vertretbarem Aufwand nicht möglich wäre, eine CA (Certificate Authority) selbst aufzusetzen.

Der Wetterbericht oder „Security by Forecast“

Nach „Security by Design“ und „Security by Obscurity“ kommen wir abschließend auf „Security by Forecast“ zu sprechen, um dem Ganzen einen Ausblick zu verleihen. Quantencomputer sind mittlerweile in aller Munde. Ohne dabei zu sehr ins Detail zu gehen, können wir konstatieren, dass die Bastionen der heutigen Kryptografie wie etwa RSA oder auch elliptische Kurven fallen würden, sobald diese neuartigen Rechenmaschinen die nötige Komplexität erreichen. Wir können heute noch gar nicht so genau sagen, wann diese Schallmauer erreicht wird. Trotzdem werden schon jetzt folgenschwere Entscheidungen auf nationaler Ebene getroffen.

Die NSA etwa hat bereits 2015 ihren Blick (und den sämtlicher von ihrer Vorgabe abhängigen nationalen Institutionen) auf Quantencomputer gerichtet. Zwar hat das NIST kurz danach einen Standardisierungsprozess für quantencomputerresistente Verfahren angekündigt, gestartet wurde er allerdings noch ein Jahr später (2017). Das allein waren schon zwei Jahre, in denen die angesprochenen Institutionen und Sicherheitssysteme der USA auf elliptische Kurven verzichten mussten. Paradoxerweise fordert die aufkommende neue TLS-Spezifikation 1.3 genau diese und zwingt einen regelrecht dazu, das klassische RSA aufs Abstellgleis zu schicken – welches im Übrigen unter Beachtung sämtlicher kritischer Parameter immer noch als sicher gilt.

Das BSI schreibt in seinem technischen Leitfaden für kryptografische Schlüssellängen (BSI TR-02102-1) interessanterweise, dass Vorhersagen (Forecasts), die über sechs bis sieben Jahre in die Zukunft blicken, insbesondere bei asymmetrischen Verfahren (die am meisten von Quantencomputern bedroht sind) wenig bis gar nicht praktikabel sind. Dafür kann in einem solchen Zeitraum zu viel passieren. Allerdings haben wir mit Verfahren wie TLS oder SRP große Vertreter von Sicherheitsprotokollen, die sich seit über 20 Jahren wacker schlagen. Da liegt es nahe, die goldene Mitte zu suchen und Sicherheitsarchitekturen auf deren Basis gemäß dem „Security by Design“-Prinzip zu entwerfen bzw. zu verbessern, statt neue ungetestete Lösungen ins Rennen zu schicken, die Augen vor altbekannten Lücken zu verschließen oder entscheidende Komponenten zu verschleiern.

Vielleicht würde sich auch eine DIN-Norm an der Stelle gut machen, um die Fahne der „IT-Security made in Germany“ hochzuhalten. Die ersten Lösungen aus Deutschland gibt es jedenfalls schon und auch weltweit, wie das Beispiel der FIDO-Allianz zeigt, sind wir noch ziemlich am Anfang.

Witali Bartsch
PointBlank Security

Die Admins müssen leider draußen bleiben

Ein technisches Maßnahmenpaket beschränkt den privilegierten Zugriff

Privilegierte Zugriffsberechtigungen bergen zahlreiche Risiken und können Unternehmen im Ernstfall teuer zu stehen kommen. Durch versiegelte IT-Infrastrukturen lassen sich die Rechte von Administratoren soweit eindämmen, dass sensible Daten jederzeit zuverlässig geschützt sind.

Administratoren wandeln auf einem schmalen Grat: Auf der einen Seite steht der reibungslose Betrieb von Hard- und Software, auf der anderen geht es um Datenschutz und Informationssicherheit. Sie sind dafür verantwortlich, dass der Betrieb möglichst störungsfrei erfolgt. Mit dieser Aufgabe sind etliche Privilegien verbunden: Admins haben nicht nur die Möglichkeit, Konfigurationen am Server zu verändern, sie können auch Speicherinhalte auslesen. Zudem sind sie in der Lage, auf die auf dem Server verarbeiteten Daten zuzugreifen – ein Umstand, der Unternehmen schnell teuer zu stehen kommen kann (vgl. Art. 83 DSGVO). Das als „Versiegelung" bezeichnete Maßnahmenpaket (auch Sealed Computing) soll diese Privilegien eindämmen und privilegierte Zugriffe zuverlässig ausschließen – und das mit rein technischen Mitteln. Auf diese Weise lassen sich nicht nur einzelne Server, sondern ganze IT-Infrastrukturen absichern.

