Eine Themenbeilage der
Heise Medien GmbH & Co. KG

I 2018

# SICHERHEIT & DATENSCHUTZ

## EU-DSGVO, Verschlüsselung und Cyber Security

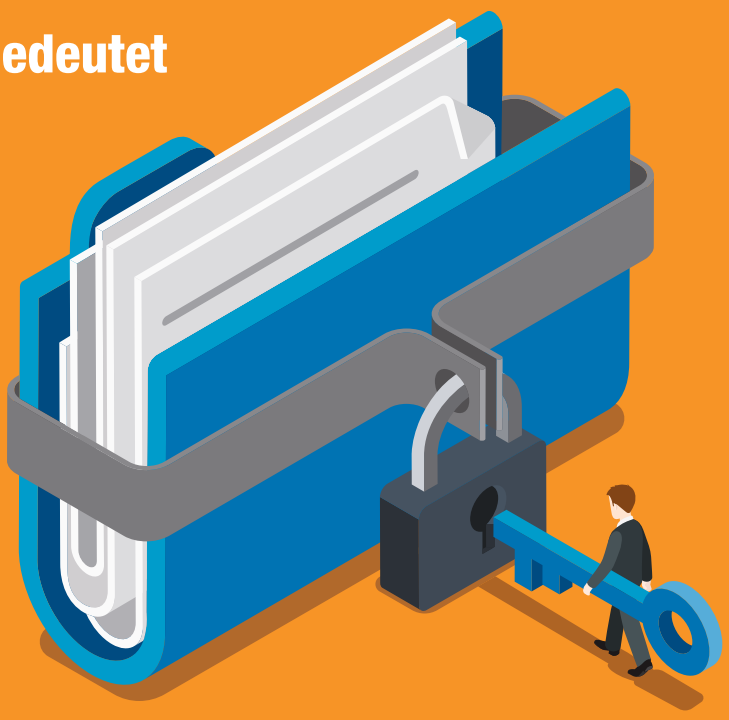
Identity Management:
**Wo Passwörter nicht mehr ausreichen**

EU-DSGVO:
**Was „Stand der Technik“ bedeutet**

Verschlüsselung:
**Wo Krypto-Software ansetzen muss**

Cyber Security:
**Warum vorher besser ist als nachher**

Security by Design:
**Wie DSGVO-Vorgaben umgesetzt werden**



BYOD:
**Wann Mobilgeräte datenschutzkonform sind**

Schadsoftware:
**Wie Malware Sandboxen überlistet**

Ausbildungsinitiative:
**Wer in KMU für Datensicherheit sorgt**

www.it-security-und-management.de

powered by: TeleTrusT Pioneers in IT security. iX

# INTERNET SECURITY DAYS 2018

**20. – 21. September**
**Phantasialand, Brühl**

## FACHMESSE, KONFERENZ, NETWORKING – DIE PLATTFORM FÜR SECURITY-EXPERTEN

Am 20. & 21. September finden die Internet Security Days in Brühl unter dem Motto **„Cybercrime: Vorbeugen – Abwehren – Reagieren"** statt. Im Mittelpunkt stehen dieses Jahr die Themen **Cybercrime, Rechts- und Normenrahmen, Zukunftstechnologien** und **Tipps und Tricks für den Unternehmensalltag**.

Erstmals können Interessierte neben dem Vortragsprogramm ihr Wissen in **Fachworkshops** vertiefen. Die zweistündigen Zusatzangebote vermitteln beispielsweise Details zur Absicherung anfälliger Windowssysteme, zum Schutz vor Wirtschaftsspionage, zur Umsetzung der Datenschutzgrundverordnung und mehr. Über aktuelle Security-Produkte informiert eine **begleitende Ausstellung**. Sich vernetzen oder einfach entspannen können alle Teilnehmer schließlich beim **Abendevent im Phantasialand**.

Sichern Sie sich jetzt Ihr Ticket!

