Eine Themenbeilage der
Heise Medien GmbH & Co. KG

I
2016

SICHERHEIT & DATENSCHUTZ

Authentifizierung, Rechtsnormen und Industrie 4.0

Security Awareness:
Was unser Bauchgefühl für gefährlich hält

IT-Sicherheitsgesetz & NIS-Richtlinie:
Welche KRITIS-Betreiber nachbessern müssen

Mobile Security:
Wie man BYOD-Risiken in den Griff bekommt

Industrial Security:
Wer in der Industrie 4.0 für Sicherheit sorgt

Telemediengesetz:
Was Website-Betreiber nicht verschlafen sollten

www.it-security-und-management.de

powered by: TeleTrusT Pioneers in IT security. iX

Eine Veranstaltung von heise Events

Bis zum 21. Juli 15 % Frühbucherrabatt sichern!

6. Bremer IT-Sicherheitstag

IT-Sicherheit – Auf dem Stand der Technik

Das am 25.07.2015 in Kraft getretene Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (ITSiG) schreibt den Betreibern von kritischen Infrastrukturen vor, zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse angemessene organisatorische und technische Vorkehrungen nach dem „Stand der Technik“ zu treffen.

Im Rahmen des 6. Bremer IT-Sicherheitstages beleuchten Fachleute anhand ausgewählter Szenarien den „Stand der Technik“ und liefern Anregungen für die Umsetzung in der Praxis.

Zeit und Ort: 1. September 2016, Bremen

Themenschwerpunkte:

- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (ITSiG)
- Sicherung kritischer Infrastrukturen
- Gewährleistung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von IT-Systemen

Frühbucherticket (bis 21. Juli): 123,50 EURO (inkl. MwSt.) **Standardticket:** 145,00 Euro (inkl. MwSt.)

Gold-Sponsoren: dacoso data communication solutions, ADVA, BOMGAR, IBS

Silber-Sponsoren: ectacom, NEROSOFT, KASPERSKY lab

Organisiert von: heise Events

In Zusammenarbeit mit: IS-BREMEN

Weitere Informationen und Anmeldung unter: **www.heise-events.de/bremerITST6**

Starker Schutz tut not

Liebe Leserinnen und Leser,

die Meldungen über Sicherheitslecks und erfolgreiche Hackerangriffe reißen nicht ab. So sind seit Längerem Verschlüsselungstrojaner wie „Locky“ aktiv und erpressen das Geld der Betroffenen. Selbst vor Krankenhäusern machen Hacker nicht Halt. Jüngst wurden Computerviren auf Rechnern eines deutschen Atomkraftwerks entdeckt. Laut Betreiber war zwar kein kritisches System betroffen und die Bevölkerung nicht in Gefahr. Dennoch zeigt dies, dass auch Systeme, die nicht am Internet hängen, durch das Verhalten der Nutzer gefährdet sein können.

Die Verantwortung für IT-Sicherheit bedarf also eines umfassenden Ansatzes und muss branchenübergreifend als Herausforderung begriffen werden. Sie sollte in Unternehmen auf Geschäftsführerebene angesiedelt sein, jedoch die Praxis sieht vielerorts anders aus.

Was im Falle der „Panama Papers“ zweifelhafte Strukturen offenlegt und bestenfalls für mehr Transparenz sorgt, kann in anderen Fällen für viele Unternehmen bedeuten, Forschungsergebnisse und Geschäftsgeheimnisse zu verlieren. Nicht selten ist so die blanke Existenz bedroht. Es zeigt sich, dass Sicherheit immer aus einer Kette verschiedener Glieder besteht. Deshalb reicht es nicht aus, nur die IT-Systeme so sicher wie möglich zu gestalten. Auch die Anwender müssen sich richtig verhalten und entsprechend geschult werden.

Im Falle kritischer Infrastrukturen – etwa dem gehackten Atomkraftwerk – kann die Allgemeinheit und jeder einzelne Bürger immens betroffen sein. Der deutsche Gesetzgeber hat dies erkannt und mit dem IT-Sicherheitsgesetz ein Vorsorgeinstrument geschaffen. Analog zu IT-Sicherheit und technologischer Entwicklung muss aber auch die Gesetzgebung als fortlaufender Prozess verstanden werden. Systeme müssen nach dem „Stand der Technik“ abgesichert werden. Das klingt gut und richtig, aber was bedeutet das eigentlich genau?

Die vorliegende Beilage „Sicherheit & Datenschutz“ will Ihnen Einblick in ausgewählte Themen der IT-Sicherheit verschaffen, die uns als Bundesverband IT-Sicherheit derzeit beschäftigen. Unsere Beiträge zielen dabei auf grundsätzliche Fragen ab, mit denen Sie sich als IT-Verantwortlicher befassen sollten. Neben den rechtlichen Rahmenbedingungen und den Auswirkungen des „IT-Sicherheitsgesetzes“ (S. 16), der angekündigten „NIS-Richtlinien“ (S. 7) und der „eIDAS-Verordnung“ (S. 18) geben wir Ihnen Praxisbeispiele zur IT-Sicherheit im Bereich „Mitarbeiterfortbildung und Industrie 4.0“ (S. 14).

Themen wie „Awareness“ (S. 4) und „Access Control“ (S. 20) sollen ebenfalls nicht zu kurz kommen. Abgerundet wird die Beilage durch Beiträge zum „Mobile-Device-Management“ (S. 11) und der „Zukunft der Verschlüsselung“ (S. 24).

Allen Herausforderungen zum Trotz ist ein starker Schutz möglich. Die mittelständisch geprägte deutsche IT-Sicherheitsbranche ist sehr gut aufgestellt und besitzt durch innovative Produkte – gepaart mit der starken deutschen Datenschutzgesetzgebung – ein Alleinstellungsmerkmal. „IT Security made in Germany“ ist Garant für hohe Schutzstandards. Auch wenn Angreifer scharfe Schwerter einsetzen, die richtigen Schutzschilder sind verfügbar.

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

Inhalt

Risikobewertung aus dem Bauch heraus

Bei der Einschätzung von IT-Risiken spielen psychologische Faktoren eine große Rolle

Manchmal können zierliche Pekinesen gefährlicher sein als stämmige Pitbulls. Gerade beim Thema IT-Sicherheit sollte man die Tücken der subjektiven Risikowahrnehmung kennen. Denn ihr Einfluss auf das Sicherheitsbewusstsein ist genauso beachtenswert wie die Ergebnisse statistischer Berechnungen.

Beim Thema IT-Sicherheit gibt es oft eine bemerkenswerte Diskrepanz zwischen der Verbreitung von verschiedenen technischen Sicherheitsmaßnahmen in Unternehmen und Behörden und der immer wieder in diversen Erhebungen belegten tatsächlichen Bedrohungslage. Untersucht man dieses Missverhältnis eingehender, wird schnell deutlich, dass psychologische Phänomene bei der Risikowahrnehmung eine große Rolle spielen. Der Bauch siegt bei der Entscheidung für oder gegen eine Sicherheitsmaßnahme oft über den Kopf – nicht selten mit fatalen Konsequenzen.

Die gefühlte Bedrohung

„Die Risiken, die uns umbringen, sind nicht immer die, vor denen wir uns fürchten und über die wir uns aufregen." Mit diesem Statement in seinem Artikel „Facing public outrage" bringt der Kommunikationswissenschaftler Peter M. Sandman seine Theorie des „Outrage" (Empörung) bei der subjektiven Risikowahrnehmung auf den Punkt. Genauer ist damit gemeint, dass emotionale Faktoren wie Wut und Bestürzung, aber auch Neugier oder die Aussicht auf Lustgewinn, beispielsweise beim Rauchen oder beim Konsum von Alkohol, einen großen Einfluss darauf ausüben, wie Menschen Gefährdungspotenziale einschätzen und wie sie darauf reagieren. Das gilt für IT-Risiken wie für alle anderen möglichen Gefahren des täglichen Lebens auch. Zieht man in Betracht, dass eine Risikoanalyse zu den Grundlagen jedes Informationssicherheitsmanagementsystems (ISMS) – insbesondere nach dem internationalen Standard ISO 27001 – zählt, lohnt ein tiefergehender Blick auf die irrationale, also emotionale Seite der Risikowahrnehmung allemal.

Ein Beispiel aus dem Alltagsleben mag die Diskrepanz zwischen subjektiver Einschätzung und objektiver Wahrscheinlichkeit illustrieren: Statistisch gesehen beißen Pekinesen weitaus häufiger zu als die gefürchteten Pitbulls, und zwar unabhängig von der jeweiligen Verbreitung der Hunderasse. Das ist durch etliche wissenschaftliche Studien, etwa der „Analysis of Dog Bites in Children Who Are Younger Than 17 Years" der Medizinischen Universität Graz, mehrfach belegt. Da aber die Vorstellung, Opfer eines Pitbull-Angriffs zu werden, ein weitaus größeres Schreckenspotenzial birgt, als jene, von einem niedlichen kleinen Pekinesen gebissen zu werden, erscheint uns das Risiko beim Pitbull sehr viel größer. Wie furchterregend ein mögliches Ereignis auf uns wirkt, ist ein Schlüsselfaktor des Outrage-Modells.

Die so gerne angewandte Formel *Risiko = Eintrittswahrscheinlichkeit x Schadensausmaß* mag in der Welt von Zahlen, Daten, Fakten und Versicherungspolicen ihre Berechtigung haben. Sie liefert jedoch keine adäquate Beschreibung für individuell wahrgenommene Risiken. Denn in der subjektiven Einschätzung sind die Faktoren Eintrittswahrscheinlichkeit und Schadensausmaß eben nicht gleichberechtigt, vielmehr übt das (nicht messbare) furchterregende Ausmaß eines potenziellen Schadens einen ungleich größeren Einfluss auf unsere Psyche aus, als die (berechenbare) Eintrittswahrscheinlichkeit.

Einen wichtigen Einflussfaktor stellt zudem der Status von (theoretischen) Kontrollmöglichkeiten dar. Während wir zum Beispiel täglich unbekümmert Auto fahren und keinen Gedanken an Unfallstatistiken und die hohe Zahl von Todesopfern auf unseren Straßen verschwenden, beschleicht uns ein mulmiges Gefühl, wenn wir ins Flugzeug steigen und dem Geschick des Piloten ausgeliefert sind.

Bauch- und Kopfmenschen

In der Risikoforschung unterscheidet man zwischen der Bewertung von Risiken durch Laien und durch Experten. Damit ist allerdings keine Wertung der jeweiligen Stichhaltigkeit einer Einschätzung gemeint, sondern lediglich, ob die Beschäftigung mit dem Risiko auf messbaren Daten (Experten) oder eher auf emotionalen Faktoren (Laien) beruht. Es hat sich häufig genug gezeigt, dass für eine angemessene Risikobewertung und das daraus abgeleitete Handeln beide Perspektiven berücksichtigt werden sollten. Denn beide Sichtweisen existieren nicht unabhängig nebeneinander, sondern sie beeinflussen sich gegenseitig. Führt beispielsweise ein gefühltes hohes Risiko in einer größeren Gruppe zu einer Vermeidungsstrategie, so resultiert daraus unter Umständen ein Rückgang in der Schadensstatistik der Experten. Diese wiederum errechnen daraus ein abnehmendes Risiko.

SCHLÜSSELFAKTOREN DES OUTRAGE-MODELLS

Outrage fördernd	Outrage abmildernd
Unfreiwilligkeit	Freiwilligkeit
Fremdheit	Vertrautheit
Furchterregend	Nicht furchterregend
Diffuse Verteilung in Raum und Zeit	Fixierung in Raum und Zeit
Kontrolliert durch System	Kontrolliert durch Individuum
Unfair	Fair
Moralisch relevant	Moralisch irrelevant

Mobile Geräte sicher in die Unternehmens-IT einbinden

Während Server und PCs automatisch der Kontrolle der IT unterstehen und fest eingebunden sind, müssen bei der Verwaltung mobiler Geräte andere Gefahren und Herausforderungen betrachtet werden. Die meisten heute populären Smartphones und Tablets wurden ursprünglich für Privatanwender entwickelt. Infolgedessen nehmen die Managementmöglichkeiten mobiler Betriebssysteme erst allmählich zu und sind anders als für PCs. Dazu kommt: Administratoren müssen in der Regel mehrere Mobilplattformen unterstützen, die Geräte einrichten und sicher konfigurieren. Ein sicheres und effizientes Enterprise-Mobility-Management (EMM) gehört deshalb inzwischen zu einer der wichtigsten Aufgaben für IT-Abteilungen.

Was bringt eine Enterprise-Mobility-Management-Lösung?

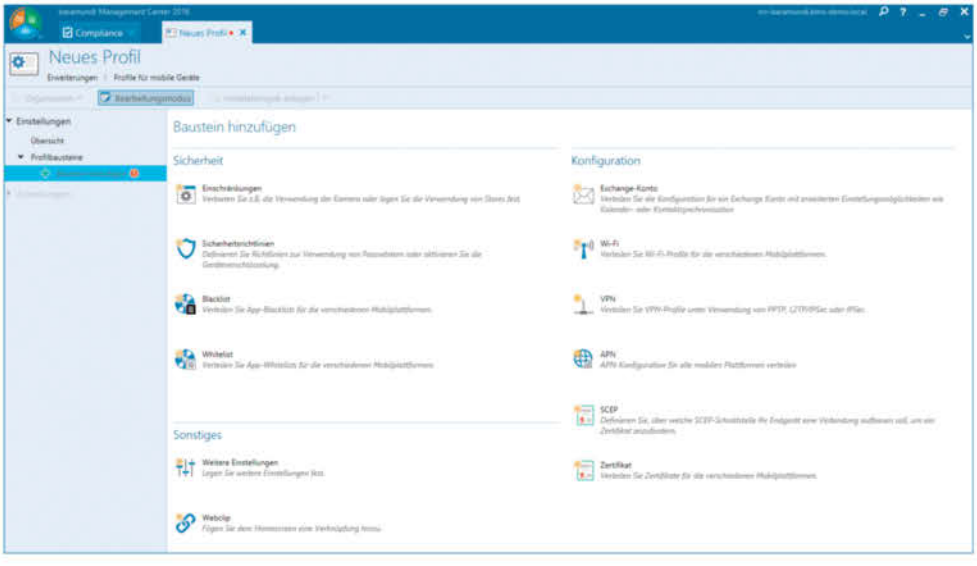
Vergleicht man die drei gängigsten Mobilplattformen iOS, Android und Windows Mobile, zeigt sich schnell, dass dieselben Parameter wie beispielsweise Name, E-Mail-Adresse, Server oder Domäne für die Einrichtung von Exchange-Konten an jeweils unterschiedlichen Stellen eingegeben werden müssen. Für die Praxis bedeutet das einen hohen Aufwand und setzt voraus, dass der Administrator sich mit allen Eingabemasken beschäftigt. Hier hilft eine Verwaltungssoftware, den Aufwand für das Management der mobilen Geräte zu reduzieren und effizienter zu gestalten. Besonders wichtig bei einer Enterprise-Mobility-Management-Lösung ist, dass auch hier die Vorgaben des Deutschen Datenschutzes eingehalten werden und keine Daten über die Nutzer erhoben werden, die dagegen verstoßen. So wäre es beispielsweise nicht ohne weiteres zulässig über eine MDM-Lösung Daten zu erheben, wo sich ein Nutzer zu einer bestimmten Zeit aufhält. Mit einem deutschen Anbieter, der darauf Rücksicht nimmt, ist man hier auf der sicheren Seite.

Einfaches Enrollment in die Management-Lösung

Das mobile Gerät wird einmalig in die Enterprise-Mobility-Management-Lösung aufgenommen, zum Beispiel durch das Scannen eines bereitgestellten Barcodes. Nach dem Enrollment kann der Administrator Managementaufgaben wie beispielsweise die Exchange-Konfiguration oder App Black- bzw. Whitelisting zentral durchführen. Dazu setzt er die Einstellungen zentral und verteilt diese dann über das Internet auf alle mobilen Geräte. Die Mitarbeiter müssen nicht extra dem Administrator das Gerät zur Verfügung stellen, damit dieser die Einstellungen manuell vornimmt. Für den Administrator verringert das Arbeiten mit nur noch einer Oberfläche die Komplexität, spart Zeit und reduziert die Fehleranfälligkeit des Prozesses.

Mobile Geräte absichern

IT-Verantwortliche sollten außerdem berücksichtigen, dass mobile Geräte leichter abhandenkommen können als ein PC. Hierfür müssen entsprechende Vorkehrungen getroffen werden. In Betracht kommen beispielsweise das automatische Sperren beim Ausschalten des Bildschirms, die Möglichkeit, das vergebene Profil auch aus der Ferne zu löschen und nicht zuletzt die Vergabe starker Passwörter. Weiterhin muss sichergestellt sein, dass der Administrator die Geräte jederzeit im Blick hat und beispielsweise informiert wird, wenn ein Nutzer das Betriebssystem kompromittiert (per Jailbreak bzw. Rooting).
Aus diesem Grund sollte eine EMM-Lösung die Möglichkeit bieten, Compliance-Regeln zu definieren, welche dann automatisch und regelmäßig geprüft werden. Bei Verstößen wird der Administrator informiert und hat dann die Möglichkeit, Gegenmaßnahmen, wie eine E-Mail an den Nutzer bis hin zum Komplett-Löschen aus der Ferne, zu ergreifen.
Die sichere Einbindung von mobilen Geräten in die Unternehmens-IT ist ein wichtiger Baustein einer umfassenden Sicherheitsstrategie und darf im eigenen Interesse der Unternehmen auf keinen Fall vernachlässigt werden.