Organisatorische Maßnahmen reichen nicht aus

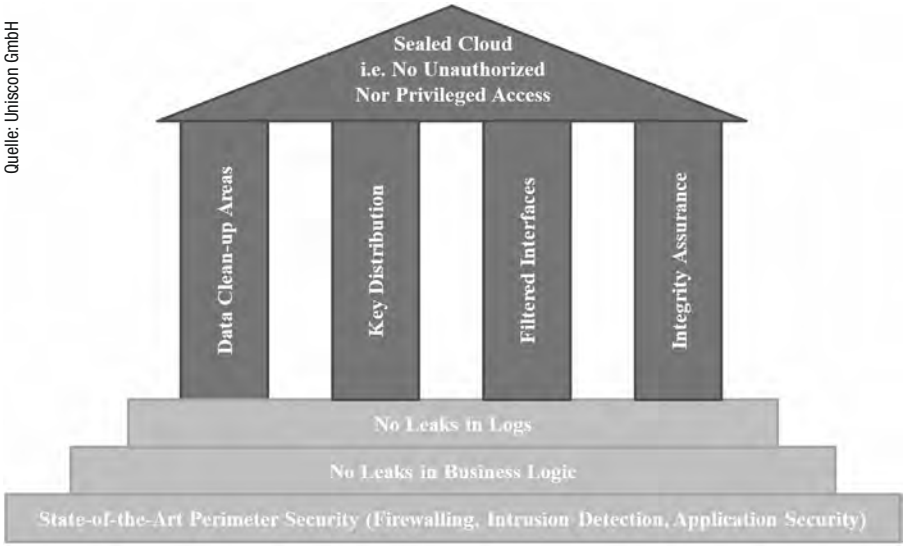
Üblicherweise setzen Anbieter von Cloud-Lösungen auf ein Zusammenspiel aus technischen und organisatorischen Maßnahmen, um unerwünschte Datenzugriffe oder Angriffe zu unterbinden. Organisatorische Maßnahmen wie Rollen- und Rechtekonzepte oder eine lückenlose Überwachung lassen sich allerdings mit verhältnismäßig wenig Aufwand umgehen: Interne Angreifer – etwa Mitarbeiter des Dienstbetreibers oder Admins – könnten sich unbefugt Zugriff zu Daten verschaffen und diese anschließend manipulieren oder entwenden. Ein rein technischer Schutz vor solchen Insider-Angriffen wäre daher ein konstruktiver Grundpfeiler des sicheren Cloud-Computing.

Bei allen Cloud-Anwendungen ist es selbstverständlich, dass die Daten während der Übertragung von den Geräten der Cloud-Nutzer zur Cloud-Infrastruktur verschlüsselt sind. Die Absicherung der Daten gegen Diebstahl aus den Speichermedien unter Zuhilfenahme von Verschlüsselung ist ebenfalls bewährte Geschäftspraxis. Die Daten sind also während der Übertragung („data on the move") und während der Speicherung („data at rest") hinreichend abgesichert. Bei der Verarbeitung in den Cloud-Servern („data in use") müssen die Daten jedoch zwangsläufig unverschlüsselt vorliegen. Sie sind dann dort quasi ungeschützt dem Zugriff durch Administratoren, den Betreiber des Rechenzentrums und seine Mitarbeiter ausgesetzt.