**https://isd.eco.de**

heise Events
Conferences, Seminars, Workshops

eco
VERBAND DER INTERNETWIRTSCHAFT

# Datenschutz schon umgesetzt?

**Liebe Leserinnen und Leser,**

es ist soweit, mit Erscheinen dieser Beilage wird an diesem Wochenende die europäische Datenschutz-Grundverordnung (EU-DSGVO) am 25.05.2018 europaweit verbindlich. In der Übergangsfrist von zwei Jahren, seit dem formellen Inkrafttreten am 25.05.2016, hatten Unternehmen und Organisationen Zeit, diese umzusetzen. Die DSGVO vereinheitlicht das Datenschutzrecht innerhalb der EU und regelt den Umgang mit bzw. die Verarbeitung von personenbezogenen Daten.

Bei der Umsetzung herrschte (und herrscht vermutlich immer noch) bei vielen Unklarheit darüber, wie bestimmte Konstellationen, z. B. im Auftraggeber-Auftragnehmer-Verhältnis, zu behandeln sind. Die EU-DSGVO zieht mitunter größere Aktivitäten nach sich. So wurde bekannt, dass Facebook die Daten von 1,5 Mrd. Nutzern in Rechenzentren aus der EU in die USA verschiebt, damit die Daten dieser Nicht-EU-Bürger nicht unter die Regelungen der EU-DSGVO fallen. Ebenso migriert LinkedIn die Daten von Nicht-Europäern in die USA. Solche Beispiele zeigen die Tragweite der Einführung dieser nicht zu unterschätzenden rechtlichen Umwälzung. Die EU-DSGVO scheint (nicht nur außerhalb der Europäischen Union) auch zu Vermeidungsstrategien zu führen.

Die vernetzte Welt benötigt normative Vorgaben. Auch Deutschland braucht einen starken Datenschutz und bestmöglich geschützte IT-Systeme. Wirtschaft und Verwaltung sowie private Anwender sind mehr denn je auf sichere und vertrauenswürdige Informationsinfrastrukturen angewiesen und dies auch über Landesgrenzen hinweg.

Als Bundesverband IT-Sicherheit e.V. sind wir bestrebt, Sie mit der TeleTrusT-Initiative „IT Security made in Germany“ zu unterstützen. Die beteiligten deutschen IT-Sicherheitsunternehmen stehen gemeinsam für mehr Vertrauenswürdigkeit und Informationssicherheit ein. Dafür sind wir als Verband auch in europäischen Institutionen wie ETSI und ECSO aktiv, um hier IT-Sicherheit und Datenschutz gemeinsam mit den europäischen Partnern voranzubringen. Neben der EU-DSGVO wird 2018 in der neuen Legislaturperiode in Deutschland auch die mögliche Neuausrichtung der Digitalpolitik ein spannendes Themenfeld sein. Erstmals wurde hierfür eine Staatsministerin für Digitalisierung in das Kanzleramt berufen. Das ist ein Schritt in die richtige Richtung. Ebenso wie IT-Sicherheit ist die Digitalisierung wirtschaftlich existenziell und sollte auf höchster politischer Entscheiderebene angesiedelt sein.

Die vorliegende Sonderpublikation informiert Sie über Lösungen und Konzepte, die deutsche Unternehmen im Bereich der IT-Sicherheit entwickelt haben. Diese weisen einen starken Bezug zur EU-DSGVO auf. Gemeinsam mit den TeleTrusT-Mitgliedern wünsche ich Ihnen eine informative Lektüre und hoffe, dass Sie zahlreiche Anregungen erhalten, um ggf. Lücken bei Ihrer Umsetzung der EU-DSGVO aufzuspüren.

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

## Inhalt

# Passwörter haben ausgedient

## Der Schutz digitaler Identitäten erfordert bessere Authentifizierungsmethoden

Immer noch werden unsere digitalen Identitäten völlig unzureichend durch den Unsicherheitsfaktor Passwort abgesichert. Dagegen sorgen etablierte Verfahren wie die Multi-Faktor-Authentifizierung (MFA) für ein sicheres Identity- und Access-Management (IAM) in Zeiten stetiger Digitalisierung.