Mit der baramundi Management Suite setzen Administratoren vielfältige Sicherheitseinstellungen einfach und zentral

baramundi software AG
Beim Glaspalast 1
86153 Augsburg

Weitere Informationen und das kostenfreie Whitepaper von baramundi erhalten Sie hier: **www.baramundi.de/emm-sicherheit**

Gefahren vor der eigenen Haustür

Die meisten Variablen des Outrage-Modells fallen in die Kategorie der sogenannten quellenbezogenen Faktoren der Risikowahrnehmung, beziehen sich also auf Eigenschaften des potenziellen Schadensereignisses. Daneben gibt es jedoch noch weitere Kategorien wie Kontext- und Personenbezug. Und auch bei den quellenbezogenen Faktoren sind die von Sandman benannten Outrage-Bedingungen nicht ganz ausreichend.

Ein wichtiger Aspekt ist die Identität des oder der potenziellen Opfer eines Schadens. Kombiniert man dieses Merkmal mit Zeit und Ort eines Schadenseintritts, erhält man einen wichtigen Begriff: die Betroffenheit. Bin ich selbst oder eine mir nahestehende Person möglicher Leidtragender eines Schadens, schätze ich das Risiko in der Regel höher ein, als wenn irgendjemand anderer betroffen ist. Psychologen nennen dies das NIMBY-Phänomen. Dabei steht NIMBY für „Not in my backyard!“ (Nicht in meinem eigenen Garten!). Aus diesem Grund sollten Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Anwender (Security Awareness) möglichst auf eine persönliche Betroffenheit abzielen und nicht nur im Allgemeinen stecken bleiben.

Die Firewall im Bauch

Im Bereich der IT-Sicherheit ist für viele die Firewall ein Synonym für einen verlässlichen Schutzschild. Das spiegelt sich auch darin wider, dass es praktisch keine Unternehmens-IT mehr ohne Firewall gibt. Technisch betrachtet trennt sie zwei Netzwerksegmente. Sie steht typischerweise zwischen dem internen Netzwerk einer Organisation und dem Internet und steuert dort den ein- und ausgehenden Netzwerkverkehr. Die gängige Meinung über Firewalls ist, dass sie Hacker, Datendiebe und andere Cyberschädlinge aus dem diffusen Internet vom guten internen Netz fernhalten. Das ist auch prinzipiell richtig, aber häufig impliziert diese Denkweise auch die Idee, dass alles Böse immer nur von außen kommt – und von innen keine Gefahr droht. Dass dies ein Fehlschluss ist, beweisen wiederholte Pressemeldungen über Datenklau oder diverse Statistiken über IT-Sicherheitsverletzungen durch interne Beschäftigte.

Hier manipuliert unsere emotionale Firewall den Blick auf das Ganze. In der Tat sind nach innen gerichtete Schutzmechanismen, wie beispielsweise Datenklassifizierung und Verschlüsselung für vertrauliche Datenbestände, viel weniger verbreitet. Es herrscht immer noch häufig die Meinung vor, dass Daten im internen Netz per se sicher seien. Ein Trugschluss, wie zum Beispiel die seit 1998 regelmäßig durchgeführten Sicherheitsstudien der Fachzeitschrift *kes* eindrucksvoll belegen. Wie etwa in der kes/Microsoft-Sicherheitsstudie 2014 nehmen unbefugte Kenntnisnahme, Fehler und Sicherheitsverletzungen durch interne Mitarbeiter immer wieder eine Position unter den ersten drei Plätzen ein, meistens sogar Platz eins.

Positiv ist anzumerken, dass die Erkenntnis, wie sehr das Bewusstsein für Risiken bei den Anwendern die Sicherheit von IT-Systemen mitbestimmt, inzwischen auch bei vielen Firmen angekommen ist. Workshops und Kampagnen zur Security Awareness erfreuen sich wachsender Beliebtheit und auch moderne Tools zur Risikoanalyse in Netzwerken berücksichtigen mittlerweile ein mangelndes Sicherheitsbewusstsein bei den Anwendern als Risikofaktor. So lässt sich direkt prüfen, ob eine Security-Awareness-Schulung nicht vielleicht doch die sinnvollere Maßnahme gegenüber immer mehr neuer Technik ist.

Angewendet werden die Erkenntnisse der psychologischen Risikoforschung auch im Bereich der sicheren Softwareentwicklung. In ihrem Buch „Sichere Systeme“ betrachten die Autoren Walter Kriha und Roland Schmitz beispielsweise Cross-Site Scripting im Web-Application-Kontext unter dem Licht der Risikowahrnehmung. Eine beispielhafte Analyse über die flächendeckende Verbreitung von Virenscannern aus Sicht der Wahrnehmungsforschung findet sich im „Tagungsband zum 10. Deutschen IT-Sicherheitskongress des BSI“ von 2007.

Das passiert mir nicht!

Ein sehr häufig anzutreffendes Phänomen beim individuellen Umgang mit Risiken ist, dass eine Gefahr zwar erkannt, jedoch immer als ein Problem gesehen wird, das einen selbst nicht betrifft. Psychologen wie Neil D. Weinstein sprechen bei diesem unerschütterlichen Glauben an die eigene Unverwundbarkeit vom „It won’t happen to me“-Syndrom. Bestärkt wird dies vor allem, wenn ein potenzieller Schaden nicht unmittelbar eintritt und unter Umständen nicht einmal bemerkt wird.

Das Ausspionieren von Daten ist ein typischer Fall aus dem IT-Bereich, in dem diese Faktoren sich zur unheiligen Allianz paaren: Da durch Spionage keine Daten geändert werden, fällt der Angriff nicht weiter auf. Ein Schaden entsteht nur mittelbar und mit Zeitverzögerung, nämlich dann, wenn die unbefugte Kenntnis, beispielsweise über Angebote an Kunden, dazu führt, dass ein Konkurrent eine bessere Offerte erstellt und anschließend den Zuschlag dafür bekommt. Ob das nun einfach Pech ist, oder ob da durch Datenklau nachgeholfen wurde, wird man im Zweifel nie erfahren.

Gewinnchancen und Verlustrisiken

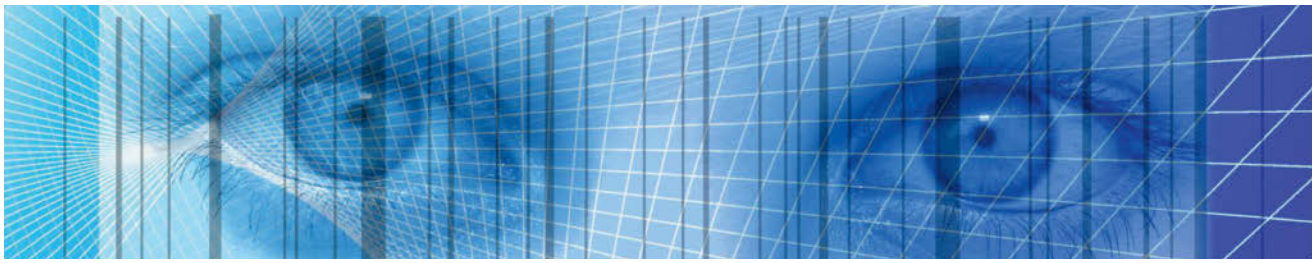
Eine berühmte Untersuchung zum menschlichen Handeln in Risikosituationen führte zu der sogenannten Prospect Theory (auch: Neue Erwartungstheorie) von Daniel Kahneman und Amos Tversky, die den beiden Psychologen im Jahr 2002 den Nobelpreis für Wirtschaftswissenschaften einbrachte. Ein zentrales Ergebnis dieser Arbeit ist, dass die Motivation eines Menschen bei der Aussicht auf Gewinn langsamer wächst, als wenn es um die Abwendung von Verlusten geht. Ein sehr wahrscheinlicher oder sogar sicherer kleiner Gewinn wirkt für die meisten attraktiver als ein hoher Gewinn mit geringer Gewinnchance. Der Volksmund sagt dazu: „Der Spatz in der Hand ist besser als die Taube auf dem Dach.“ Geht es hingegen um die Vermeidung von Verlusten, nehmen die meisten Menschen höhere Risiken in Kauf.

Ein Beispiel hierfür, das in der Welt der IT-Sicherheit ein kaum auszumerzendes Problem darstellt, sind Passwortrichtlinien. Der Gewinn in dieser Situation ist die Steigerung der Sicherheit bei der Einführung von Komplexitätsregeln. Dem gegenüber stehen der Verlust von Bequemlichkeit und das Risiko des Vergessens. Je komplexer die Richtlinien für die Passwortvergabe werden, desto schwerer wiegt die Verlustseite. Die Motivation, mehr Sicherheit zu erreichen, steigt mit wachsender Komplexität immer langsamer, bis irgendwann die Bequemlichkeit und die Angst vor dem Vergessen des Passwortes überhandnehmen – und wieder einmal ein Post-it am Monitor klebt.

Fazit

Psychologische Faktoren spielen eine enorm große Rolle bei der Einschätzung von Bedrohungsszenarien, nicht zuletzt auch bei der Bewertung von IT-Risiken. Wer diesen Aspekt aus seinem Informationssicherheitskonzept ausklammert, muss sich nicht wundern, wenn als Pekinesen getarnte Hacker in seinem Netz ein- und ausgehen.

Dr. Volker Scheidemann,
Direktor Marketing, Applied Security GmbH



Quelle: Jürgen Fälchle - Fotolia

Orientierungshilfe im Gesetzesdschungel

Das IT-Sicherheitsgesetz und die kommende europäische NIS-Richtlinie stellen in vielen Bereichen die Weichen neu

Vor dem Hintergrund einer komplexen Bedrohungslage in Europa und zunehmender Cyberangriffe auf private und öffentliche IT-Infrastrukturen erscheinen neue gesetzliche Regelungen unvermeidbar und auch vernünftig. Was genau aber haben die Unternehmen in Deutschland zu erwarten?

Unser Ziel ist es […], dass die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit gehören“, erklärte Bundesinnenminister de Maizière bei der Verabschiedung des IT-Sicherheitsgesetzes. Dieses Ziel sollte nicht lediglich als frommer Wunsch verstanden werden. Vielmehr ist es für den Technologiestandort Deutschland zwingend erforderlich, seine IT-Infrastruktur und damit auch sein Know-how zu schützen. Der Bericht zur Lage der IT-Sicherheit in Deutschland spiegelte für das Jahr 2015 hingegen noch ein anderes Bild wider. So stellte das Bundesamt für Sicherheit in der Informationstechnik (BSI) fest, dass die Anzahl der Schwachstellen und Verwundbarkeiten in deutschen IT-Systemen weiterhin auf hohem Niveau liegt und sich die Bedrohungslage im Cyberraum weiter zuspitzt.

Angesichts der vom Bundeskriminalamt (BKA) geschätzten 30.000 Cyberangriffe, denen deutsche Unternehmen täglich ausgesetzt sind, ist es für Unternehmen essenziell, IT-Sicherheit als wesentlichen Teil des unternehmerischen Risikomanagements zu betrachten.

Besonders kritisch sieht es im deutschen Mittelstand aus. So ergab eine Umfrage der Beratungsgesellschaft PricewaterhouseCoopers, dass jedes zehnte mittelständische Unternehmen im Jahr 2014 mindestens einmal Opfer eines Cyberangriffs wurde. Durchschnittlich entstand pro Unternehmen ein wirtschaftlicher Schaden in Höhe von 80.000 EUR, wobei der Schaden im Einzelfall deutlich höher ausfallen kann. So werden auch in Deutschland immer mehr Firmen Opfer einer Erpressung oder zumindest eines Erpressungsversuchs, beispielsweise durch sogenannte Verschlüsselungstrojaner, die relevante Daten verschlüsseln und nur nach Zahlung eines Lösegelds wieder freigeben. Im März 2016 berichtete das BSI, dass allein von Oktober 2015 bis Februar 2016 deutschlandweit die Anzahl der Erpressungstrojaner um das Zehnfache stieg.

Der erste Streich…

Im Gegensatz zum Datenschutzrecht, wo Deutschland im internationalen Vergleich anerkanntermaßen eine Vorreiterstellung innehat, hinkt es in IT-Sicherheitsfragen eher hinterher. Allgemein verbindliche Vorgaben gibt es kaum, die rechtlichen Anforderungen an Unternehmen bleiben schwammig und die Sanktionen bei Fehlverhalten überschaubar.

Mit dem am 25.06.2015 in Kraft getretenen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) hat der deutsche Gesetzgeber nun erstmals durch Änderung einer Vielzahl bereits bestehender Gesetze einen übergreifenden Rechtsrahmen für die Gewährleistung von IT-Sicherheit in Deutschland geschaffen, wobei er etablierte Standards wie die internationale Norm ISO/IEC 27001 oder den deutschen BSI-IT-Grundschutz für verbindlich erklärt und regelmäßige Kontrollen einführt.

Allgemeinverbindliche Vorgaben setzt das IT-Sicherheitsgesetz – entgegen seinem etwas irreführenden Namen – nur bedingt: So sind zwar sogenannte Betreiber kritischer Infrastrukturen (KRITIS) gemäß § 8a BSI-Gesetz verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer IT-Systeme zu treffen, bei deren Umsetzung stets der „Stand der Technik“ einzuhalten ist. Das IT-Sicherheitsgesetz regelt hingegen nicht, welche konkreten Vorkehrungen umzusetzen sind. Stattdessen können die anzulegenden Mindestsicherheitsstandards von den KRITIS-Betreibern selbst und ihren Branchenverbänden branchenspezifisch erarbeitet werden. Das BSI muss jedoch auf Antrag deren Eignung feststellen.

Zudem ist die Einhaltung dieser branchenspezifischen Mindeststandards von den KRITIS-Betreibern mindestens im Zweijahresrhythmus nachzuweisen. Dies erfolgt in Form von Sicherheitsaudits, Prüfungen oder Zertifizierungen, die das BSI näher konkretisieren kann. Zudem soll zur besseren Bekämpfung der Cyberkriminalität eine umfassende Wissensbasis durch den Austausch von Informationen zwischen Staat und Wirtschaft aufgebaut werden. KRITIS-Betreiber sind deshalb gemäß § 8b BSI-Gesetz verpflichtet, durch Cyberangriffe verursachte erhebliche Störungen mit Auswirkungen auf die öffentliche oder die Versorgungssicherheit unverzüglich zu melden.

… der zweite folgt sogleich

Dass das IT-Sicherheitsgesetz hierbei nur den Anfang einer gesetzlichen Entwicklung darstellt, lässt sich schon anhand des Adressatenkreises ersehen. Zudem wird auch der europäische Gesetzgeber in diesem Jahr eine neue Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) verabschieden. Sie muss binnen 21 Monaten nach Verabschiedung auf europäischer Ebene (also voraussichtlich bis Mitte 2018) in deutsches Recht umgesetzt werden und sieht eigene Anforderungen an die IT-Sicherheit der KRITIS-Betreiber (operators of essential services) und der Anbieter digitaler Dienste (digital service providers) vor. Die NIS-Richtlinie wird den Mitgliedsstaaten voraussichtlich einen gewissen Umsetzungsspielraum belassen, und es bestehen bereits zahlreiche Überschneidungen mit den Anforderungen des IT-Sicherheitsgesetzes: So wird den KRITIS-Betreibern in ähnlicher Weise auferlegt, technische und organisatorische Sicherheitsmaßnahmen zu ergreifen, um die Kontinuität ihrer Leistungserbringung zu gewährleisten. Wie auch unter dem IT-Sicherheitsgesetz werden sie zur Meldung relevanter Störungen verpflichtet.

Zwar ist nicht jede Abweichung von den Vorgaben der NIS-Richtlinie verboten. Insbesondere in Fällen, in denen das IT-Sicherheitsgesetz höhere Anforderungen setzt, können diese zusätzlichen nationalen Verpflichtungen in verschiedenen Fällen durchaus auch nach Inkrafttreten der NIS-Richtlinie Bestand haben. So definiert das IT-Sicherheitsgesetz beispielsweise eine niedrigere Schwelle als Auslöser für Meldepflichten und sieht umfangreichere Informationspflichten beim Eintritt von Störungen vor. In Detailfragen verfolgt die NIS-Richtlinie jedoch eine etwas andere Stoßrichtung, sodass ein Anpassungsbedarf der nationalen Vorschriften an die europäischen Vorgaben bestehen dürfte.

Wer ist vom IT-Sicherheitsgesetz betroffen?

Wenngleich sich das IT-Sicherheitsgesetz nicht nur an KRITIS-Betreiber wendet (es bestehen beispielsweise auch Anforderungen an Telemediendienste-Anbieter), so sind diese doch dessen primäre Adressaten. Kritische Infrastrukturen definiert § 2 Abs. 10 BSI-Gesetz als: „Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“ Geschützt werden soll also die Daseinsvorsorge. Noch nicht erfasst sind hingegen die öffentliche Verwaltung oder reine Wirtschaftszweige wie die Automobilindustrie, die jedoch die Stärke der deutschen Wirtschaft begründen.