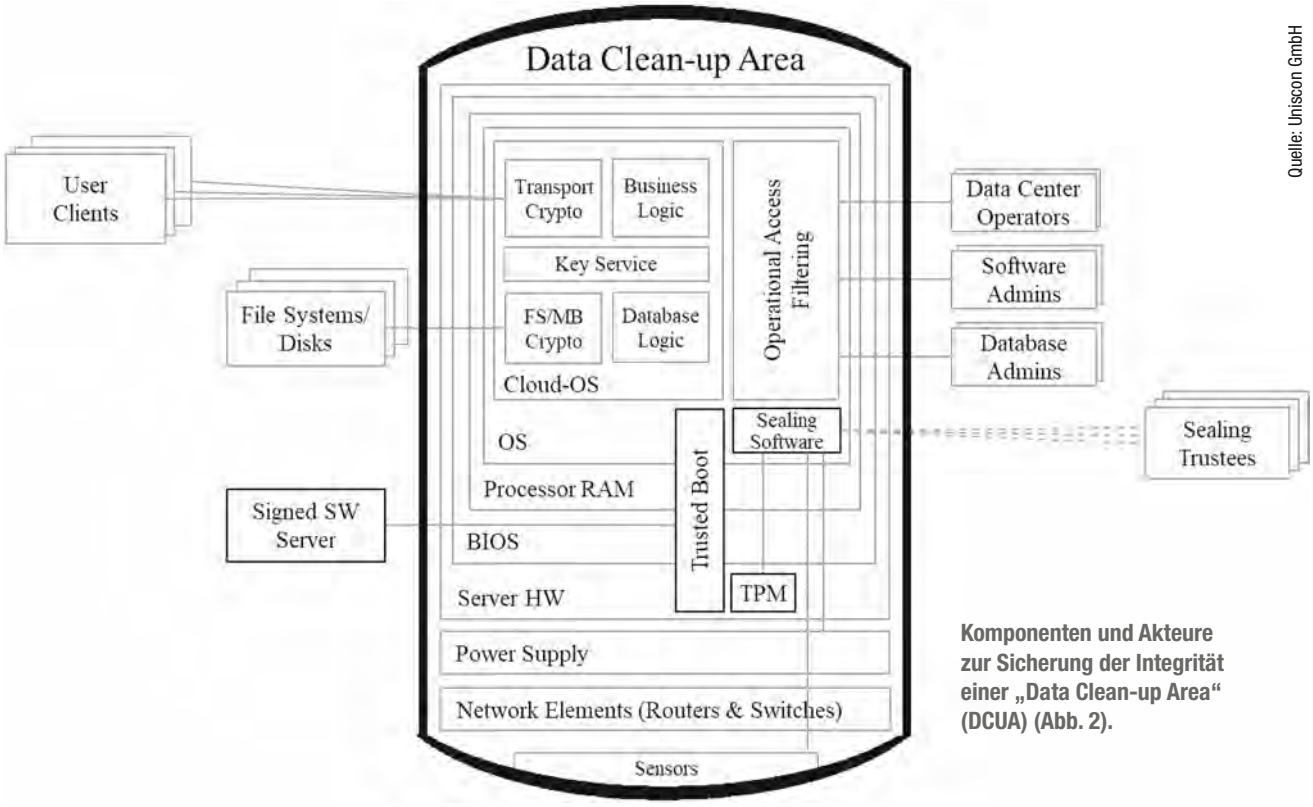
Versiegelte Infrastrukturen verhindern privilegierten Zugriff

Beim Sealed Computing ist das hingegen anders: Die Cloud-Server werden in einer Kapsel betrieben, welche die Daten während der Verarbeitung vor jeglichem Zugriff schützt. Diese Kapsel ist rein technisch reali-

Quelle: Uniscon GmbH



Überblick zum Satz der Maßnahmen, mit dem nicht nur der unbefugte, sondern auch der privilegierte Zugriff und jede Möglichkeit zur Kenntnisnahme von verarbeiteten Daten ausgeschlossen werden können (Abb. 1).



Quelle: Uniscon GmbH

Komponenten und Akteure zur Sicherung der Integrität einer „Data Clean-up Area" (DCUA) (Abb. 2).

siert. Bei herkömmlichen Cloud-Lösungen kann etwa durch einen einfachen Verstoß gegen organisatorische Vorschriften ein unbefugter Zugriff auf die verarbeiteten Daten erfolgen, oft sogar unbeobachtet. Im Falle der nachfolgend beschriebenen Infrastrukturen ist das jedoch nicht möglich, da die organisatorischen Schutzmaßnahmen durch technische ersetzt wurden. Auf diese Weise sind selbst der Betreiber des Dienstes und seine Mitarbeiter und natürlich auch die Administratoren zuverlässig vom Zugriff auf die Daten ausgeschlossen.