Ein Leben ohne digitale Identität ist heute nicht mehr denkbar. Vom Online-Banking über den E-Mail-Account und Social-Media-Profile bis hin zum digitalen Personalausweis. Doch keine Woche vergeht ohne Hiobsbotschaft über einen Hack, die Kompromittierung von Daten oder neue Sicherheitslücken. Selbst IT-Netze der höchsten Sicherheitsstufe sind nicht davor gefeit. Und oft vergehen mehrere Monate, bis ein Hack überhaupt bemerkt wird. In der Zwischenzeit können Unbefugte nach Lust und Laune das geknackte IT-System durchstöbern und mit weiteren erbeuteten Zugangsdaten gegebenenfalls auch weitere Fremd-Systeme und Daten übernehmen. So wird das eigene Passwort dann ebenfalls bei Google, Microsoft, Amazon und Co. ausprobiert. Ein wesentlicher Grund, warum Hacker bis heute leichtes Spiel haben, ist das Passwort. Es gehört längst abgelöst durch die Multi-Faktor-Authentifizierung, die eine deutlich bessere Absicherung von Logins und Transaktionen gewährleistet.

### Offene Einladung an Hacker

Möglichst lang, mit Groß- und Kleinbuchstaben und Sonderzeichen. Dazu regelmäßige Änderungen und für jeden Dienst etwas Individuelles – Tipps und Tricks für ein sicheres Passwort gibt es viele, doch scheitern sie letztlich an der Realität. Denn trotz aller Ratschläge sind Passwörter noch immer in 81 % aller Fälle die Ursache für einen Hack, so der „Verizon Data Breach Investigations Report 2017“. Kein Wunder, schließlich sind Passwörter einfach nicht dafür geeignet, umfangreiche Sicherheit zu schaffen: Wirklich komplex sind sie kaum bis gar nicht zu merken, sie sind generell leicht zu knacken und als einziger Faktor schlicht unzureichend.

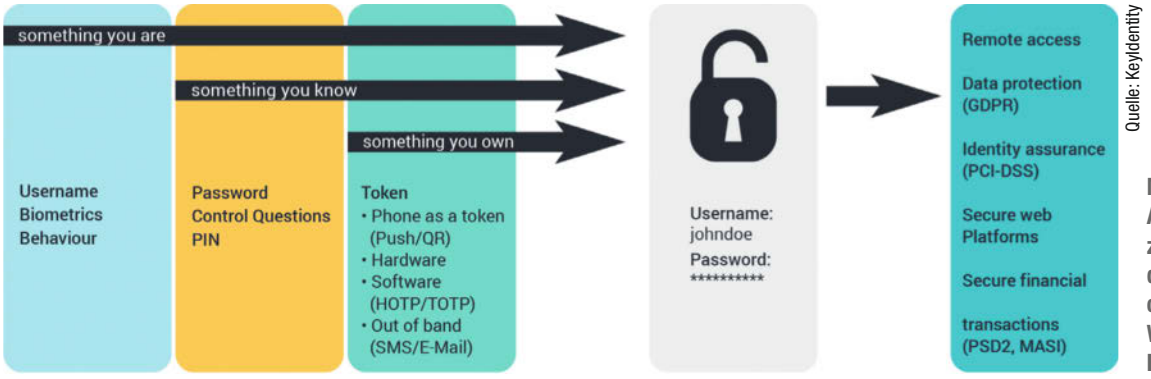
Allen Warnungen zum Trotz wählen Nutzer noch immer einfachste Passwörter. So landeten laut Hasso-Plattner-Institut 2017 auf den ersten drei Plätzen der beliebtesten Passwörter der Deutschen die Zahlenreihen 123456, 123456789 sowie 1234. Das liegt allerdings nicht nur an der reinen Bequemlichkeit der User. Denn allein die schiere Anzahl an Accounts macht es unmöglich, sich dutzende komplexe Passwörter zu merken – geschweige denn sie auch noch regelmäßig zu ändern. Daher greifen die meisten Nutzer auf die immer gleichen Schemata bei ihrer Passworterstellung zurück.

Selbst wer komplizierte Kombinationen verwendet, kann leicht zum Opfer von Hackern werden. Denn auch vermeintlich komplexe Passwörter können entweder abgeleitet (Targeted Password Guessing) oder erfragt (Social Engineering) werden. Nicht selten ist das eigene Passwort bereits in den Weiten des Darknet bekannt, wo Login-Daten rege gehandelt werden. Dient ein Passwort dann für mehrere Logins, sind gleich verschiedene Accounts kompromittiert. Über die Website „Have I been pwned?“ können Interessierte herausfinden, ob Accounts, die über die eigene E-Mail-Adresse verbunden sind, bereits gehackt wurden.