Doch wen subsumiert der Gesetzgeber unter den Begriff KRITIS-Betreiber? Das IT-Sicherheitsgesetz ermächtigt das Bundesministerium des Innern (BMI) mittels Rechtsverordnung zu bestimmen, welche Einrichtungen, Anlagen oder Teile als KRITIS zu werten sind. Am 04.05.2016 ist die Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) in Kraft getreten. Die BSI-KritisV bestimmt zunächst KRITIS in den Sektoren Energie, Informationstechnik und Telekommunikation (ITK) sowie Wasser und Ernährung. Bis Anfang 2017 sollen per Änderungsverordnung auch die KRITIS-Betreiber in den Sektoren Transport und Verkehr, Gesundheit sowie Finanz- und Versicherungswesen identifizierbar werden.

Der Entwurf sieht ein dreistufiges Verfahren vor, gemäß dem die Bewertung als „kritisch“ oder „nicht kritisch“ erfolgen soll: Damit eine Infrastruktur als kritisch bewertet werden kann, muss sie für die Versorgung der Allgemeinheit mit einer elementaren Dienstleistung bestimmt sein. Daher definiert das BMI in einem ersten Schritt folgende Dienstleistungen in mehreren Sektoren, die wegen ihrer Bedeutung als kritisch anzusehen sind: Sektor Energie – Stromversorgung, Gasver-

sorgung, Kraftstoff- und Heizölversorgung, Fernwärmeversorgung; Sektor Wasser – Trinkwasserversorgung, Abwasserbeseitigung; Sektor Ernährung – Lebensmittelversorgung; Sektor Informationstechnik und Telekommunikation – Sprach- und Datenübertragung, Datenspeicherung und -verarbeitung.

Anlagentypen und Meldepflichten

In einem zweiten Schritt identifiziert das BMI diejenigen Kategorien von Anlagen, die für die Erbringung der kritischen Dienstleistungen erforderlich sind. Hierzu zählen unter anderem für den

Sektor Energie: Erzeugungsanlagen, Speicheranlagen, Messstellen, Gasförderanlagen, Gasspeicher, Verteilernetze für Strom und Gas, Ölförderanlagen, Raffinerien, Öl- und Produktendlager, Tankstellennetze, Heizwerke, Heizkraftwerke, Fernwärmenetze;

Sektor Wasser: Kanalisation, Kläranlagen, Leiteinrichtungen, Gewinnungsanlagen, Aufbereitungsanlagen, Wasserverteilungssysteme;

Sektor Ernährung: Anlagen zur Produktion von Agrarerzeugnissen, Anlagen zur Lagerung von Lebensmitteln, Anlagen für die Lebensmittelproduktion und -verarbeitung sowie den Lebensmittelhandel, Anlagen zum Verkauf von Lebensmitteln;

Sektor Informationstechnik und Telekommunikation (ITK): Übertragungsnetze für öffentlich zugängliche Telefon-, Telekommunikations-, Datenübermittlungs- oder Internetzugangsdienste, Rechenzentren, Serverfarmen, Content Delivery Networks, Trust-Center.

In einem dritten Schritt bestimmt das BMI konkrete Anlagen oder Teile, die einen aus gesamtgesellschaftlicher Sicht bedeutenden Versorgungsgrad aufweisen. Die Bestimmung erfolgt anhand von Schwellenwerten, die jeder Anlagenkategorie zugeordnet wurden. Die Schwellenwerte werden hierbei mittels einer 500.000er-Regel berechnet. Das bedeutet, dass das BMI ab einer Versorgung von mindestens 500.000 Menschen grundsätzlich von einer Meldepflicht ausgeht. Da die Anzahl der versorgten Personen häufig nicht ohne Weiteres festzustellen ist, ergibt sich der Schwellenwert im Regelfall anhand des statistischen Verbrauchs der Dienstleistung in Bezug auf 500.000 Abnehmer (so liegt z.B. der Verbrauch von 500.000 Menschen bei 21,9 Millionen m^3 Wasser pro Jahr, der kritische Schwellenwert im Bereich der Wasserversorgung betrüge somit ebendiese 21,9 Millionen m^3 Wasser pro Jahr). Wird dieser Schwellenwert erreicht oder überschritten, gilt die Anlage als kritisch.

Mehr Rechtssicherheit, aber offene Fragen

Ein erstes Ziel dürfte das BMI mit dem Entwurf der BSI-KritisV bereits erreicht haben: Sie wird zu mehr Rechtssicherheit führen. Dennoch bleiben auch einige kritische Fragen. Die 500.000er-Regel erscheint auf den ersten Blick zwar plausibel – schließlich soll verhindert werden, dass kleinere Unternehmen kostspielige IT-Sicherheitsmaßnahmen ergreifen müssen, welche sie schlechterdings nicht wirtschaftlich tragen können. Dennoch darf bezweifelt werden, dass Ausfälle oder

Beeinträchtigungen in der Versorgung von weniger als 500.000 Menschen tatsächlich stets ohne Weiteres abgefangen werden können.

Im Sektor der Wasserversorgung ist z.B. festzustellen, dass diese vorwiegend dezentral erfolgt, sodass die Schwellenwerte möglicherweise nicht im angemessenen Verhältnis zur Relevanz der Bevölkerungsversorgung mit Wasser stehen. Vor allem, weil die IT-sicherheitsrechtlichen Bestimmungen die Sicherstellung der Daseinsvorsorge und der öffentlichen Sicherheit zum Ziel haben, wäre zu fragen, ob nicht ein Bewertungsspielraum, der qualitative Kriterien berücksichtigt, in Bezug auf die zu versorgenden Menschen angemessener wäre.

Europäische und nationale Normen

Solche qualitativen Kriterien sowie die Berücksichtigung etwaiger Domino-Effekte fehlen aber gänzlich. So wäre beispielsweise zu berücksichtigen, dass es KRITIS-Betreiber gibt, die zwar nicht unmittelbar 500.000 Menschen versorgen, jedoch Unternehmen nebst deren Produktions- und Industrieanlagen, die wiederum ihrerseits die Versorgung einer Vielzahl von Menschen sicherstellen. Eine Pro-Kopf-Berechnung erscheint in diesem Fall nicht zielführend, denn ein Ausfall einer solchen kritischen Infrastruktur dürfte zumindest genauso gravierende, wenn nicht im Einzelfall sogar schwerwiegendere Auswirkungen auf die Versorgung der Bevölkerung haben wie ein Ausfall einer KRITIS, die unmittelbar 500.000 Menschen versorgt.

Zumindest zweifelhaft erscheint auch, inwieweit das in der BSI-KritisV beschriebene Verfahren zur Ermittlung der KRITIS-Betreiber mit der kommenden NIS-Richtlinie vereinbar sein wird. Im Vergleich zu dieser zeigt sich, dass der Begriff des KRITIS-Betreibers dort eher enger gefasst sein wird als im deutschen Recht. Anstelle des gesamten Finanz- und Versicherungssektors werden nämlich nur das Banking und die Finanzmarktinfrastruktur, statt Wasser und Ernährung lediglich die Trinkwasserversorgung und -verteilung und statt des gesamten ITK-Sektors nur die digitale Infrastruktur mit drei eng definierten Subsektoren (Internet-Knoten, Domain Name System Service Provider und Top Level Domain Name Registries) erfasst. Zur Qualifikation als kritische Infrastruktur ist nach der Richtlinie zusätzlich erforderlich, dass die Leistungserbringung auf Netzwerk- und Informationssystemen beruht und dass eine Störung dieser Systeme erhebliche negative Auswirkungen auf die Leistungserbringung hätte. Da das nationale Recht der Mitgliedstaaten in vielen Fällen über den europäischen Standard hinausgehen darf, sollte allerdings ein Mehr an IT-Sicherheit nicht zwingend ein europarechtliches Problem darstellen.

Vorhersehbare Konflikte mit der kommenden NIS-Richtlinie?

Vereinzelt werden solche Problemfälle dennoch auftreten: So reguliert die NIS-Richtlinie nur Online-Marktplätze, Suchmaschinen und Cloud-Computing-Anbieter, während das IT-Sicherheitsgesetz durch die Schaffung des § 13 Abs. 7 TMG mit den Anbietern geschäftsmäßig angebotener Telemedien einen wesentlich größeren Adressatenkreis zur Einhaltung bestimmter IT-sicherheitsrechtlicher Vorgaben heranzieht. Nahezu jedes Unternehmen der IT-Branche in Deutschland, so etwa auch Softwareanbieter, wenn sie ihre Produkte beispielsweise als Cloud-Lösungen bereitstellen, ist mehr oder minder von den Änderungen des Telemediengesetzes (TMG) betroffen. Nach dem Entwurf der NIS-Richtlinie sollen erhöhte Anforderungen an Anbieter digitaler Dienste jedoch nur in eng begrenzten Ausnahmefällen zulässig sein.

Daneben soll laut NIS-Richtlinie der Kreis der Betreiber kritischer Infrastrukturen nicht nur anhand eines Schwellenwertes wie der 500.000er-Regel, sondern mittels eines Bündels verschiedener Kriterien bestimmt werden. Entscheidend ist, ob eine Beeinträchtigung der Netzwerk- und Informationssysteme eine erhebliche Störung der Leistungserbringung verursachen würde. Dazu sollen neben der Zahl der von der Infrastruktur abhängigen Nutzer auch folgende sektorübergreifende Aspekte berücksichtigt werden: die Abhängigkeit anderer kritischer Infrastrukturen von der betroffenen Leistung, die Schwere und die Dauer von Beeinträchtigungen für wirtschaftliche und gesellschaftliche Aktivitäten und die öffentliche Sicherheit, der Marktanteil des betroffenen Betreibers, die räumliche Reichweite eines möglichen Vorfalles und alternative Möglichkeiten der Versorgung.

Weiter sind auch sektorspezifische Kriterien vorgesehen. Die Erwägungsgründe des Richtlinienentwurfs nennen beispielsweise für den Energiesektor die Erzeugungs- und Fördermengen, für Banken und Finanzmarktinstitutionen ihre systemische Relevanz sowie das Verhältnis ihrer Aktiva zum Brutto-Inlandsprodukt und für den Gesundheitssektor die Zahl der jährlich versorgten Patienten.

Der Entwurf der NIS-Richtlinie sieht im Rahmen der europäischen Kooperation entsprechende – wenn auch rechtlich nicht verbindliche – Konvergenzmechanismen vor. So müssen die Mitgliedstaaten der Kommission nicht nur die Listen der von ihnen identifizierten Betreiber kritischer Infrastruktur übermitteln, sondern auch darlegen, welche Kriterien und Schwellenwerte sie dabei verwendet haben. Die darüber hinaus vorgesehenen Mechanismen zur Behördenkooperation dürften weiter zu einer Annäherung von Bewertungsmaßstäben beitragen: Es soll ein europäisches Behördennetzwerk zur Cybersicherheit geschaffen werden, um den Austausch und die Kompatibilität von IT-Sicherheitsstrategien unter den Mitgliedstaaten zu erleichtern und eine europaweite Annäherung von Standards und Verfahren zu befördern. Daher ist im Zuge der Umsetzung der NIS-Richtlinie mit einer Anpassung der BSI-KritisV zu rechnen, die den ausdifferenzierten Bewertungsmaßstäben Rechnung trägt.

Indirekte Auswirkungen auf andere Bereiche

Wer derzeit noch nicht vom IT-Sicherheitsgesetz betroffen ist – oder sich bisher noch nicht damit auseinandergesetzt hat, ob sicherheitsrelevante Anpassungen für sein Unternehmen ohnehin längst überfällig sind – kann sich dennoch nicht einfach bequem zurücklehnen. Dies gilt zum einen vor allem für Dienstleister von KRITIS-Betreibern, die sich zunehmend den steigenden Ansprüchen ihrer Kunden anpassen werden müssen. Zum anderen ist mit Blick auf eine mögliche Fortschreibung der Vorgaben des IT-Sicherheitsgesetzes und der NIS-Richtlinie sicherlich damit zu rechnen, dass schrittweise auch bislang noch nicht benannte Sektoren neue und erweiterte IT-Sicherheitsanforderungen erfüllen müssen.

Sowohl von den bereits existierenden als auch den noch zu erwartenden Regelungen betroffen sind nicht zuletzt auch die Hersteller von IT-Produkten und Softwarelösungen. Viel zu häufig wird vergessen, dass das BSI gemäß §8b Abs. 6 BSI-Gesetz von IT-Herstellern die Mitwirkung an Störungsbeseitigungen verlangen kann. Noch einschneidender dürfte sich jedoch das Recht des BSI auswirken, IT-Produkte zu untersuchen und Warnungen gegenüber der Öffentlichkeit oder betroffenen Verkehrskreisen vor der Nutzung eines IT-Produkts auszusprechen (§7 BSI-Gesetz). Die Hersteller von IT-Produkten sind somit dringend angehalten, ihre Produktion auf die neuen Sicherheitsbedürfnisse einzustellen, wollen sie KRITIS-Betreiber als Kunden behalten.

Paul Voigt und Mareike Gehrmann,
Rechtsanwälte,
Taylor Wessing Partnerschaftsgesellschaft mbB

Sicherheit beim Mobile-Device-Management

Die berufliche und zugleich private Nutzung von Mobilgeräten birgt hohe Risiken

Die Verwendung von (mindestens) zwei Smartphones ist mittlerweile ein weitverbreiteter Trend: eines für die Arbeit, das andere für die private Nutzung – dazu noch ein Tablet. Leider ist das in vielen Fällen kaum vermeidbar, weil es an einem sicheren Management der Geräte mangelt.

Besondere Herausforderungen im Mobile-Device-Management (MDM) tauchen vornehmlich bei der Umsetzung von Bring Your Own Device (BYOD) auf. Eine Lösung dieser Aufgaben ist für den Datenschutz und die Compliance dringend notwendig und soll gleichzeitig der unerfreulichen Entwicklung hin zum Zweitgerät entgegenwirken. BYOD birgt eine Reihe ernst zu nehmender Sicherheitsrisiken, und das nicht nur bei der Auswahl der Apps. Ein den speziellen Bedürfnissen des Unternehmens angepasstes MDM-System ist daher äußerst empfehlenswert. Doch welche Maßnahmen zum Schutz vor schädlichen Apps und anderen Bedrohungen sind nötig und auch machbar?

BYOD-Risiken

Die meisten Apps benötigen Zugriff auf verschiedene Sensoren und Daten, um ihren Zweck zu erfüllen. Fordert eine App aber mehr Rechte, als sie für ihre Funktion tatsächlich benötigt, sollte man sie bedenkenlos aussortieren. Denn warum muss etwa eine Taschenlampen-App auf die GPS-Daten des Nutzers zugreifen, um das Smartphone zur Lichtquelle zu machen? Möchte man jedoch beispielsweise eine Taxi-App wie Uber benutzen, dann benötigt sie sowohl die GPS-Daten wie auch einen Zugang zum Internet, denn irgendwie muss der Taxifahrer ja wissen, wo er hinfahren soll. Allerdings erfährt man mittels dieser Daten aber auch viel über einen Anwender, wie Uber unlängst mit dem Offenlegen von One-Night-Stands seiner Nutzer bewiesen hat. Für den Fall, dass die Daten legitim verwendet werden, aber dennoch ein Missbrauchspotenzial nicht auszuschließen ist, muss man als Unternehmen entweder dem Anbieter ein hohes Maß an Vertrauen entgegenbringen oder das Risiko vertraglich – falls möglich auch technisch – absichern.

Da oft nur schwer nachvollziehbar ist, wie die Kommunikation zwischen verschiedenen Apps untereinander sich auf die verfügbaren Zugriffsrechte auswirkt, wird das Einschätzen der verlangten Aktionen zusätzlich erschwert. Verlangt eine App beispielsweise zwar selbst keinen Internet-Zugriff, kann aber eine andere App auffordern, eine bestimmte Webseite zu besuchen, so genügt dies bereits, um einen unkontrollierten Datenabfluss zu initiieren. Dieses Phänomen, das eine eigentlich gutartige App zweckentfremdet, um (verborgene) Zugriffe zu gewähren, wird in der Literatur oft als Confused-Deputy-Angriff bezeichnet.

Eine andere Unwägbarkeit liegt beim Nutzer selbst: seine Gewohnheiten. Apps wie WhatsApp oder der Facebook-Messenger sind in Bezug auf den Datenschutz zumindest bedenklich. Als Unternehmen darf man ihnen keinen Zugriff auf sensible Daten gewähren. Das heißt, privates und geschäftliches Adressbuch müssen klar voneinander getrennt werden. Der Nutzer darf generell mit seinen privaten Apps auch nur mit den eigenen Daten interagieren. Eine rein organisatorische Maßnahme, die ihm verbietet, bestimmte Apps privat zu nutzen, ist hier vollkommen fehl am Platz. Eine Separierung dient nicht zuletzt auch dazu, arbeitsrechtliche Probleme zu vermeiden. Schließlich muss man die Unternehmensdaten genau überwachen, um nicht den Über-

Quelle: Backes SRT

Maßnahmen / Risiken	Fernadministration					mobile Sicherheit							BYOD			
	Fernlöschung	Ortung verlorener Geräte	Updates aus der Ferne	Backups	Policies	sichere Container	Einschränken von Zugriffsrechten	Kontrolle Inter-App Kommunikation	Verschlüsselung persistenter Daten	Analyse von Apps	Netzwerkkommunikation via VPN	Monitoring von Datenfluss und Gerätezustand	keine OS-Modifikation	keine Root-Rechte	hohe Marktabdeckung	einfaches Rollout
Zugriffsrechte																
Auswahl Business Apps																
Confused Deputies																
(blinder) Datenabfluss																
Kommunikation durch ungesicherte Netze																
physikalischer Zugriff von Unbefugten																
ungewisse Update-Zyklen																
Verlust von Geräten																
Gerätevielfalt																
Einschränkung privater Nutzung																
Nutzerakzeptanz																

Kriterien zur Auswahl eines sicheren MDM

blick zu verlieren. Der Blick auf private Mitarbeiterdaten ist hingegen absolut tabu.