Clouds mit versiegelten Infrastrukturen sind bereits seit mehreren Jahren in deutschen Unternehmen im Einsatz. Exemplarisch seien hier die Cloud-Dienste „ucloud" des Aachener Providers regio iT und die „Versiegelte Cloud" der Deutschen Telekom genannt. Mit der „Sealed Platform" der Münchner TÜV-SÜD-Tochter Uniscon existiert außerdem eine Cloud-Plattform, die explizit für den Betrieb sicherheitskritischer Business-Applikationen ausgelegt ist.

Technische Umsetzung einer versiegelten IT-Umgebung

Um den privilegierten Datenzugriff in einer Cloud wirkungsvoll auszuschließen, müssen vier Voraussetzungen erfüllt sein, denen die folgenden vier technischen Maßnahmenpakete entsprechen:

Data Clean-up Areas: Im Kern der versiegelten Infrastruktur befinden sich die „Data Clean-up Areas" (DCUA). Das sind gekapselte Zonen beziehungsweise Segmente eines Rechenzentrums, die jeweils mit einer Vielzahl von Anwendungsservern in hoher Dichte bestückt sind. Jede DCUA ist mit elektromechanischen Käfigen und einem Netz an Sensoren so gesichert, dass kein Zugriff – weder physisch vor Ort, noch logisch über eine der elektronischen Schnittstellen – möglich ist, ohne einen Alarm auszulösen. Sobald das Eindringen eines Angreifers durch die Sensoren erfasst und ein Alarm ausgelöst wird, beginnt unverzüglich der Data-Clean-up-Prozess. Dieser lässt sich alternativ auch direkt durch die Anmeldung eines Wartungsganges auslösen. In beiden Fällen werden die zwischen den Nutzern und der Cloud bestehenden Sitzungen auf andere, nicht betroffene DCUA verschoben und die Daten in der vom Clean-up betroffenen DCUA gelöscht.

Schlüsselverteilung: Damit Administratoren oder Rechenzentrumsbetreiber die verschlüsselt gespeicherten Daten nicht lesen können, werden die Schlüssel aus Geheimnissen der Cloud-Nutzer, wie etwa deren Zugangsdaten, oder ganz automatisch innerhalb der DCUA erzeugt. Auf diese Weise sind sie keiner natürlichen Person zugänglich und verlassen nie den gesicherten Verbund der DCUA. Eine solche sichere Aufbewahrung ist für eine überschaubare Zahl an Schlüsseln beispielsweise mithilfe der „Trusted Platform Module" und im größeren Stil in den flüchtigen Speichern der Server eines Clusters von DCUA, also der Zusammenschaltung mehrerer DCUA zu einem Netz möglich, welches auch „Sealed Trust Anchor Network" (STAN) genannt wird.

Filtered Interfaces: Die existierenden Serverschnittstellen müssen als „Filter" gestaltet sein, damit nur eine definierte Liste von Befehlen angenommen wird. Für diese Befehle gilt, dass deren Ausführung zu keinem Export von Nutzerdaten führen darf. Auch dürfen die Statusmeldungen und Log-Dateien keine Daten enthalten, die Rückschlüsse auf Nutzerdaten erlauben. Aus diesem Grund sind herkömmliche Wartungszugänge wie etwa die Secure Shell (SSH) abgeschaltet. Die notwendigen Funktionen stehen stattdessen über eine „Operations and Maintenance Access" (OMA) genannte spezielle Filterkomponente zur Verfügung.

Integrity Assurance: Abschließend stellt ein Attestierungsprozess den sicheren Betriebszustand der Infrastruktur her. Dieser besteht aus

einer fachgerechten Prüfung und Schließung der Data Clean-up Areas sowie der abschließenden Eingabe von nur den Versiegelungsstellen bekannten Geheimnissen. Die Versiegelung wird von mehreren, voneinander unabhängig agierenden Stellen, den sogenannten „Sealing Trustees“, vorgenommen. Je mehr dieser Stellen beteiligt sind und je unabhängiger sie voneinander handeln können, desto höher ist die Vertrauenswürdigkeit der Versiegelung.