### Unabhängig und zweifach sicher

Überraschenderweise wurde aber diese Methode der Authentifizierung nicht schon längst ad acta gelegt, obwohl seit etlichen Jahren die Multi-Faktor-Authentifizierung zur Verfügung steht. Bereits ihre Grundidee ist wesentlich sicherer: Statt nur einen einzigen Faktor abzufragen, werden (mindestens) zwei voneinander unabhängige Berechtigungsnachweise verlangt (siehe Abbildung unten).

Diese Faktoren basieren auf drei unterschiedlichen Eigenschaften: *Wissen* (Passwörter oder PINs, die nur der autorisierte Nutzer kennt); *Besitz* (Token, Smartphone-Apps oder Smartcards, die nur der berechtigte Nutzer besitzen kann oder darf); *Inhärenz* (biometrische Eigenschaften des Anwenders). Ein Hacker, der das Passwort eines Nutzers kennt, scheitert letztlich an der Verifizierung des zweiten Faktors. Das ermöglicht neben der Authentifizierung bei Logins noch weitere Anwendungsszenarien.




Quelle: KeyIdentity

**Multi-Faktor-Authentifizierung nutzt drei Dimensionen: Inhärenz, Wissen und Besitz.**

## Vier Augen sehen mehr

Dank MFA-Technologie lassen sich digitale Identitäten sicher verifizieren. Daneben schützt sie auch Transaktionen, in dem sie sicherstellt, dass diese rechtmäßig sind. Das ist gerade im Online-Banking insbesondere vor dem Hintergrund von PSD2 und angesichts der Zunahme bargeldloser Bezahlungen immens wichtig. Bei soliden Lösungen werden bei einer Überweisung sämtliche Daten mittels Public und Private Keys sicher verschlüsselt und die Parameter der Überweisung (Bankverbindung, Verwendungszweck, Betrag) kryptografisch signiert. Das erschwert sogenannte „Man-in-the-middle-Angriffe“ erheblich. Auch der Anwender kann nicht mehr im Nachgang sagen, dass er gar nicht wusste, dass das Geld an einen dubiosen Kontakt aus dem Internet geht. Schließlich muss er die Parameter noch einmal bestätigen. Damit sind Haftungsfragen eindeutig und eine Abstreitbarkeit nicht mehr möglich.

Ein weiterer Vorteil der MFA-Technologie ist das sogenannte Vier-Augen-Prinzip. Damit lassen sich besonders kritische Vorgänge wie hohe Geldtransfers oder Freigabeprozesse doppelt absichern. So kann nur durch die zusätzliche Bestätigung einer weiteren autorisierten Person im Bereich kritischer Infrastrukturen (KRITIS) etwa die Flutung eines Staudamms eingeleitet oder im Finanzwesen die Freigabe eines hohen Kredits erteilt werden. Auch der Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) empfiehlt den Einsatz starker Authentifizierung für sicherheitskritische Anwendungsbereiche. Zudem sorgt eine Vielzahl verschiedener Authentifizierungs-Token dafür, dass für alle denkbaren Login- oder Transaktionsszenarien die richtige Auswahl bereitsteht.

## OTP-Token für jede Anforderung

Die weitaus höhere Sicherheit der Multi-Faktor-Authentifizierung gegenüber dem Passwort rührt nicht nur daher, dass eine zweite Abfrage erfolgt. Die Token selbst, die als zweiter Faktor fungieren, schaffen durch die Verwendung eines Einmalpassworts (One-Time-Password = OTP) ein besonders hohes Sicherheitsniveau. Im Grunde basieren OTPs auf zwei Varianten: Entweder wird auf eine zuvor festgelegte Zahl an PINs oder Passwörtern zurückgegriffen, oder bei jedem Authentifizierungsvorgang wird ein komplett neues Passwort generiert.

Die zweite Variante ist dank des immer neuen Passworts besonders sicher: Es entsteht mittels Rückgriff auf einen Algorithmus, der während der Synchronisation zwischen Token und Server einen Beweis in Form eines Ergebnisses liefert. Der stets neue Wert kann in dreierlei Weise zustande kommen: abhängig von einem bestimmten Zeitpunkt (zeitgesteuert), von einem Ereignis wie dem Drücken eines Zählers (Event-basiert) oder in Form einer Aufgabe, die der Server dem Token stellt (challenge-response-gesteuert). Außerdem steht eine große Auswahl ganz unterschiedlicher Token zur Verfügung. Seien es klassische Hardware-Token in Form einer Chipkarte, moderne Software-Token wie QR-, Voice- sowie Push-Token oder die immer beliebteren Biometrie-Token.