Ein weiteres Problemfeld, das direkt mit BYOD zusammenhängt, ist die Handhabung einer großen Vielzahl an einzelnen Endgeräten. Zudem verlassen Mobilgeräte – im Unterschied zu anderen firmeneigenen IT-Systemen – häufig die Räumlichkeiten des Unternehmens. Zum einen sind sie somit nicht jederzeit für Administratoren verfügbar, beispielsweise für Updates. Zum anderen kann nicht sichergestellt werden, dass nur autorisiertes Personal physikalischen Zugriff auf die Geräte bekommt. Nicht zuletzt kommt es auch immer wieder zum Verlust bzw. Diebstahl von Geräten. Es muss also dafür gesorgt werden, dass Unbefugte, die unbegrenzt lange physikalischen Zugriff auf das Gerät haben, dennoch keine sensiblen Daten extrahieren können. Es ist zwar denkbar, durch Ortungsfunktionen das Auffinden des Gerätes im Verlustfall zu erleichtern. Dabei muss man aber darauf achten, dass der Betriebsrat einbezogen wird und die Nutzung der Ortung technisch regulierbar ist.

Auswahl sicherer Apps

Beurteilt man Apps nur nach ihren angeforderten Zugriffsrechten, wären einige als klar gefährlich, ein paar als angemessen, die weitaus größte Zahl aber als ungewiss einzustufen. Das liegt daran, dass für die Beurteilung der Rechte nicht das potenzielle Risiko von Interesse ist, sondern die tatsächliche Verwendung. Dafür braucht man mehr Informationen, als das Manifest oder die Beschreibung der App bietet. Man benötigt eine tief gehende Analyse, die aufzeigt, was die App mit den Daten macht, auf die sie Zugriff bekommt.

Bei Softwareanalysen unterscheidet man üblicherweise zwischen statischen und dynamischen. Statische Analysen führen den Code nicht aus, sondern inspizieren ihn, und geben Garantien, die für jede Ausführung des Codes gelten. Die Ergebnisse statischer Analysen werden dadurch eingeschränkt, dass Informationen versteckt werden können, beispielsweise durch das Nachladen von Code aus dem Internet. Dynamische Analysen führen hingegen den Code meist in einer kontrollierten Umgebung aus und sehen sich an, was bei genau dieser Ausführung gerade passiert. Sie haben allerdings den Nachteil, dass ihre Aussagekraft auf eine Ausführung des Codes beschränkt ist und dieser Vorgang nicht ohne Weiteres jedes Verhalten offenlegt. Ideal wäre eine statische Analyse, die für die meisten Apps aussagekräftige Ergebnisse liefert und bei den restlichen auf die Limitierung der Analyse hinweist. Wie vertrauenswürdig bewertet man eine App, auf der mit Geschäftsdaten gearbeitet werden soll, die Code aus dem Internet nachladen muss?

Um die Verwendung von Daten zu bestimmen, ist eine sogenannte Informationsflussanalyse eine geeignete statische Analyse. Sie findet heraus, ob beispielsweise ein Zugriff aufs Internet von einem Wert im Adressbuch abhängig ist, und kann somit bestimmen, ob Informationen abfließen. Es gibt hier eine Vielzahl von Analyse-Frameworks, die alle ihre unterschiedlichen Vor- und Nachteile haben. Einen Nachteil haben alle präzisen Methoden: Sie sind sehr rechenintensiv und ihre Ergebnisse werden meistens nur für Experten verständlich aufbereitet. Auch können legitime, aber unerwartete Flüsse auftauchen, die dann weiter analysiert werden müssen. So kann beispielsweise eine Synchronisationsfunktion im Adressbuch für einen Informationsfluss ins Internet führen. Geht dieser Prozess jedoch ausschließlich über den konfigurierten Server und somit verschlüsselt vonstatten, ist er zulässig und für die gewünschte Funktionalität notwendig. Kurz: Wie bei Schadsoftware ist es auch bei allen eingesetzten Apps gut zu wissen, was sie tun. In den meisten Fällen genügt es aber, wenn man sich vor eventuellen unerwünschten Funktionen schützen kann.

Schutz vor unsicheren Apps

Bei unsicheren Apps gibt es grundsätzlich zwei Szenarien: Die App greift das Betriebssystem an, oder sie greift die Daten an. Ein Angriff aufs Betriebssystem lässt sich oft nur beobachten und nicht verhindern, sodass sich in diesem Szenario die MDM-Lösung sperren und weitere Interaktion verweigern kann. Dennoch ist diese Situation besonders gefährlich, da man sich ab diesem Zeitpunkt nicht mehr auf die Sicherheitsmechanismen des Betriebssystems verlassen solte. Im anderen Fall, wenn die App also direkt die Daten abzugreifen versucht, kann eine MDM-Lösung intervenieren und Zugriffe unterbinden. Eine App kann schließlich nur die Daten stehlen, zu denen sie Zugang hat. Der Zugriff auf Sensoren lässt sich hingegen oft nur schwer abschätzten. Beispielsweise kann über Bewegungssensoren von Smartphones ein Password abgegriffen werden, wenn es neben der Tastatur liegt.

Im Vergleich zu klassischen Desktop-Betriebssystemen bieten mobile Betriebssysteme bereits dadurch Schutz, dass jede App ihre Daten kapseln kann, andere Apps also nicht einfach auf die Daten zugreifen können. Das MDM-System muss die Zugriffsrechte insgesamt beschneiden, aber auch Apps voneinander trennen können, damit diese nicht mehr beliebig untereinander kommunizieren, um etwa einen Confused-Deputy-Angriff auszulösen. In diesem Fall spricht man von sicheren Container-Lösungen. In solchen Containern sollte das MDM-System dann klar definieren, welche App auf welche Daten und Sensoren zugreifen darf. Hier ist es hilfreich, wenn das MDM es erlaubt, verständliche Policies festzulegen und zu kombinieren. Das vereinfacht es auch, die Compliance nachzuweisen. So könnte man für verschiedene gesetzliche Regelungen Policies definieren. Das MDM erzwingt dann, dass ein Zugriff nur gewährt wird, wenn alle Policies erfüllt sind. Ein sicherer Container sollte auch garantieren, dass die Daten nur verschlüsselt abgelegt werden, damit im Fall eines Betriebssystem-Exploits oder Gerätediebstahls der Schlüssel gelöscht werden kann, um zeitnah den Zugriff auch auf größere Datenmengen zu sperren.

Ein weiterer Schutz, der erfolgreich bei Desktop- und Serversystemen genutzt wird, sind Netzwerk-Gateways wie Firewalls oder Virenscanner, die den Datenverkehr untersuchen und gegebenenfalls blockieren, bevor er das Endgerät erreicht. Diese Schutzmaßnahme ist auf Mobilgeräten aus zwei Gründen schwerer umzusetzen. Zum einen muss das Gerät ja nicht mit dem Firmennetz verbunden sein, es kann beispielsweise gerade in einem Starbucks das offene WLAN nutzen. Organisatorische Maßnahmen sind hier zwar möglich, etwa eine Vorschrift: „Mobilgeräte dürfen nicht mit offenen WLANs genutzt werden“. Jedoch muss man der Realität ins Auge blicken und davon ausgehen, dass es trotzdem passieren wird. Daher ist eine technische Lösung des Problems, beispielsweise ein VPN (Virtual Private Network), das den Datenverkehr immer verschlüsselt durch das interne Netz tunnelt, zu bevorzugen. So können die Mobilgeräte zudem dieselben Netzwerk-Gateways verwenden, die auch die Desktoprechner im Unternehmen absichern.

Zum anderen möchte man keine privaten Apps auf den Geräten über das Unternehmensnetz kommunizieren lassen, genießen sie doch in der Kommunikation mit Firmenservern oft mehr Vertrauen und somit Zugriffsrechte. Folglich sollte es ein zuverlässiges MDM ermöglichen, gezielt die Businesscontainer per VPN mit dem Firmennetz zu verbinden. Insbesondere umgeht man bei solchen Lösungen arbeitsrechtliche Problemstellungen, da man die Firmenpakete per Deep Packet Inspection (DPI) analysieren kann, ohne zu riskieren, mit den privaten Daten der Mitarbeiter in Berührung zu kommen.

Fazit

Große Trends wie das Internet of Things (IoT) und Industrie 4.0 wirken sich auch auf BYOD aus. So steigt etwa Anzahl und Art der verbauten Sensoren in den Geräten kontinuierlich an. Die sogenannten Wearables bringen Sensoren auch an Orte, die es vereinfachen, Daten abzugreifen. Die Bewegungen des Handgelenks, gemessen von einer Smartwatch, geben beispielsweise deutlich präzisere Auskunft über Tastatureingaben als ein neben der Tastatur liegendes Smartphone. Sensoren, die den Puls oder die Körpertemperatur messen, bieten bislang ungeahntes Potenzial für neuartige Seitenkanalangriffe.

Auch das Wachstum der Hausautomation (Smart Homes) sorgt dafür, dass neuartige Angriffsmethoden und Einfallstore für Schadsoftware beachtet werden müssen. Zukünftig könnte z.B. ein Botnetz aus Kontrolleinheiten der Hausautomation den Strompreis manipulieren oder ein infizierter Toaster im Privathaushalt über ein privat genutztes Business-Smartphone angreifen und zu einer realen Bedrohung für die Unternehmensinfrastruktur werden. Es ist also höchste Zeit, sich um ein sicheres MDM-System zu bemühen, das alle verwendeten Mobilgeräte sowohl voll einsatzfähig als auch sicher macht.

Fabian Bendun,
Geschäftsführer Backes SRT

Erfolgsfaktor Mitarbeiter

Steigende Sicherheitsstandards in der Industrie 4.0 erfordern mehr qualifiziertes Personal

Industrie 4.0 wird in der Regel mit Maschine-zu-Maschine-Kommunikation, Automation und neu zu entwickelnden technischen Standards und Protokollen in Verbindung gebracht. Doch immer mehr erweist sich die Qualifikation der Mitarbeiter als der erfolgsentscheidende Dreh- und Angelpunkt.

Die Vernetzung von Anlagenherstellern, Integratoren und Betreibern löst einen hohen, prozess- und unternehmensübergreifenden Bedarf an Know-how in Planung, Produktion, Beschaffung und HR aus. Erforderliche Qualifikationen und organisatorische Strukturen müssen in den Industrieunternehmen jedoch erst noch aufgebaut werden.

Neue Risiken verlangen ein Umdenken

Das Zusammenwachsen von Produktion und IT und die wachsende Anzahl an Schnittstellen und Zugangsmöglichkeiten vergrößern die Angriffsfläche und somit auch das Gefährdungspotenzial. Die bekannten Sicherheitslösungen in der Office-IT sind jedoch nicht eins zu eins auf die Produktions-IT übertragbar. Die produktionsnahe IT kann zwar vom allgemeinen Entwicklungspfad lernen und Fehlentwicklungen vermeiden; die umzusetzenden Lösungen müssen jedoch auf Verträglichkeit mit den Rahmenbedingungen der Produktion geprüft und dementsprechend angepasst werden. Erforderlich ist hier fachübergreifendes technisches Know-how.

So entstehen an der Schnittstelle zwischen Produktion, IT und Security neue Rollen und Tätigkeitsprofile mit hohen Anforderungen an Qualifikationen und Ausbildung. Das betrifft sowohl Produktionsmitarbeiter, die über ein Grundverständnis für IT-Sicherheit verfügen sollten, aber auch beispielsweise Chief Information Security Officer (CISO), die ihre Kenntnisse um Produktionsaspekte erweitern müssen. Denn der Begriff Sicherheit umfasst zwei Dimensionen: Safety und Security. Während Safety traditionell im Produktions- und Ingenieursbereich verwurzelt ist, kommen mit dem Begriff Security IT-Anforderungen aus einer anderen Denkwelt hinzu. Ein gegenseitiges Verständnis beider Perspektiven ist in der Praxis entscheidend, um ein ausreichendes Sicherheitsniveau erreichen zu können.

Auch die kontinuierliche IT-Sicherheitsüberwachung von Anlagen und Systemen erfordert ein übergreifendes, über die jeweiligen Sicherheitsdefinitionen hinausgehendes Verständnis und Know-how der Mitarbeiter. Ein Beispiel: Werden in der Produktion bislang Patches und Updates fast ausschließlich während Wartungsfenstern eingespielt, so wird das künftig, wenn Produktions- und Office-IT eng verbunden sind, zu erheblichen Sicherheitsproblemen führen können. Hier müssen entsprechende Lösungen und auch Handlungsanweisungen für Mitarbeiter entwickelt werden.

Ein Großteil des Fachwissens wird künftig auf einzelne Mitarbeiter verteilt sein und nicht mehr zentral zur Verfügung stehen. Das stellt neue Herausforderungen an die Mitarbeiterführung: Eine dezentrale, serviceorientierte Struktur ist nur mit gut geschulten, eigenverantwortlichen Beschäftigten möglich. Neben dem erforderlichen technischen Know-how wird Industrie 4.0 insbesondere durch organisatorische Aspekte und erforderliche Soft Skills zu einer Herausforderung. Die Fähigkeit zum kooperativen Handeln über Abteilungsgrenzen hinweg, Interdisziplinarität und das Arbeiten in interprofessionellen Teams sind dafür unverzichtbar.

Mit neuen Anforderungen wird auch das Wissensmanagement konfrontiert: Das in langen Jahren angesammelte, wertvolle praktische Know-how der Produktionsmitarbeiter, etwa hinsichtlich des Zustands von Maschinen, des Wartungsbedarfs und der Fehlerbehebung, muss im Rahmen der Digitalisierung in die digitale Welt übertragen werden.

Spezialisten, die in der Lage sind, Industrie-4.0-Infrastrukturen sicher zu entwickeln, aufzusetzen und zu managen, sind auf dem Arbeitsmarkt derzeit kaum zu finden. Die Anforderungen sind vielfältig: Sie haben über IT-, IT-Sicherheits-, Ingenieurs- und Managementkenntnisse sowie Soft Skills zu verfügen, wie sie in dieser Form und Konstellation bislang noch nicht ausgebildet werden.

Nicht zuletzt deshalb fordert daher unter anderem der Bundesverband IT-Sicherheit e.V. (TeleTrusT) eine Anpassung und Neuordnung der Ingenieursausbildung in Deutschland. Umfassende und integrierte Qualifizierungen, die auch das Thema Security angemessen berücksichtigen, haben in Deutschland bislang leider Seltenheitswert.

Qualifizierung durch Weiterbildung

Während die Ausbildung mittel- und langfristig die Basis für eine adäquate Qualifikation sicherstellen sollte, kann schon jetzt Weiterbildung akuten Qualifizierungsbedarf kurzfristig abdecken. Mit dem Thema Industrial Security betrauen Unternehmen Mitarbeiter unterschiedlichster Abteilungen und Erfahrungswelten. Deren differenzierte Vorkenntnisse gilt es in Schulungen zu berücksichtigen.

Grundlegende Ansatzpunkte für Weiterbildungsmaßnahmen beinhalten unter anderem: modulartige Schulungseinheiten; ein Schulungsangebot mit unterschiedlicher Lernintensität und Trainingsdauer, um den Know-how-Anforderungen der verschiedenen Zielgruppen gerecht zu werden; eine besondere Berücksichtigung von Führungskräften als Promotoren für die Qualifizierung der Fachkräfte; Brückenseminare zur interdisziplinären Vermittlung von Technikwissen; die Berücksichtigung sogenannter weicher Faktoren (z. B. Kooperations- und Konfliktlösungsfähigkeit); interdisziplinäre und abteilungsübergreifende Trainings; eine Kombination aus Präsenzschulungen, Webinaren und E-Learning-Angeboten sowie Schulungen für Produktionsmitarbeiter entsprechend ihrer Vorkenntnisse.

Voraussetzung für die Qualifikation der Trainer ist eine mehrjährige praktische Erfahrung im Bereich industrieller Anlagen. Auch IT-Sicherheitsexperten, die über praktische Erfahrung in der Beratung verfügen, eignen sich als Referenten.

Empfehlungen des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schlägt für die Weiterbildungsmaßnahmen eine Aufteilung in zwei Zielgruppen vor, die je nach Vorkenntnissen im Rahmen von komprimierten Überblicksveranstaltungen oder mehrtätigen Intensivschulungen auf den aktuellen Stand der Sicherheitstechnik gebracht werden sollten:

Management: Zum Management werden Produktionsverantwortliche, Führungskräfte (C-Level), gegebenenfalls (neue) Mitarbeiter mit operativem Security-Bezug gezählt. Hauptziele einer etwa eintägigen Schulung sind das Aufzeigen der Bedrohungslage und des Handlungsbedarfs sowie die Vermittlung elementarer Begrifflichkeiten und systematischer Ansätze. Es sollen Kenntnisse der wichtigsten organisatorischen und technischen Maßnahmen vermittelt werden, um Projekte anstoßen zu können.