Zusätzliche Eigenschaften auf Anwendungsebene

Diese vier eng miteinander verzahnten technischen Maßnahmenpakete bilden eine solide Grundlage für die Sicherheit der Daten in der Cloud. Allerdings sind noch einige zusätzliche Eigenschaften auf der Anwendungsebene notwendig, um einen privilegierten Zugriff vonseiten (unberechtigter) Dritter in der Cloud-Infrastruktur zuverlässig und überprüfungssicher auszuschließen:

- Um die Schutzfunktion der Versiegelung nicht zu unterlaufen, darf die in der Cloud betriebene Software keinerlei Lecks in den Log-Dateien enthalten. Die Konfiguration der Log-Funktion ist dementsprechend so einzustellen, dass keine Nutzerdaten und keine Daten, die Rückschlüsse auf solche ermöglichen, enthalten sind.
- Darüber hinaus darf kein fahrlässig oder vorsätzlich in der Anwendungslogik verankerter Code existieren, der solche Daten aus der Cloud exportiert.
- Dasselbe gilt für bekannte Sicherheitslücken und Angriffsmöglichkeiten in der Anwendungslogik. Daher ist der Stand der Technik in Bezug auf die Anwendungssicherheit und gegen Angriffe von externen Angreifern im Allgemeinen einzuhalten, regelmäßig zu überprüfen und – wenn nötig – nachzubessern.

Sealed Computing – weitere Ansätze und ein Ausblick

Die oben beschriebenen Kapseln um ganze Servergruppen (DCUA) sind nicht der einzige Ansatz, um Administratoren von privilegierten Zugriffen auszuschließen. Weitere Beispiele für ähnliche Technologien stammen von den großen Prozessorherstellern Intel und AMD. Konkret handelt es sich dabei um Intels „Software Guard Extensions“ (SGX) und AMDs „Secure Encrypted Virtualization“ (SEV). Beide Technologien sehen vor, dass die schützenswerten Daten innerhalb der Prozessorkerne unverschlüsselt verarbeitet werden, außerhalb dieser, also bereits auf dem Systembus und dem Arbeitsspeicher (RAM), jedoch nur verschlüsselt vorliegen.

Durch Arbeiten im Rahmen des Marie-Curie-Research Networks „Privacy & Usability“ etablierte sich mittlerweile „Sealed Computing“ bzw. „Sealed Computation“ als Oberbegriff der Technologien Sealed Cloud, SGX und SEV; darüber hinaus ist in diesem Zusammenhang auch von „Confidential Computing“ die Rede. Mittelfristig ist zu erwarten, dass sich die verschiedenen Technologien ergänzen, da die Versiegelung auf Prozessorebene besser gegen Exploits auf der Ebene der Systemsoftware und die Versiegelung auf Serverebene besser gegen Exploits in der Hardware schützt.

Dr. Hubert Jäger
CTO (Geschäftsführer) Uniscon GmbH

Impressum
Themenbeilage Sicherheit & Datenschutz

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

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

Autoren dieser Ausgabe:
Witali Bartsch, Dr. Falk Herrmann, Dr. Hubert Jäger, Dr. Holger Mühlbauer, Marco Schmid, Tobias Theelen

DTP-Produktion:
Lisa Hemmerling, Matthias Timm, Heise Medienwerk GmbH & Co. KG, Rostock