## Goodbye Passwort, hallo MFA

Lange genug haben Passwörter zur Authentifizierung von digitalen Identitäten gedient. Aber ihr Unsicherheitsfaktor ist angesichts der endlosen Fälle von Missbrauch nicht mehr zu leugnen. Da zudem sichere Logins und Transaktionen im Zuge der Digitalisierung nicht wichtig genug eingeschätzt werden können, ist es an der Zeit, endlich eine überzeugende Technik umfangreich zu etablieren. Nicht nur zur Absicherung der eigenen Zugänge, sondern auch zur Absicherung von Web-Portalen bzw. Cloud-Anwendungen.

Die Multi-Faktor-Authentifizierung bietet nicht nur deutlich mehr Sicherheit. Sie ist zudem dank der Vielzahl an Token-Typen hochflexibel, benutzerfreundlich und außerdem problemlos auch in Legacy-Systeme integrierbar. Demzufolge ist es kein Wunder, dass immer mehr Anbieter Formen der MFA bereitstellen: von Social-Media-Portalen wie Facebook oder Twitter über E-Mail-Betreiber wie Gmail oder Yahoo bis hin zu Spieleherstellern wie Nintendo oder Blizzard.

*Dr. Amir Alsbih*
*CEO, KeyIdentity*

# Was bedeutet „Stand der Technik“?

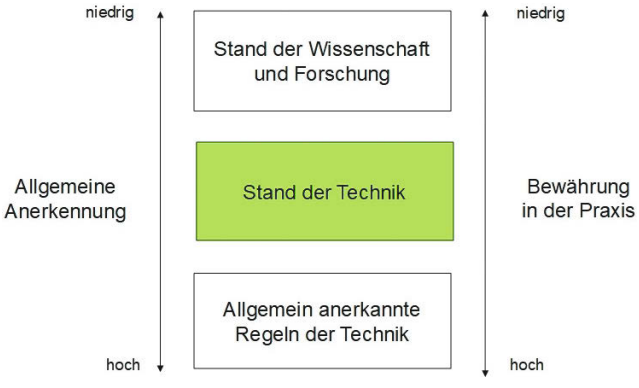
## Wie sich der gesetzlich geforderte Technologiestand ermitteln lässt

In der neuen Datenschutz-Grundverordnung spielt der Technologiestand der im Unternehmen eingesetzten Maßnahmen eine wichtige Rolle. Wie aber lässt sich dieser sogenannte „Stand der Technik“ methodisch bestimmen, um der geforderten Dokumentationspflicht nachzukommen?

Man könnte annehmen, alle Unternehmen in ganz Europa befinden sich bereits auf der Zielgeraden zum 25. Mai 2018. Als Vorbereitung wurden endlich die Verarbeitungsprozesse vollständig beschrieben, Risiken im Hinblick auf die personenbezogenen Daten bewertet und eingesetzte Maßnahmen dokumentiert. Auch die Dienstleister hat man nachdrücklich auf die Einhaltung der Datenschutzrichtlinie hingewiesen und entsprechend verpflichtet. Und die Kunden sind ebenfalls über die bevorstehende oder schon erfolgte Anpassung der Datenschutzrichtlinie des Unternehmens benachrichtigt worden. Die wichtigsten Schritte für die Einhaltung der europäischen Datenschutz-Grundverordnung (DSGVO) sind offenbar getan.

### Regelmäßiges Benchmarking

Doch das ist erst der Anfang. Der Artikel 32 DSGVO (Abs. 1) schreibt vor: „Unter Berücksichtigung des Stands der Technik […] treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Sicherheitsmaßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.“ Was der Gesetzgeber konkret unter „Stand der Technik“ der eingesetzten Maßnahmen versteht und wie geeignete Maßnahmen identifiziert werden können, ist in der DSGVO nicht definiert. Bei diesem Schritt werden die Unternehmen allein gelassen. Wie können also die Verantwortlichen nachweisen, dass sie die eingesetzten Maßnahmen an den gesetzlich geforderten Gegebenheiten ausgerichtet haben und fortlaufend einhalten?