Neue Rollenmodelle

Viele Unternehmen haben unterschiedlich begonnen, das Thema Industrial Security in ihre Organisationen einzubinden. Hierbei lassen sich stark zentralisierte und dezentralisierte Strukturen unterscheiden. In Erprobung sind unterschiedliche Organisationsmodelle, die konträr diskutiert werden. Die künftige Qualifikation des CISO ist dabei erheblich von der Wahl des Organisationsmodells abhängig. Soll er auch die Security in der Produktion mitverantworten, so benötigt er zusätzliche Kenntnisse, um die Belange der Produktion angemessen berücksichtigen und bewerten zu können.

Diskutiert wird unter anderem, Industrial Security von der IT verantworten zu lassen, die somit auch an die Produktion angepasste Richtlinien verfasst. Zum anderen gibt es aber auch Varianten, in denen Unternehmen die Industrial Security unabhängig von der Office-IT autark der Produktion zugeordnet haben und diese somit eigenverantwortlich bleibt. Dazu wird ein eigener Informationssicherheitsbeauftragter/Officer Produktion (ISO-Prod) eingesetzt.

Fazit

Industrie 4.0 hat erhebliche Auswirkungen auf Mitarbeiterqualifizierung, Organisationsentwicklung und Unternehmensführung. Besonders im Bereich der Industrial Security sind erhebliche Änderungen zu erwarten. Der Schulungsbedarf insgesamt wird erheblich steigen. Neben den Soft Skills wird auch die Vermittlung von interdisziplinärem Wissen, von IT- und Produktions-Know-how, Industrial-Security-Kenntnissen sowie einem gemeinsamen Begriffsverständnis in den Mittelpunkt rücken.

Christian Jacobs und Harald Kesberg,
qSkills GmbH & Co. KG; Kesberg Consulting

Erweiterte Sicherheitsregeln im Online-Business

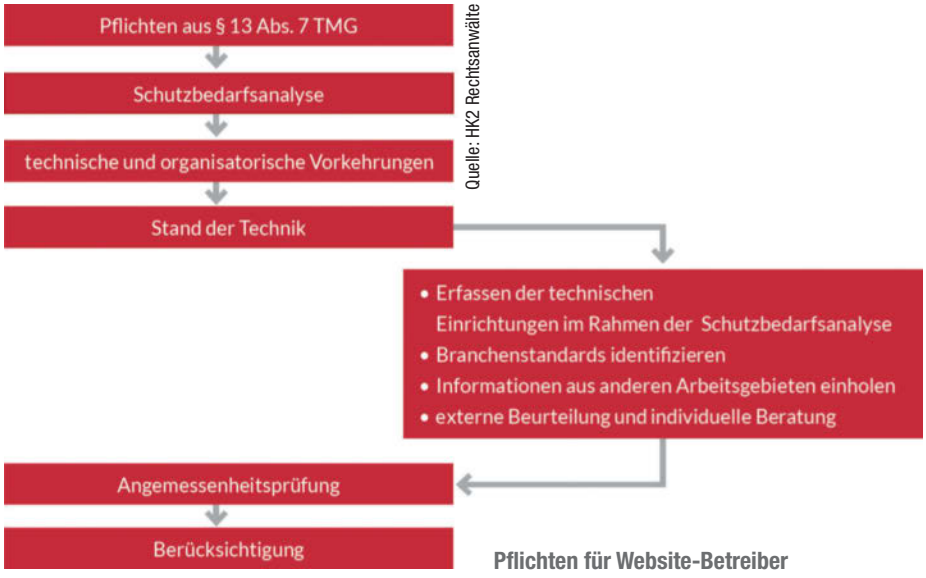
Auch das Telemediengesetz verlangt die Umsetzung neu definierter IT-Sicherheitsmaßnahmen

Die Anbieter von Online-Diensten, vom kleinen Website-Betreiber bis zum großen Online-Auktionshaus, müssen sich jetzt ebenfalls mit den Anforderungen des IT-Sicherheitsgesetzes auseinandersetzen. Für viele kleinere Unternehmen empfiehlt es sich, externe Fachleute damit zu beauftragen.

Seit dem 25.07.2015 ist nun das IT-Sicherheitsgesetz (ITSiG) in Kraft – und noch immer wird nahezu ausschließlich auf die neuen Pflichten für Betreiber kritischer Infrastrukturen fokussiert. Weit weniger Aufmerksamkeit erhielt die vom ITSiG vorgenommene Änderung des Telemediengesetzes (TMG), obwohl hier umfangreiche und sanktionsbelegte Pflichten geschaffen wurden, die nahezu jedes Unternehmen der Branche betreffen. Auch viele Softwareanbieter sind davon nicht ausgenommen.

Die zentrale Norm: § 13 Absatz 7 TMG

Diensteanbieter haben nunmehr TMG-konforme technische und organisatorische IT-Sicherheitsmaßnahmen einzurichten und zu unterhalten. Es gibt weder einen gesetzlichen Mindeststandard noch eindeutige Beurteilungsmaßstäbe oder eine Übergangsfrist. Da die rechtlichen Anforderungen kompliziert und diffus sind, ist zu erwarten, dass insbesondere kleine und mittelständische Unternehmen die konkrete Festlegung und Umsetzung der Anforderungen in die Hände Dritter legen werden. Dabei ist jedoch einiges zu beachten.



Pflichten für Website-Betreiber

Zunächst ist nach § 13 Absatz 7 TMG ein unerlaubter Zugriff durch Unbefugte auf die technischen Einrichtungen zu verhindern (Nr. 1). Hierunter fallen sämtliche genutzten Systeme, wie etwa Server oder Web-Applikationen. Zudem sind die Telemedien auch gegen die Verletzung personenbezogener Daten (Nr. 2a) und ebenso gegen Störungen – auch durch äußere Angriffe (Nr. 2b) – zu sichern. Praktisch bedeutet das: Es sind die herkömmlichen Schutzziele der IT-Sicherheit (VIVA-Prinzip: Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität) gemäß Nr. 1 und Nr. 2b zu beachten; in Nr. 2a sind die datenschutzrechtlichen Anforderungen angelegt, die als Spezialnorm dem Bundesdatenschutzgesetz (BDSG) vorgehen.

Limitierte Schutzbedarfsanalyse

Die erste Herausforderung ist die Ermittlung des konkreten Schutzbedarfs und der notwendigen Anpassungen. Der Gesetzgeber hat hier – anders als etwa in der Anlage zu § 9 BDSG - die Anforderungen nicht konkretisiert. Das Gesetz fordert einen erfolgsbestimmten Schutz: Die technischen Einrichtungen sind gegen die in den Tatbestandsvarianten genannten Gefahren zu schützen. Damit können die erforderlichen Vorkehrungen nicht durch eine klassische, vollumfängliche Schutzbedarfsanalyse ermittelt werden, bei der sich über eine Einschätzung von Schadensfolgenerheblichkeit und Eintrittswahrscheinlichkeit typische Schadensszenarien identifizieren lassen, anhand derer dann die Schutzbedarfskategorie bestimmt wird. Eine an die Vorgaben des § 13 Abs. 7 TMG angepasste – limitierte – Schutzbedarfsanalyse ist dennoch vorzunehmen, da ja nur so eine Bestimmung der gesetzlichen Vorkehrungen möglich ist. Mithilfe dieser Bewertung müssen dann die technischen sowie organisatorischen Vorkehrungen identifiziert werden, die erforderlich und geeignet sind, den festgestellten Schutzbedarf zu erfüllen.

Stand der Technik

Zu den so identifizierten Vorkehrungen ist sodann der im Einzelnen geltende „Stand der Technik“ zu ermitteln. Dabei handelt es sich um einen unbestimmten Rechtsbegriff, der aber gerichtlich voll überprüfbar ist. Der Stand der Technik grenzt sich nach unten hin ab zu den „allgemein anerkannten Regeln der Technik“ sowie nach oben hin zum „Stand von Wissenschaft und Forschung“.

Die allgemein anerkannten Regeln der Technik bezeichnen dabei zwar bewährte Verfahren, die aber nicht zu den besten am Markt verfügbaren Leistungen gehören. Dagegen beinhaltet der Stand von Wissenschaft und Forschung eine Reihe von Maßnahmen an vorderster Front der technischen Entwicklung, jedoch unabhängig davon, ob diese für den Anwender einsetzbar oder am Markt verfügbar sind. Der Stand der Technik liegt hingegen vor, wenn die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheint (vgl. Gesetzesbegründung zu § 8a BSIG). Das bedeutet verkürzt, dass zumeist Spitzenprodukte eingesetzt werden müssen.

Angemessenheit

Wurden der individuelle Schutzbedarf und der jeweilige Stand der Technik ermittelt, folgt daraus aber noch keine unbegrenzte Umsetzungspflicht. Vielmehr sieht die Norm Einschränkungen vor, mit denen die Verhältnismäßigkeit gewährleistet werden soll. Insbesondere ist der Stand der Technik lediglich zu „berücksichtigen“. Wann eine Berücksichtigung als gegeben gelten darf, ist allerdings nicht geregelt. Sie liegt jedenfalls vor, wenn der Stand der Technik aufgrund anderer IT-Sicherheitsmaßnahmen oder -ziele begründet unterschritten wird. Das ist z.B. der Fall, wenn das Einspielen eines aktuellen Patches an anderer Stelle zu einem Abfall der IT-Sicherheit insgesamt führen würde. Die Unterschreitung des Standes der Technik setzt also eine tragfähige Begründung voraus, die sich ebenfalls auf die Sicherheit der Systeme bezieht.

Darüber hinaus müssen die Vorkehrungen nur realisiert werden, soweit dies „technisch möglich und wirtschaftlich zumutbar“ ist. Die Einschränkung der technischen Möglichkeit bezieht sich auf eine subjektive Unmöglichkeit, etwa wenn die Vorkehrung die Mitwirkung eines Dritten erfordert, so z.B. bei einer Kanalverschlüsselung. Für die wirtschaftliche Zumutbarkeit ist der finanzielle Einsatz mit dem Wirkungsgrad der Maßnahme ins Verhältnis zu setzen. Wird bei hohen Kosten die Sicherheit nur geringfügig gesteigert, muss die Maßnahme tendenziell nicht umgesetzt werden.

IT-Sicherheit beauftragen

Rechtlich und technisch stellen die neuen Pflichten hohe Anforderungen an die Unternehmen. Da die IT-Sicherheit zum Risikomanagement gehört, für dessen Mängel die Geschäftsleitung auch persönlich haften kann, sollte die Umsetzung des ITSiG nicht vernachlässigt werden. Dazu kann die Expertise Dritter in Anspruch genommen werden. Auch bei Einbeziehung von Dienstleistern und Beratern verbleibt die gesetzliche Verpflichtung aber stets beim Diensteanbieter.

Somit verlagert sich die Prüfung auf die vertragliche Ebene. Die Aufträge werden sich also in der Regel nicht auf die Implementierung einzelner IT-Sicherheitsmaßnahmen beschränken, sondern komplexe Maßnahmenbündel umfassen, die sich aus einer ausdrücklich mitbeauftragten Schutzbedarfsanalyse samt anschließender Auswahlentscheidung ergeben.

Ein wichtiger Tipp!

Es ist wichtig, die Ergebnisse von Schutzbedarfsanalyse und Auswahlentscheidung so zu dokumentieren, dass sich daraus die Gründe eines Zurückbleibens hinter dem Stand der Technik nachvollziehen lassen. Ohne eine Dokumentation lässt sich der Nachweis eines gesetzeskonformen „Berücksichtigens“ gegenüber der zuständigen Aufsichtsbehörde praktisch nicht führen.

RA Karsten U. Bartels LL.M.,
HK2 Rechtsanwälte

Elektronische Unterschrift per Handy

Eine neue EU-Verordnung soll das digitale Signieren bequem und zugleich sicher machen

Ab Juli 2016 kommt die Fernsignatur. Damit wird das Smartphone für die elektronische Unterschrift interessant. Doch welche Kompromisse sind nötig und möglich, um einerseits dem Komfort, andererseits aber auch einer hohen Dokumentensicherheit Rechnung zu tragen?

Mit fortschreitender Digitalisierung wird es immer wichtiger, auch Dokumente mit Unterschrift digital abzubilden – und das möglichst mit hoher Rechtsgültigkeit. Eine qualifizierte elektronische Signatur ersetzt die handschriftliche Unterschrift und sorgt für Urhebernachweis und Manipulationsschutz digitaler Dokumente. Bisher ist sie allerdings für die Nutzer, insbesondere für Privatpersonen, mit relativ hohen Umsetzungshürden behaftet, da eine Signaturkarte und ein Kartenleser erforderlich sind.

Europaweite Regelung

Ab 01.07.2016 gibt es da neue Möglichkeiten. Die „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ (eIDAS-VO) schafft europaweit standardisierte rechtliche und technische Rahmenbedingungen für elektronische Vertrauensdienste, zu denen auch digitale Signaturen zählen. Ein in der EU qualifiziert elektronisch signiertes Dokument muss dann in jedem Mitgliedsstaat anerkannt werden.

Hervorzuheben ist, dass die eIDAS-VO das Spektrum an elektronischen Signaturen erweitert. So soll die sogenannte Fernsignatur (auch Serversignatur) die Hürde zur Nutzung digitaler Signaturverfahren deutlich senken und eine Unterschrift mittels Handy – die sich in Österreich bereits hoher Beliebtheit erfreut – ermöglichen. Mit der Fernsignatur ist seitens der EU die Motivation verbunden, dass mit ihr vielfältige wirtschaftliche Vorteile realisiert werden können (vgl. Erwägungsgrund Nr. 52 eIDAS-VO).

Speicherung des Signaturschlüssels

Möglich wird die Handy-Signatur durch eine Änderung der Anforderungen für die Speicherung des privaten Signaturschlüssels. Dieser muss sich nach der eIDAS-VO nicht mehr im unmittelbaren Besitz des Signierenden befinden. Zur sicheren Speicherung des Schlüssels diente bisher die Signaturkarte mit ihrem Kryptochip. Nun kann er zentral von einem Vertrauensdiensteanbieter (VDA, Trustcenter) in einer sicheren Signaturerstellungseinheit in Form eines Hardware Security Module (HSM) gespeichert werden. Das erspart dem Endanwender die bislang notwendige Hardware wie Signaturkarte und Lesegerät, was zu einer erheblichen Steigerung des Komforts führen sollte.

Voraussetzung für die Nutzung des Fernsignaturdienstes ist, dass sich der Anwender bei einem qualifizierten VDA registriert und dabei auch belegbar identifiziert. Zukünftig kommt hierfür auch eine Online-Videoidentifizierung zum Einsatz. Anschließend wird ein geheimer Signaturschlüssel generiert und ein qualifiziertes Zertifikat ausgestellt. Für den Betrieb hat der VDA hohe Auflagen zu erfüllen, mit dem Ziel, dass der Endanwender den Signaturschlüssel unter seiner alleinigen Kontrolle behält. Es müssen eine Zertifizierung nach anerkannten Verfahren, z.B. Schutzprofile nach Common Criteria, eine regelmäßige Auditierung sowie die Überwachung durch eine Aufsichtsstelle erfolgen.

Quelle: secrypt GmbH

Die Kontrolle über den Signaturschlüssel bleibt beim Anwender.

Realisierung der Handy-Signatur

Derzeit befindet sich die Entwicklung der Fernsignatur an einem Scheideweg: Wird sie komfortabel nutzbar sein, aber dafür an Sicherheit einbüßen? Oder wird sie durch eine hochsichere Ausgestaltung zu umständlich und somit von den Anwendern abgelehnt? Fakt ist, dass das Einprägen von Passwörtern und PINs oder das Einsetzen kosten-

verursachender Hardware-Tokens wie Signaturkarten die Akzeptanz schmälern. Infolgedessen muss das Europäische Komitee für Normung (Comité Européen de Normalisation, CEN), das für die Ausgestaltung der Fernsignatur verantwortlich ist, eine Gratwanderung zwischen ausreichendem Komfort und notwendiger Sicherheit vollziehen. Keine einfache Aufgabe. Zudem erfolgt die Normierung im Spannungsfeld unterschiedlicher Interessengruppen. Während eine Fraktion rein softwarebasierte Lösungen auf Anwenderseite präferiert, die natürlich eine gewisse Verantwortung bei der Nutzung voraussetzen, stehen dem starke Absatzinteressen für hardwarebasierte Secure Elements entgegen.

Der im März veröffentlichte Normentwurf „Sicherheitsanforderungen für vertrauenswürdige Systeme, die Serversignaturen unterstützen DIN CEN/TS 419241-1“ legt die technikneutrale Umsetzung unter Berücksichtigung von Komfort und Sicherheit fest. Der Entwurf soll bis September finalisiert und bis März 2017 verabschiedet werden. Derzeit sieht er die Authentifizierung des Unterzeichners durch zwei Faktoren unterschiedlicher Kategorie (z.B. Besitz, Wissen, Biometrie) vor. Die Übertragung der beiden Faktoren muss über zwei unterschiedliche Interfaces und Kanäle erfolgen. Erst nach der Authentifizierung kann der Signaturschlüsselinhaber auf seinen privaten Schlüssel zugreifen.