Korrektorat:
Marei Stade, Heise Medienwerk GmbH & Co. KG, Rostock

Titelbild:
© shutterstock, piick

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

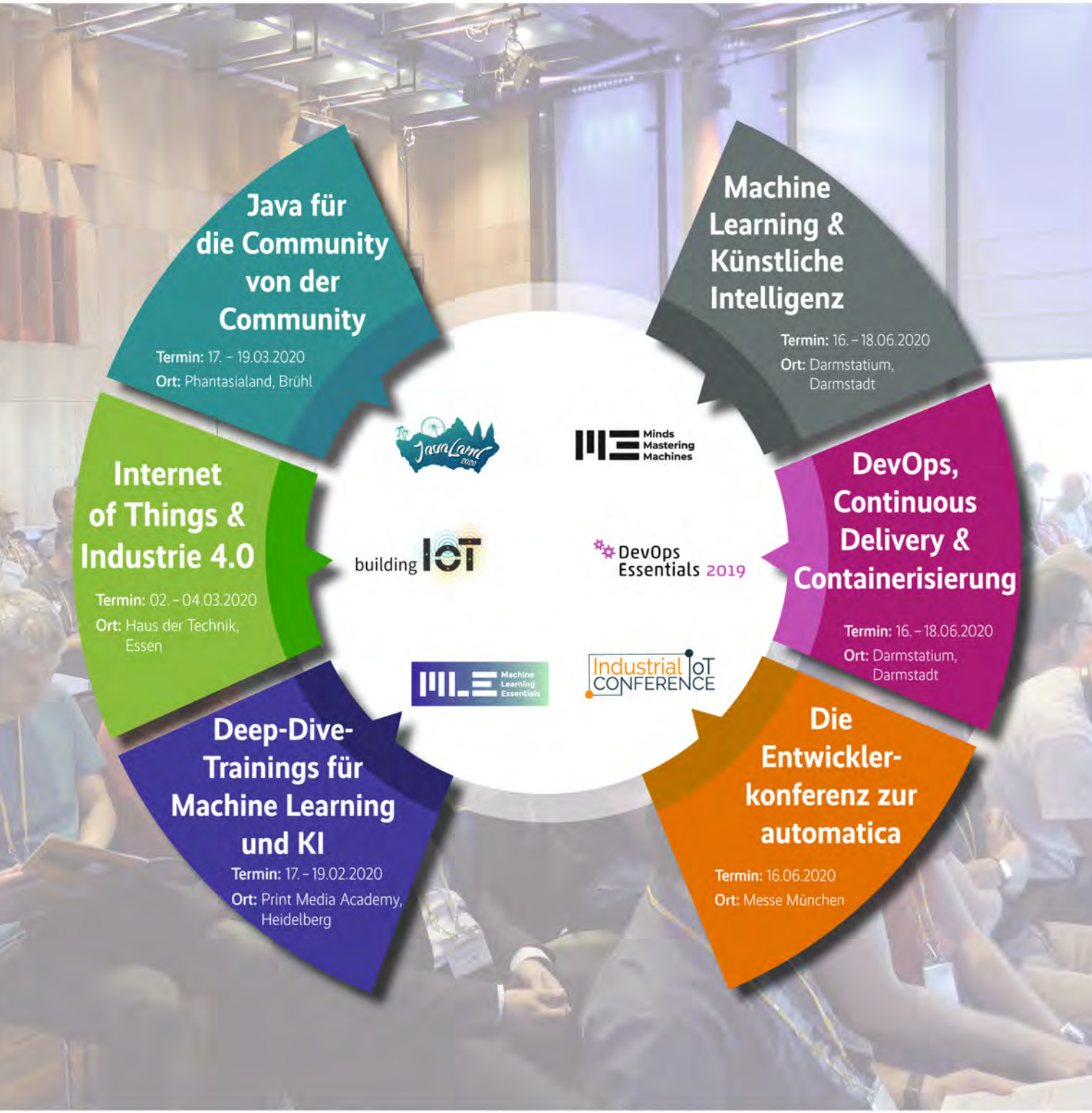
Leiter Vetrieb und Marketing:
André Lux

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

Die Inserenten

Die hier abgedruckten Seitenzahlen sind nicht verbindlich. Redaktionelle Gründe können Änderungen erforderlich machen.

DEVELOPER-KONFERENZEN + -WORKSHOPS 2020



Java für die Community von der Community

Termin: 17. – 19.03.2020
Ort: Phantasialand, Brühl

Machine Learning & Künstliche Intelligenz

Termin: 16. – 18.06.2020
Ort: Darmstatium, Darmstadt

Internet of Things & Industrie 4.0

Termin: 02. – 04.03.2020
Ort: Haus der Technik, Essen

DevOps, Continuous Delivery & Containerisierung

Termin: 16. – 18.06.2020
Ort: Darmstatium, Darmstadt

Deep-Dive-Trainings für Machine Learning und KI

Termin: 17. – 19.02.2020
Ort: Print Media Academy, Heidelberg

Die Entwickler-konferenz zur automatica

Termin: 16.06.2020
Ort: Messe München

JavaLand 2020 · Minds Mastering Machines · building IoT · DevOps Essentials 2019 · Machine Learning Essentials · Industrial IoT CONFERENCE

Veranstalter: iX · heise Developer · dpunkt.verlag

Weitere Informationen unter:

www.heise.de/developer/

Managed Threat Response

Andere informieren Sie nur über Bedrohungen. Wir werden aktiv.

Mit Sophos MTR erhält Ihr Unternehmen 24/7 Managed Detection and Response mit aktiver Bekämpfung von Bedrohungen durch ein Expertenteam, als Fully-Managed-Service.

JETZT INFORMIEREN
www.sophos.de/mtr

SOPHOS

Die Evolution der Cybersecurity.