Ein Beispiel für eine Zwei-Faktor-Authentifizierung: Faktor 1 – Anmeldung per Benutzername und Passwort über Kanal 1 (z.B. Workstation); Faktor 2 – Kryptografische Authentisierung über Kanal 2 (z.B. Fingerabdruck, mTAN oder PIN-Eingabe via Smartphone). Das Verfahren mit mTANs (mobile Transaktionsnummern) ist zwar bequem einsetzbar, wird jedoch für hohe Authentifizierungsniveaus kritisch bewertet. Eine neue Klasse von Schadsoftware ist darauf spezialisiert, mTANs abzufangen und an den Angreifer weiterzuleiten. Hier ist an den Signierenden und seine Sorgfaltspflichten zu appellieren.

Der Ablauf der Fernsignatur in einem unternehmerischen Geschäftsprozess könnte folgendermaßen aussehen (siehe Abbildung): 1. Der Nutzer öffnet eine Signaturanwendung (Nutzerkomponente) in seiner Arbeitsumgebung (Kanal 1), z.B. einem Dokumenten-Management-System, und meldet sich mit Benutzername und Passwort (Faktor 1) an. 2. Anschließend markiert er ein Dokument und betätigt die Schaltfläche „Signieren“. 3. Das Dokument wird dann zusammen mit weiteren Daten zum Schutz der Transaktion (SAD: Signaturaktivierungsdaten) über einen sicheren Kommunikationskanal (SAP: Signaturaktivierungsprotokoll) an den VDA gesendet. 4. Der VDA wiederum startet eine Authentifizierungsanfrage und der Anwender authentisiert sich z.B. mittels Fingerabdruck (Faktor 2) über eine App auf seinem Smartphone (Kanal 2). 5. Bei erfolgreicher Authentifizierung wird das Dokument mit dem beim VDA hinterlegten Signaturschlüssel signiert und 6. an die Nutzerkomponente des Anwenders gesendet.

Die Signaturaktivierungsdaten und das -protokoll sollen sicherstellen, dass der Signaturschlüssel ausschließlich durch den Inhaber verwendet wird. Die Aktivierungsdaten befinden sich unter alleiniger Kontrolle des Anwenders. Dabei wird die Authentisierung an die zu signierenden Daten und an den Signaturschlüssel gebunden. Der VDA prüft die Aktivierungsdaten mittels seines Fernsignaturmoduls, das er in einer manipulationssicheren Umgebung betreibt. Erst nach erfolgreicher Prüfung erfolgt die Signaturerzeugung innerhalb des Kryptomoduls. Das Signaturaktivierungsprotokoll gewährleistet dabei die sichere Übertragung der Aktivierungsdaten von der Nutzerkomponente zum Fernsignaturmodul.

Fazit

Die Fernsignatur wird voraussichtlich eine vereinfachte Signaturerzeugung ermöglichen und so vermutlich zu einer stärkeren Verbreitung elektronischer Signaturen führen – nicht nur im Businessalltag, sondern auch bei Privatanwendern. Mit ihr lässt sich die handschriftliche Unterschrift in vielen Szenarien ersetzen, etwa auf unternehmensbezogenen Dokumenten, im Gesundheitswesen und bei digitalen Amtswegen. Ihr Einsatz hängt allerdings entscheidend von der Ausgestaltung ab. Eine erfolgversprechende Umsetzung muss hohen Komfort bei gleichzeitig größtmöglicher Sicherheit gewährleisten. Es bleibt also spannend, ob am Ende eine praxistaugliche Lösung vor dem Hintergrund aktueller Sicherheitsdiskussionen auf den Weg gebracht werden kann.

Tatami Michalek,
Geschäftsführer secrypt GmbH

Neue Konzepte für eine sichere Authentifizierung

Die FIDO-Allianz bietet mit ihrem U2F-Protokoll ein breites Anwendungsspektrum

Immer mehr Geschäftsprozesse wandern in die Cloud. Das bringt viele Vorteile, doch die Online-Verfügbarkeit birgt auch Risiken. Eine wichtige Komponente dabei ist die sichere Authentifizierung der Nutzer. Fast immer kommen Benutzername/Passwort-Verfahren zum Einsatz, die jedoch einige Nachteile haben.

Die Online-Authentifizierung wird nach wie vor zu 99 % mit Benutzername/Passwort-Systemen (BPS) durchgeführt. Insbesondere gilt dies für Privatnutzer. Obwohl fast keine Woche vergeht, in der nicht irgendein Webdienst zugeben muss, Passwörter oder andere wichtige Kundendaten verloren zu haben. 2014 gab es fast jeden Monat einen signifikanten Angriff, u.a. auf eBay mit 145 Millionen gestohlenen Datensätzen und auf JP Morgan Chase (83 Millionen). Nach den Analysen des Gemalto Breach Level Index wurden 2014 über eine Milliarde Datensätze in mehr als 1500 sicherheitsrelevanten Vorfällen (Breaches) verloren oder gestohlen. 2015 belief sich der Verlust auf mehr als 707 Millionen Datensätze bei 1673 Vorfällen. Davon wurden etwa 307 Millionen Datensätze von Diensten der öffentlichen Verwaltung verloren oder gestohlen.

Experten gehen davon aus, dass in 80 % der Fälle gestohlene oder einfach zu ratende Passwörter verantwortlich sind. Warum gibt es, wie es scheint, kaum neue Technologien, die die überholte Nutzung von Benutzername/Passwort-Systemen beenden und durch moderne Verfahren ablösen?

Was ist Authentifizierung?

Der Duden beschreibt den Begriff Authentifizierung (engl. Authentication) kurz und knapp als „Identitätsprüfung eines Benutzers als Zugangs- und Rechtekontrolle für ein System (zum Beispiel durch ein Passwort)“. Dies kann im Prinzip auf drei verschiedene Arten erfolgen: wissensbasierte Authentifizierung (what you know) – z.B. PIN, Passwort, Passphrase oder die Antwort auf eine Sicherheitsfrage; besitzbasierte Authentifizierung (what you have) – z.B. Schlüssel, digitale Zertifikate, Chipkarten, Transaktionsnummer (TAN) oder Einmal-Passwörter (OTP); biometrische Authentifizierung (who you are) – z.B. Fingerabdruck-, Venenmuster-, Stimmen-, Iris- oder Gesichtserkennung.

Diese Authentifizierungsarten können auch kombiniert werden, um ein höheres Sicherheitsniveau zu erzielen. Die Abfrage eines Passwortes und das Beantworten einer Sicherheitsfrage gelten jedoch nicht als Zwei-Faktor-Authentifizierung (2FA), weil es sich bei beiden Abfragen um wissensbasierte Merkmale handelt. Eine Bankkarte mit PIN vereinigt hingegen die wissens- und besitzbasierte Authentifizierung und zählt daher zur echten Zwei-Faktor-Authentifizierung oder auch Multi-Faktor-Authentifizierung. Manche Anbieter erlauben eine Kombination von verschiedenen zweiten Faktoren mit dem Passwort, so z.B. Google (SMS, Einmal-Passwort, Cookie, USB Security Key), das sein Verfahren Zwei-Stufen-Authentifizierung (Two Step Verification) nennt.

Der Begriff „starke Authentifizierung“ (Strong Authentication) hat keine feste Definition. Je nach Hersteller kann damit Multi-Faktor-Authentifizierung per Einmal-Passwort wie auch per Authentifizierung über eine Public-Key-Infrastruktur (PKI) bzw. Zertifikate gemeint sein. Für die Europäische Zentralbank z.B. liegt eine starke Authentifizierung dann vor, wenn zwei oder mehr Elemente der Authentifizierungsarten kombiniert werden, die voneinander unabhängig sind.

Welche Rolle spielen Secure Elements?

Um ein höheres Vertrauensniveau zu erreichen, gibt es Systeme, die zu wissens- und besitzbasierten Faktoren auch noch biometrische Merkmale hinzuziehen. Die Smart Card Alliance sowie auch NIST (SP-800-63-1) haben vier Assurance Levels definiert, wobei Benutzername/Passwort-Systeme Level 1 erreichen. Für das höchste Sicherheitsniveau (Level 4) muss die Authentifizierung mithilfe kryptografisch abgesicherter Protokolle auf sicherheitszertifizierten Verschlüsselungs-Token stattfinden. Um diese Sicherheitsanforderungen zu erreichen, setzen im Prinzip alle Smart-Card- und USB-Key-Hersteller speziell geschützte, sogenannte gehärtete (tamper resistant) Sicherheitsmikrocontroller (Secure Elements) ein, für die eigene Sicherheitsevaluierungen wie beispielsweise Common Criteria existieren.

Secure Elements haben Ihr eigenes vor Seitenkanal- und anderen Angriffen geschütztes Betriebssystem sowie geschützte flüchtige und nichtflüchtige Speicherbereiche. Daneben gibt es spezielle Komponenten wie hardwarebasierte Zufallszahlengeneratoren (True Random Number Generators) oder verschiedene Coprozessoren, die symmetrische und asymmetrische Verschlüsselungsalgorithmen wie AES, RSA und ECC effektiv ausführen helfen. Dieser Aufwand wird betrieben, damit die geheimen Schlüssel nur innerhalb einer geschützten Umgebung aufbewahrt und verwendet werden.

Die Geheimhaltung der Schlüssel beruht auf Kerckhoffs Maxime, die besagt, dass die Sicherheit eines Verschlüsselungsverfahrens auf der Geheimhaltung des Schlüssels beruht und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus. Bei der symmetrischen Verschlüsselung gibt es nur einen Schlüssel, der auf beiden Seiten der Kommunikationspartner geheim gehalten werden muss. Bei der asymmetrischen Verschlüsselung hat jeder Kommunikationspartner zwei Schlüssel, einen öffentlichen und einen privaten (geheimen) Schlüssel. Typischerweise werden private Schlüssel nur innerhalb gehärteter Sicherheitsmikrocontroller erzeugt und können nicht exportiert werden.

Warum Passwörter?

Passwort-Systeme gibt es schon seit Tausenden von Jahren (Losungen oder Parolen). Sie bestanden oft aus einem Doppelwort, womit eine gegenseitige Authentifizierung durchgeführt werden konnte. Einen erneuten Einsatz fanden Passwörter dann mit dem Beginn der modernen IT-Welt. Der wohl wichtigste Grund, warum Benutzername/Passwort-Systeme zu den nach wie vor weitverbreitetsten Verfahren zählen, ist die relativ einfache Implementierung. Zudem entstehen beim Einsatz keine externen Kosten und es müssen keine technischen Geräte wie Chipkarten, Einmal-Passwort-Token, Kartenleser oder Fingerprintsensoren beschafft, installiert und an die Nutzer verteilt werden. Jedoch haben sie auch einige Nachteile, allen voran das generell schwache Sicherheitsniveau.

Auf Clientseite sind folgende Angriffe auf Passwort-Systeme typisch: Passwörter ausspähen (shoulder surfing), belauschen (Keylogger), ausprobieren (brute force/dictionary), Man-in-the-Middle (MITM) oder Phishing. Die Verwundbarkeit der Passwörter hat hierbei hauptsächlich der Nutzer in der Hand. Er muss dafür sorgen, dass der Rechner frei von Schadsoftware bleibt, dass er ein starkes Passwort benutzt, dass ihn niemand bei der Passworteingabe beobachtet, dass er die Nutzung von TLS sicherstellt und dass er nicht auf einer Phishing-Seite seine Logindaten eingibt. Serverseitig ist natürlich eine ganze Reihe von Angriffen auf den Webservice und dessen Systeme möglich. Auch darf die Kommunikation mit den Clients nur per TLS erfolgen. Insbesondere für die Passwortverarbeitung müssen spezielle Verfahren benutzt werden. Stand der Technik ist hier die Anwendung von Password-based Key Derivation Functions, die Hashwerte der Passwörter sowie Salts (zufällige Zeichenfolgen) benutzen.

Multi-Faktor-Authentifizierung

Im professionellen Umfeld wurden BPS schon vor langer Zeit um besitzbasierte Authentifizierungsmethoden erweitert. Sicherheitsanwendungen zur Multi-Faktor-Authentifizierung umfassen typischerweise Login, Festplatten- und E-Mail-Verschlüsselung, Virtual Private Networks, Web-Authentifikation, Single Sign-on sowie Systeme zur digitalen Signatur. Hierfür wurden diverse Zwei-Faktor-Systeme entwickelt, die sich grob in zwei Klassen einteilen lassen: Einmal-Passwort- und PKI- bzw. zertifikatbasierte Systeme. Sie unterscheiden sich geringfügig in der Benutzung, aber signifikant bei den Serverkomponenten.

Für den Server gibt es lokale Installationen, aber natürlich auch cloudbasierte Lösungen. Beide Systeme haben ihre Vor- und Nachteile, Bedrohungspotenzial und Systemanforderungen müssen genau bestimmt werden. Für beide Klassen stehen außerdem Software- und Hardwareprodukte zur Auswahl, wobei nur die hardwarebasierten PKI/Zertifikat-Systeme eine nach dem Stand der Technik ausreichend hohe Sicherheit garantieren können. Dies bezieht sich nicht nur auf die Qualität der Authentifizierung, sondern auch auf die Verwundbarkeit gegenüber anderen Angriffen. So können sie etwa gegen MITM, Man-in-the-Browser (MITB) und Phishing schützen.

Den Vorteilen stehen die Kosten für Integration, Distribution, USB Keys oder Smart Cards und weitere Hardwareanschaffungen entgegen. Einmal-Passwort-Systeme haben hingegen eine geringere Komplexität, sind schneller und einfacher auszurollen, können auch als Mobile App implementiert werden, sind als Hardware-Implementierung kostengünstiger und bedürfen keines freien USB-Ports oder Smart-Card-Lesers.

Auch im privaten Bereich hat sich die Multi-Faktor-Authentifizierung für einzelne Anwendungsbereiche durchgesetzt. Das gilt vor allem für das Online-Banking. Je nach Finanzinstitut und legislativem Umfeld gibt es eine Vielzahl von Möglichkeiten, angefangen von reinen Benutzername/Passwort-Systemen, Einmal-Passwort-Systemen auf Papier oder Token über Cookies oder Sicherheitsfragen, SMS- oder Mobile-App-Systeme bis hin zum PKI- bzw. zertifikatbasierten USB-Key- und Smart-Card-System mit zertifizierten Kartenlesern. Länderspezifisch sind die Anforderungen sehr unterschiedlich: In einigen Schwellenländern wie China oder Brasilien existieren höhere Sicherheitsanforderung für Online-Banking-Systeme als in manchen europäischen Ländern.

Akzeptanzprobleme

Für sicherheitskritische Anwendungen kann derzeit nur zu hardwarebasierten PKI/Zertifikat-Systemen geraten werden. Diese haben jedoch gewisse technische Einschränkungen, die vor allem im Endnutzerbereich eine wichtige Rolle spielen.

Interoperabilität: Smart Cards bzw. PKI-USB-Token und ihre Schnittstellen sind zum großen Teil standardisiert. Jedoch ist typischerweise die Interoperabilität zum Authentifikations-Server (Backend) begrenzt.

Middleware: Um Smart Cards bzw. PKI-USB-Token zur Authentifizierung für Sicherheitsanwendungen (Login, Festplatten- oder E-Mail-Verschlüsselung) benutzen zu können, ist üblicherweise zusätzliche Middleware (Clients) auf den Rechnern notwendig. Dies ist im stark fragmentierten Endanwenderbereich eher hinderlich.

PKI: Im Unternehmenseinsatz wird jedes Authentifizierungs-Token registriert (Issuance), die Zertifikate von einer Certificate Authority (CA) signiert, in einer PKI verwaltet und dann an einen bestimmten Nutzer ausgegeben. Das ist im Endnutzerbereich ebenfalls unerwünscht.

Anonymität: Im Vergleich zum Unternehmenseinsatz, in dem Anonymität nicht erwartet werden kann, spielt diese für die Akzeptanz bei Privatnutzern eine wichtige Rolle.

All diese Punkte, die erklären, warum zertifikatbasierte USB-Key- und Smart-Card-Systeme – trotz der überragenden Vorteile für die IT-Sicherheit – keine große Verbreitung in Endnutzeranwendungen gefunden haben, sowie die Einschränkungen von BPS stellten die Ausgangslage für die Gründung der FIDO-Allianz 2012 dar.

Die FIDO-Allianz

FIDO steht für Fast IDentity Online. Ziel der FIDO-Allianz ist es, gängige Benutzername/Passwort-Verfahren abzulösen und die Online-Authentifizierung einfacherer und sicherer zu machen. Um dies zu erreichen, entwickelt die Allianz mithilfe ihrer Mitglieder offene technische Spezifikationen, die sichere interoperable Mechanismen zur Verfügung stellen. Darunter sind auch Vorschriften, die sich um Sicherheits- und Zertifizierungsaspekte kümmern. Sie betreibt Programme, die helfen sollen, eine erfolgreiche weltweite Einführung der Spezifikationen zu gewährleisten, und reicht technische Spezifikationen bei anerkannten Standardisierungsorganisationen ein, um die formelle Standardisierung zu ermöglichen.

Die FIDO-Allianz ist weltweit aktiv, wobei ein Schwerpunkt auf Nordamerika liegt, weil hier die ersten Diensteanbieter FIDO-Technologie in ihre Anwendungen integrierten. Die Anzahl der Mitglieder ist bisher auf über 250 Firmen angewachsen, darunter viele Anbieter für Authentifizierungslösungen, aber auch Geräte- und Halbleiterhersteller, Biometriefirmen, Finanzdienstleister, Online- sowie Gesundheitsdiensteanbieter.

Bisher wurden zwei Gruppen von Spezifikationen veröffentlicht. Das Universal Authentication Framework (UAF) ist ein Protokoll, das für die

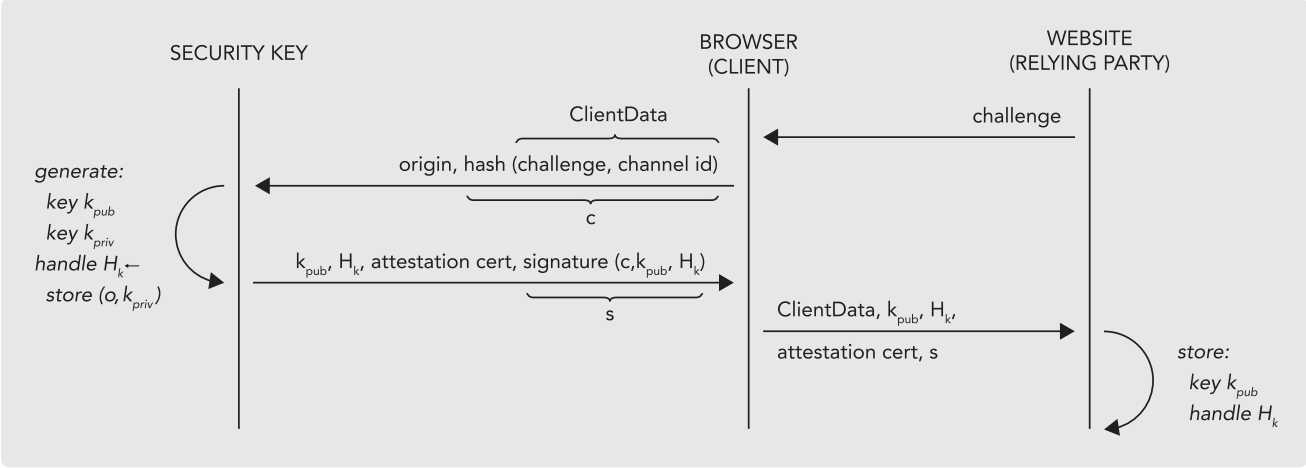
FIDO-Unterstützung auf mobilen Geräten gedacht ist und eine sichere Multi-Faktor-Authentifizierung ermöglicht. Dafür muss es hardware- und softwaretechnisch integriert sein. Dies kann in Kombination mit biometrischen Sensoren, aber auch mithilfe von Secure Elements, Trusted Execution Engines (TEE) oder Trusted Platform Modules (TPM) verwirklicht werden. Das Universal Second Factor (U2F) Protocol erlaubt Online-Dienstleistern die Ergänzung ihrer Benutzer/Passwort-Authentifizierung mit einem sicheren Public-Key-basierten Token. Da das bisher genutzte BPV bestehen bleibt, lässt sich U2F relativ leicht nachträglich realisieren.

Beide Lösungen, UAF und U2F, benutzen kryptografische Verfahren, die dem aktuellen Stand der Technik entsprechen. Während die technischen Arbeitsgruppen für UAF und U2F sich um Erweiterungen der derzeitigen Spezifikationen kümmern, gibt es bereits eine Arbeitsgruppe, die das FIDO-2.0-Projekt weiterentwickelt, das beide Protokolle vereinen soll. Darüber hinaus arbeitet die FIDO-Allianz mit dem World Wide Web Consortium (W3C) zusammen und hat technische Spezifikationen eingereicht, um das Web-API zu definieren und als Standard zu verabschieden. Damit wird FIDO in der Betriebssystemebene der verschiedenen Plattformen integriert.

U2F ist ein relativ einfach aufgebautes Challenge-Response-Protokoll, das eine gesicherte TLS-Verbindung zwischen Browser und Webserver erfordert. Die Anwendung besteht aus zwei Phasen: Registrierung und Authentifizierung. Die Registrierung findet einmal pro Account statt, wobei der Nutzer sich per Benutzername und Passwort anmelden muss und dann in den Kontoeinstellungen ein U2F-Token als Zwei-Faktor-Device registrieren kann. Bei jeder Authentifizierung protokolliert das Token die URL bzw. Web Origin, um Phishing-Angriffe zu vereiteln. Bei jedem Login wird nach Benutzername und Passwort gefragt sowie das Token verlangt, bei dem dann per Tastendruck der Login bestätigt wird.

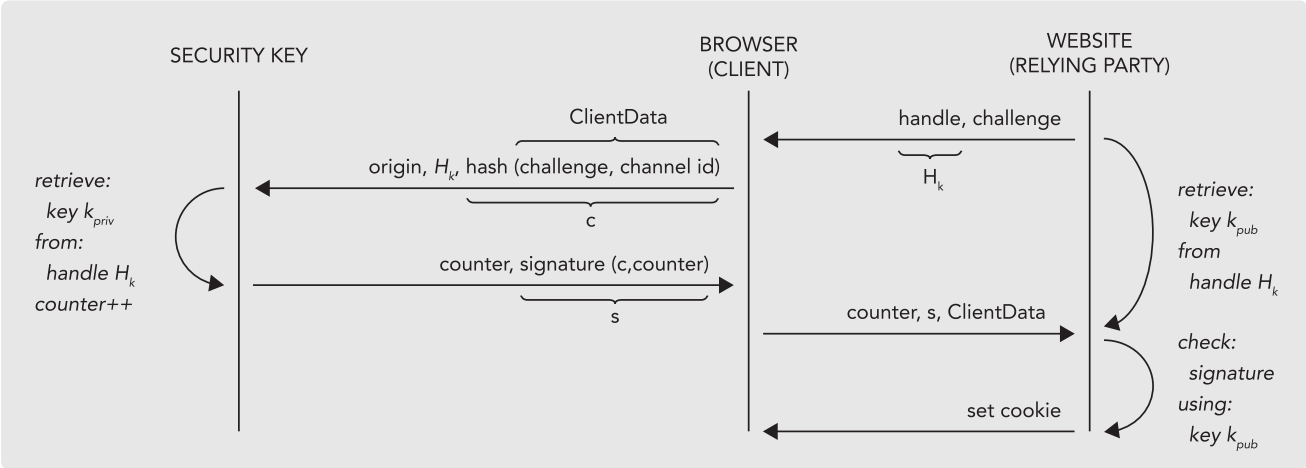
Das U2F-Protokoll

Abbildung 1 beschreibt im Detail die Protokollschritte bei der Registrierung: Fordert der Benutzer die Registrierung eines Keys an, sendet der Server eine zufällige Challenge. Der Browser verpackt die Challenge und die Channel-ID in die Client Data. Dann sendet der Browser die Server Web Origin und den Hash über die Client Data an das Token, das daraufhin ein Server-spezifisches Schlüsselpaar generiert und das Key Handle berechnet. Danach sendet das Token den öffentlichen Schlüssel, das Key Handle, das Attestation-Zertifikat sowie eine Signatur. Der Browser leitet alles zusammen mit der Client Data zurück an den Server. Dieser kann nun die Signatur mithilfe des öffentlichen



Quelle: FIDO Alliance

Ablauf der Kommunikation: Registrierung (Abb. 1)

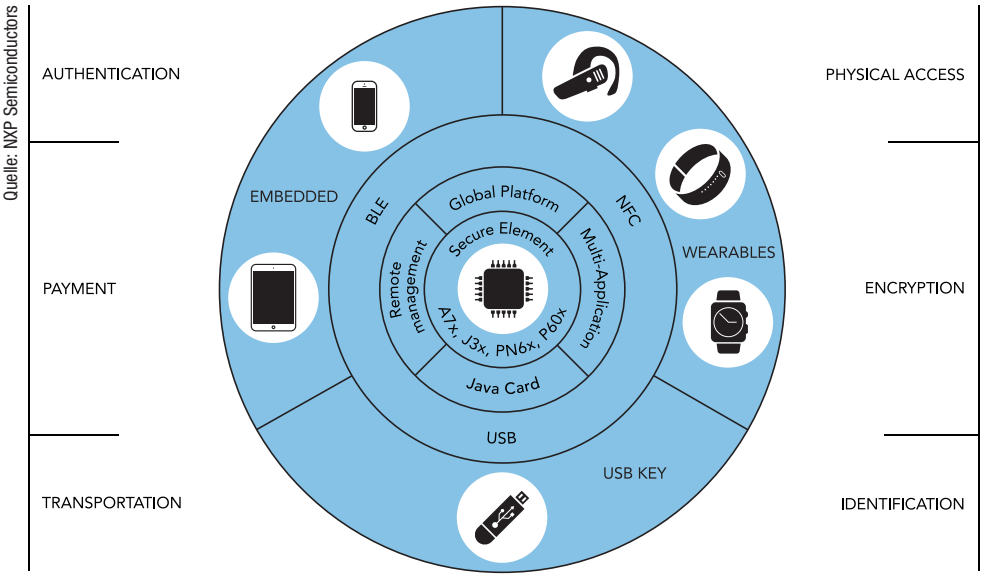


Quelle: FIDO Alliance

Ablauf der Kommunikation: Authentifikation (Abb. 2)

Schlüssels überprüfen und speichert das Key Handle sowie den öffentlichen Schlüssel zum jeweiligen User. Für das Signieren wird ECDSA über NIST P-256 benutzt. Für das Hashing SHA-256.

Abbildung 2 zeigt die Protokollschritte bei der Authentifizierung. Dabei sendet der Server das gewünschte Key Handle und eine Challenge an den Browser. Der Browser generiert die Client Data und sendet den Hash der Client Data, das Key Handle und die Serveridentität an das Token. Wenn das Token dieses Key Handle nicht erkennt oder das Key Handle nicht zur Serveridentität passt, verweigert das Token die Signaturanfrage. Falls beides korrekt ist, signiert das Token die Client Data mit seinem privaten Schlüssel. Zudem signiert es noch zwei weitere Attribute: einen bestandenen Benutzeranwesenheitstest und einen Counter. Der Browser sendet diese Daten an den Server, der wiederum die Signaturen mithilfe des gespeicherten öffentlichen Schlüssels überprüft.



Transportmechanismen und Funktionen (Abb. 3)

Bisher sind in U2F drei verschiedene Transportmechanismen definiert, um möglichst viele Endgeräte zu unterstützen: USB, NFC und Bluetooth LE, wobei USB und NFC schon in der finalen Version vorliegen. BLE folgt voraussichtlich im Sommer 2016. Die verschiedenen Transportmechanismen, die bisher definiert sind, erlauben eine Vielzahl von Formfaktoren für Secure-Element-basierte U2F-Token. Dies geht von diversen USB- sowie USB/NFC-Token, reinen NFC-Token und Wearables (als BLE-only oder in Kombination mit USB und/oder NFC) bis hin zu Embedded Secure Elements in mobilen Geräten wie Mobiltelefonen oder Tablets.

Die Kommunikationsschnittstelle auf der Clientseite kann auf verschiedene Arten implementiert werden. Bisher ist sie mit dem Chrome-Browser nur auf PCs, Laptops und dem Macintosh verfügbar, jedoch für alle relevanten Betriebssysteme (Windows, MacOS, Linux, ChromeOS). Microsoft hat im Februar 2015 FIDO-Unterstützung für Windows 10 zugesagt, in der derzeit ausgerollten Version ist sie jedoch noch nicht enthalten. Mozilla arbeitet an einer Integration in den Firefox-Browser, für den U2F als Add-on bereits vorliegt. Weitere Browser lassen sich relativ schnell per Add-on, Extension oder Plug-in erweitern.

Daneben gibt es noch einige native Client-Implementierungen, die für den Einsatz in Unternehmensumgebungen entwickelt wurden. Für mobile Endgeräte gibt es U2F-Unterstützung derzeit nur unter Android (NFC, BLE und per App). Verschiedene Hersteller bieten U2F-Apps bzw. U2F-Frameworks für weitere mobile Betriebsysteme an. Server können entweder vom Diensteanbieter selbst betrieben werden oder als Cloud-Service angebunden sein.

Warum FIDO?

Die wichtigsten Vorteile der FIDO-Lösungen liegen in der einfachen Nutzung und dem hohen Sicherheitsniveau. Sie bieten Schutz gegen MITM und Phishing, sind relativ unaufwendig zu implementieren, herstellerunabhängig und interoperabel, benötigen keine PKI, wahren die Anonymität der Endnutzer und erfordern keine Middleware-Installation.

Im Unternehmenseinsatz finden sich noch weitere Vorteile. Google z.B. bescheinigt eine gestiegene Produktivität (weniger fehlgeschlagene Authentifizierungen) und betont, dass die Hardwarekosten durch geringere Supportkosten aufgewogen werden.

U2F ist bei einigen Dienstanbietern auch für Privatanwender schon seit Jahren verfügbar. Google etwa unterstützt seit 2010 die Zwei-Faktor-Authentifizierung, die mittlerweile mit U2F-Hardware-Token auch per App auf mobilen Geräten funktioniert. 2015 folgten Dropbox und Github. Zuletzt ging im März 2016 mit UK.GOV/Verify das englische Bürgerportal mit FIDO-U2F-Unterstützung live.

Daneben befasst sich eine ganze Reihe von Projekten mit dem Einsatz in Unternehmensumgebungen. Ein zusätzlich mit CCID- und Crypto-API-Unterstützung ausgestattetes Token kann U2F und alle geläufigen Sicherheitsanwendungen wie Login, Festplattenverschlüsselung, E-Mail-Verschlüsselung, Virtual Private Networks, Web Authentifikation, Single Sign-on sowie Systeme zur digitalen Signatur absichern.

Fazit

Es ist erschreckend, mit welcher Gelassenheit die regelmäßigen Berichte über Datenverluste im Millionenmaßstab zur Kenntnis genommen werden und wir uns nach wie vor schwertun, auf dem schmalen Grat zwischen Sicherheit und Benutzerfreundlichkeit nicht zu stolpern. Das Risiko realer Schäden ist bekannt, und die Aussicht, Opfer eines Identitätsdiebstahls zu werden, ist nicht verlockend. Dennoch scheinen viele diese Gefahr nicht ernst zu nehmen.

Seit Langem existieren Methoden für eine sichere Authentifizierung, doch sie haben sich aufgrund spezifischer Einschränkungen bisher nicht auf breiter Basis durchsetzen können. Entweder sind die Hürden für die Diensteanbieter zu hoch, oder das Interesse der Nutzer ist (noch) zu gering. Mit der FIDO-Technologie besteht nun eine reelle Möglichkeit, Methoden starker Authentifizierung weitaus mehr interessierten Nutzern zur Verfügung zu stellen und damit das Internet für uns alle sicherer zu machen.

Michael Poitner,
Global Segment Marketing Director,
Cyber Security Solutions

Den Gefahren der Zukunft auf der Spur

Post-Quantum-Kryptografie setzt neue Maßstäbe für Verschlüsselungsverfahren

Die NSA-Affäre hat uns gezeigt, welche Macht einzelne Gruppierungen in unserer vernetzten Welt haben. Es geht aber nicht allein um massenhafte Bespitzelung, sondern auch um ein weithin unterschätztes Problem: praxistaugliche Quantencomputer, die herkömmliche kryptografische Verfahren angreifen können.

Man stelle sich vor, dass von heute auf morgen alle Sicherheitsmaßnahmen unserer IT-Systeme ausgehebelt sind. Hacker haben Zugriff auf praktisch jedes vernetzte Informationssystem und können nach eigenem Ermessen Daten manipulieren. Die Konsequenzen eines solchen Szenarios wären dramatisch. Natürlich verfügen wir heute über verschiedene, gut untersuchte kryptografische Primitive, beispielsweise starke Chiffren, Signaturverfahren oder Hashfunktionen, die relevante Subsysteme absichern. Mit aktuellen Rechnern und selbst riesigen Rechenzentren könnten sie nicht oder nur mit riesigem Aufwand gebrochen werden.

Apokalypse der vernetzten Welt

Gäbe es aber bereits einen skalierbaren Quantenrechner, wären alle heute im Einsatz befindlichen asymmetrischen Verfahren, wie RSA für Verschlüsselung, Diffie-Hellman für den Schlüsselaustausch, DSA für digitale Signaturen und viele weitere, nicht mehr sicher einsetzbar. Aber auch symmetrische Kryptosysteme, etwa AES oder Hashfunktionen wie SHA2, verlören wesentlich an Sicherheit. Darauf aufbauende Sicherheitsprotokolle, wie TLS, SSH und IPsec zur vertraulichen Kommunikation über das Internet, würden ebenfalls keine Sicherheit mehr bieten. Und Angreifern wäre es möglich, sich unbemerkt in Verbindungen einzuklinken und diese abzuhören oder zu manipulieren. Im E-Commerce gäbe es keine sichere Zahlung mehr, Online-Banking wäre aus sicherheitstechnischer Sicht undenkbar. Auch bei kritischen Infrastrukturen gäbe es Probleme: Netze von Energieversorgern, Behörden, Militär, Krankenhäusern und Mobilfunkunternehmen könnten keine sichere Kommunikation mehr bieten.

Post-Quantum-Kryptografie

Die Ursprünge der Quantencomputer gehen in die frühen 1980er-Jahre zurück. Nachdem der Nobelpreisträger Richard Feynman bestehende Grundideen ausgearbeitet hatte, legte der Physiker David Deutsch 1985 ein Berechnungsmodell für Quantencomputer vor. Zunächst wurden diese Ideen vom Großteil der Fachwelt als Spielerei abgetan. Doch 1994 zeigte Peter Shor, dass es tatsächlich möglich ist, zwei bestimmte kryptografische Probleme mit solchen hypothetischen Rechnern zu lösen. 2001 lieferte dann IBM einen praktischen Nachweis für die Verwendbarkeit des Shor-Algorithmus. Das warf die Frage auf, wie man sich gegen den neuartigen Algorithmus wappnen könnte. Über die folgenden Jahre wurden quantenresistente kryptografische Verfahren entwickelt. In den Fokus der Medien geriet das Thema erst 2013, als die durch Edward Snowden veröffentlichten Dokumente belegten, dass sich die NSA auch mit Post-Quantum-Kryptografie beschäftigt. Die NSA hat mittlerweile die empfohlenen Schlüssellängen gängiger kryptografischer Verfahren deutlich erhöht und sucht nach neuen Standards, die in der Post-Quantum-Ära noch als sicher einzustufen sind. Auch das amerikanische NIST und Organisationen wie ETSI oder IETF interessieren sich verstärkt für das Thema.

Wie funktionieren Quantencomputer?

Im Gegensatz zu klassischen Rechnern, die auf der Verarbeitung diskreter Zustände 0 und 1 basieren, nutzen Quantencomputer Überlagerungen dieser beiden Möglichkeiten, sogenannte Quantenbits, kurz: Qubits. Ein Qubit wird durch ein quantenmechanisches System mit zwei Grundzuständen $|0\rangle$ und $|1\rangle$ realisiert und rechnet gewissermaßen gleichzeitig mit den beiden möglichen Ergebnissen 0 und 1 (Abbildung 1).

Mehrere Qubits werden mittels Verschränkung zu einem größeren quantenmechanischen System verbunden, das mehr als zwei verschiedene mögliche Grundzustände hat, korrespondierend zu den denkbaren Ergebnissen der Berechnung. Der Einsatz von Qubits ermöglicht ein völlig neues Berechnungsmodell, das Probleme weitaus schneller lösen kann als herkömmliche Rechenprozesse.

Für die Kryptografie hat das weitreichende Konsequenzen. Bislang beruht die Sicherheit von Verschlüsselungsverfahren auf der Annahme, dass man mit heutigen Mitteln den zugehörigen Schlüssel durch Ausprobieren nicht finden kann. Daher haben gängige Standards, wie der Advanced Encryption Standard (AES), Schlüssellängen von mindestens 128 Bit. Zum Finden des Schlüssels benötigt ein Angreifer mit einem Brute-Force-Angriff auf AES-128 also etwa 2^{128} Operationen. Das entspricht mit modernen CPUs etwa 3 000 000 Billionen CPU-Jahren und liegt jenseits des heute Machbaren. Mit dem Grover-Algorithmus könnte man AES-128 bereits in ungefähr 2^{64} (Quanten-)Operationen brechen – mit 1,74 CPU-Jahren durchaus möglich. Demnach wäre es künftig notwendig, AES mit 256 Bit Schlüssel zu verwenden, um eine mit heute vergleichbare Sicherheit zu erhalten.

Auch asymmetrische Verschlüsselungsverfahren wie RSA könnten mit Quantenrechnern leicht gebrochen werden. Im Gegensatz zu den oben erwähnten symmetrischen Verfahren sieht die Situation sogar noch viel schlechter aus. Es genügt nicht, einfach längere Schlüssel zu verwenden. Dies trifft auch auf zahlreiche weitere kryptografische

Verfahren wie den verbreiteten Diffie-Hellman-Schlüsselaustausch zu, und es ist nicht absehbar, welche Fortschritte im Bereich der Angriffsmethodik demnächst gemacht werden.

Falltüren in der Quantenwelt

Deshalb ist es ein zentrales Forschungsthema der Kryptografie, geeignete Kandidaten für die Post-Quantum-Ära zu finden und zu analysieren. Man benötigt dazu mathematische Probleme, mit denen man eine sogenannte Falltür umsetzen kann. Das kann man sich wie einen Briefkasten vorstellen, in den jemand eine Nachricht einwirft, die nur von einem Empfänger mit dem richtigen Schlüssel gelesen werden kann. Kandidaten dafür gibt es viele: multivariate oder gitterbasierte Systeme, Algorithmen auf Basis von fehlerkorrigierenden Codes, hashbasierte Verfahren, Isogenien von supersingulären elliptischen Kurven und algebraische Probleme mit Gröbnerbasen. Dank der Forschung der letzten Jahre nimmt das Verständnis für die Sicherheit dieser Systeme zu, doch sowohl in der Theorie als auch in der Praxis steht noch einiges an Arbeit an.

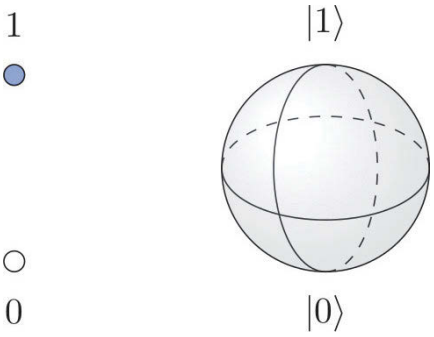
Dabei sind einige Verfahren seit Jahrzehnten bekannt, blieben aber uninteressant, weil sie aus damaliger Sicht zu rechenintensiv waren oder zu große Schlüssel nutzten. So benötigen manche Post-Quantum-Verfahren bei erhöhten Sicherheitsansprüchen bereits mehrere Megabyte große Schlüssel – statt wenigen Kilobytes wie bei RSA. Auch bei den Protokollen zeigt sich, wie sehr man früher auf möglichst kleine Datenmengen bedacht war. In der Datenkommunikation gibt es Größenbeschränkungen, die wegen Speicherbedarf und Geschwindigkeit zwar gewünscht, aber aus heutiger Sicht nicht mehr nötig sind.

Aus diesem Grund setzten sich über die Jahre nur einige wenige Primitive durch, im Bereich der symmetrischen Kryptologie etwa (Triple-) DES oder später AES, bei den asymmetrischen Kryptosystemen z.B. RSA, DSA und ECDSA. Dies führte zu fast monopolistischen Verhältnissen, bei denen in der Praxis neben theoretischen Sicherheitsresultaten insbesondere darauf vertraut wurde, dass lange genug niemand einen effizienten Angriff fand. Erst als in den 1990ern klar wurde, dass sowohl Quantencomputer als auch die Anwendung praxisrelevanter Quantenalgorithmen keine Hirngespinste sind, begann man, Alternativen zu suchen.

Vorhandene Lösungsmodelle

Will man Post-Quantum-Verfahren einsetzen, so führt kaum ein Weg an einer Veränderung mancher Schranken vorbei. Dennoch ist die Optimierung bekannter bzw. Konstruktion ähnlicher oder neuer Algorithmen wichtig und ein Ziel der aktuellen Forschungen. Schließlich will man langsamere Geschwindigkeiten und höheren Speicherbedarf nicht zwangsweise in Kauf nehmen. Doch genau diese Optimierungen ermöglichen auch neue Angriffe. So nutzt etwa das Verschlüsselungssystem von McEliece sogenannte fehlerkorrigierende Codes. Mit einem öffentlichen Schlüssel wird die Nachricht in einen solchen Code eingebettet und lässt sich nur mit dem privaten Schlüssel finden. Gegen dieses Kryptosystem kennt man bis heute keine starken Angriffe, nicht einmal mit Quantenalgorithmen. Die Schlüsselgrößen sind jedoch beträchtlich. Deshalb wurde versucht, das Verfahren zu verbessern, indem man die Wahl des Codes einschränkt. Doch genau das ermöglichte es wieder, optimierte Systeme zu brechen.

Andere Post-Quantum-Kryptosysteme setzen auf sogenannten Gittern auf. Diese kann man sich als regelmäßig angeordnete Punkte in einem Raum vorstellen. In niedrigen Dimensionen, z.B. zweidimensional, wäre es relativ einfach – indes nicht offensichtlich –, für einen beliebig gesetzten Punkt in der Ebene herauszufinden, wo sich der nächste Punkt befindet (Abbildung 2). Für höhere Dimensionen steigt der Rechenaufwand aber enorm an, und man kann auf dem Problem eine Falltür aufbauen. Aber es ist noch weitere Arbeit nötig, um die Verfahren effizienter und praktikabler zu gestalten.

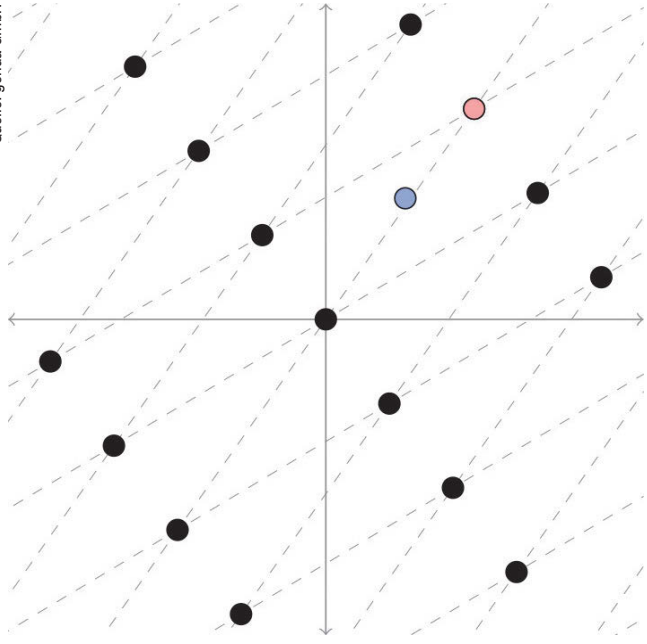


Quelle: genua GmbH

Im Gegensatz zu einem Bit, das die Werte 0 oder 1 annehmen kann (links), sind bei einem Qubit alle auf einer Kugel befindlichen Punkte möglich (rechts). Die Messung ergibt entweder den Südpol |0⟩ oder den Nordpol |1⟩. (Abb. 1)

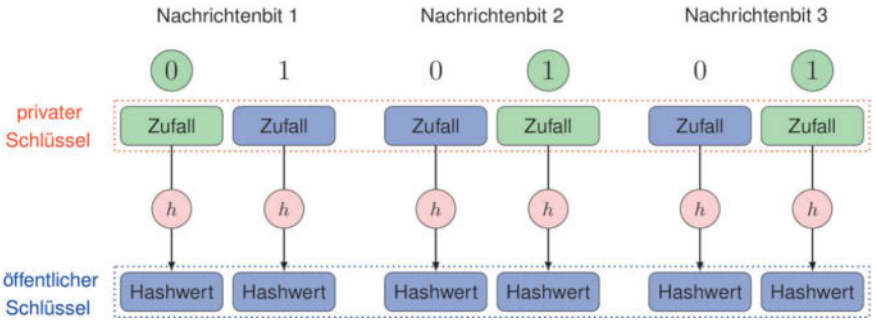
Hashbasierte Signaturen

Besser schneiden hier hashbasierte Signaturen ab. Damit lassen sich Daten nur signieren, aber nicht verschlüsseln. Die zugrundeliegende Theorie ist gut verstanden und die Sicherheit solide einschätzbar. In der Praxis nutzt praktisch jedes Signaturverfahren eine Hashfunktion, um eine große Nachricht auf einen Hashwert fester Länge zu verkleinern, der dann signiert wird. Das heutige Sicherheitsniveau kann gewisser-



Quelle: genua GmbH

Ein zweidimensionales Gitter. Es ist gar nicht so leicht zu erkennen, dass der rote Gitterpunkt dem (nicht auf dem Gitter befindlichen) blauen Punkt am nächsten ist. Das Problem, den roten Punkt aus dem blauen zu berechnen, bildet die Grundlage mancher quantenresistenter Verschlüsselungsverfahren. (Abb. 2)



Quelle: genua GmbH

Das quantenresistente Lamport-Signaturverfahren für die Nachricht 011. Die Signatur (grün) kann überprüft werden, indem man blockweise die Hashfunktion h mit den Elementen des öffentlichen Schlüssels vergleicht. (Abb. 3)

maßen in einer Post-Quantum-Ära gehalten werden, indem man die Ausgabelänge verdoppelt.

Als Basisbaustein dienen Einmalsignaturverfahren wie das von Lamport aus dem Jahre 1979 (Abbildung 3): Für jedes mögliche Bit einer Nachricht werden zwei Zufallswerte generiert. Der private Schlüssel besteht aus diesen Zufallswerten, der öffentliche aus den Hashwerten der einzelnen Blöcke des privaten Schlüssels. Abhängig von der Nachricht werden die zugehörigen Elemente des privaten Schlüssels als Signatur ausgegeben. Der Empfänger kann nun die per Signatur erhaltenen Werte durch Hashen mit den entsprechenden Bestandteilen des öffentlichen Schlüssels vergleichen.

Damit lässt sich für ein Schlüsselpaar aber nur eine einzelne Nachricht unterschreiben, da jede Signatur Segmente des privaten Schlüssels verrät. Man benötigt also eine Vielzahl an Schlüsselpaaren. Da man nicht für jede einzelne Nachricht dem Empfänger einen öffentlichen Schlüssel zukommen lassen will, nutzt man sogenannte Merkle-Bäume. Damit lässt sich die Vielzahl an Schlüsselpaaren zu einem großen öffentlichen Schlüssel vereinen. Durch die Einfachheit des Verfahrens wurden inzwischen nachweisbar sichere Verbesserungen eingeführt. Für E-Mail- oder Update-Signaturen lassen sich hashbasierte Verfahren wie das moderne eXtended Merkle Signature Scheme (XMSS) einfach und sicher einsetzen.

Die Zukunft der Kryptografie

Bei neuen Verfahren sind Experten verständlicherweise vorsichtig. Doch nur in realen Einsatzszenarien lässt sich zeigen, wie gut ein Verfahren läuft und welche Angriffe eventuell möglich sind. Oft kann ein Ersteinsatz auch hybrid mit etablierten Mechanismen erfolgen und bei Unstimmigkeiten auf das bewährte System zurückgegriffen werden.

Wer sich langfristig (etwa 30 Jahre) absichern will, sollte übergangsweise größere Schlüssellängen verwenden, bevor er vollständig auf Post-Quantum-Verfahren umsteigt. Mit einem 4096 Bit langen RSA-Schlüssel wird man auch die initiale Phase praxistauglicher Quantencomputer überstehen. Heutige Quantencomputer arbeiten mit nur wenigen Qubits und sind von realen Anwendungen noch weit entfernt. Doch können sie einmal kryptografische Systeme angreifen, verhindert letztlich nur noch der immense Material- und Kostenaufwand das Knacken größerer Schlüssel. So viele Fragen auch noch offen sein mögen: Wir glauben immer, aktuell an der Grenze des Möglichen zu arbeiten. Bis jemand kommt, der es besser weiß.

Stefan-Lukas Gazdag und Daniel Loebenberger, genua GmbH

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.), Martin Fuhrmann (Redaktion), Rudolph Schuster (Lektorat)

Autoren dieser Ausgabe:
Karsten U. Bartels, Fabian Bendun, Stefan-Lukas Gazdag, Mareike Gehrmann, Christian Jacobs, Harald Kesberg, Daniel Loebenberger, Tatami Michalek, Dr. Holger Mühlbauer, Michael Poitner, Dr. Volker Scheidemann, Paul Voigt

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

Korrektorat:
Kathleen Tiede, Hinstorff Verlag, Rostock

Titelbild:
© shutterstock, Max Griboedov; Collage: Matthias Timm, Hinstorff Verlag, Rostock

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.

qSk!lls
innovation through education

Wir setzen auf Qualität.
Setzen Sie sich zu uns.

Gestalten Sie Ihre Zukunft ...

... mit IT-Trainings von qSkills

Save the date!
qSkills
Security Summit
am 17.10.16

Als unabhängiges IT-Trainingsunternehmen bietet qSkills professionelle und qualitativ hochwertige Schulungen in den Bereichen IT-Management und Security & Awareness.

qSkills arbeitet mit mehr als 170 freiberuflichen Trainern zusammen, rund 200 verschiedene Kurse sind im Angebot. Das Nürnberger Trainingscenter ist mit 200 Workstations und einem hochmodernen Rechenzentrum ausgestattet, welches den Kursteilnehmern zur Verfügung steht. Weitere Standorte befinden sich in Hamburg, Frankfurt, München, Wien und Zürich.

Haben wir Ihr Interesse geweckt?

Aktuelle Kurs-Highlights:

- Cloud - Sinnvoll für mein Unternehmen?
- Industrial Security kompakt für:
  - IT-Experten
  - Produktionsexperten
- Hacking & Digitale Forensik
- OpenStack - IaaS Cloud Computing
- Docker - Container-Verwaltung

qSkills GmbH & Co. KG
Süd-West-Park 65
D-90449 Nürnberg

info@qskills.de
www.qskills.de

Für Code-Piloten

Jetzt für **9,90 €** bestellen.

shop.heise.de/ct-programmieren2016 service@shop.heise.de

Auch als digitale Ausgabe erhältlich unter: shop.heise.de/ct-programmieren2016-pdf

heise shop

shop.heise.de/ct-programmieren2016

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