Quelle: Lawicki, Sachverständigen-Sozietät Dr. Schwerhoff

**Abb. 1: Drei-Stufen-Theorie in Anlehnung an die Kalkar-Entscheidung**

Bei einer Recherche nach dem Begriff „Stand der Technik“ stößt man schnell auf die „Drei-Stufen-Theorie“ der Kalkar-Entscheidung des Bundesverfassungsgerichts. Daran angelehnt ist „Stand der Technik“ zwischen dem „Stand der Wissenschaft und Forschung“ und den „allgemein anerkannten Regeln der Technik“ anzusiedeln (Abbildung 1).

Technische Maßnahmen im Stadium „Stand der Wissenschaft und Forschung“ sind sehr dynamisch in ihrer Entwicklung und gehen mit dem Erreichen der Marktreife (oder zumindest mit der Markteinführung) in das Stadium „Stand der Technik“ über. Dort nimmt die Dynamik z. B. durch die Standardisierung der Prozesse ab. Auch technische Maßnahmen im Stadium „Allgemein anerkannte Regeln der Technik“ sind am Markt verfügbar. Ihr Innovationsgrad nimmt ab, sie haben sich jedoch in der Praxis bewährt und werden in den entsprechenden Standards beschrieben. Zusammenfassend und einfach ausgedrückt: Der „Stand der Technik“ ist innovativer als die allgemein anerkannten Regeln der Technik und veraltet gegenüber dem Stand der Wissenschaft und Forschung.

Mit dem Artikel 32 DSGVO hat der Gesetzgeber die Vorgabe geschaffen, nach der sich die Unternehmen an den am Markt verfügbaren innovativsten Maßnahmen orientieren sollen. Für die Bewertung von technischen und organisatorischen Maßnahmen im Bereich der IT-Sicherheit sind in der DSGVO keine messbaren Kriterien definiert. Daher können also die eingesetzten Maßnahmen (oder am Markt verfügbaren Produkte) nicht anhand einer vom Gesetzgeber vorgegebenen Metrik bewertet werden.

Um den geforderten Nachweis bei der Orientierung eigener Maßnahmen nach der bestmöglichen und fortschrittlichsten Verfahrensweise zu erbringen, reicht es nicht aus, sie zu dokumentieren und durch die regelmäßige Installation von Patches zu aktualisieren. Ein solcher Nachweis kann nur gelingen, indem die eingesetzten Werkzeuge mit den am Markt verfügbaren Alternativen verglichen werden. Hierfür sollte eine transparente Benchmarking-Methode (Abbildung 2) eingesetzt werden, mit der die Maßnahme in regelmäßigen Abständen überprüft wird.

### Erweiterte Leistungsmerkmale

Bei einem Vergleich von technischen Maßnahmen, sollten neben den üblicherweise gemessenen Leistungsmerkmalen auch die Dimensionen „Eignung“, „Fortschrittlichkeit“, „Anerkennung“ und „Praxisbewährung“ einbezogen werden.

*Eignung*: Klar ist, dass die eingesetzte Maßnahme für ihren Einsatzzweck geeignet und an die sich verändernde Bedrohungslage und neue Angriffsszenarien anpassbar sein soll. Die technische Eignungsprüfung (z. B. Penetrationstest) kann nur bei der tatsächlich sich im Zugriff befindenden Maßnahme erfolgen. Lösungen, die am Markt gehandelt werden, stehen für eine solche Untersuchung nicht zur Verfügung. Diese Dimension sollte also weiter gefasst sein. Ein Beispiel hierfür sind die Ergebnisse von Maßnahmen-Untersuchungen durch unabhängige Gremien.

*Fortschrittlichkeit*: Aufgrund des technologischen Fortschritts sollte alle zwei bis drei Jahre mit einer signifikanten Verbesserung der am Markt verfügbaren technischen Maßnahmen gerechnet werden. Die Untersuchung der Fortschrittlichkeit sollte darüber hinaus auch den Innovationsgrad und die mögliche Weiterentwicklung der eigenen Maßnahme berücksichtigen.

| | | | Benchmark | | |
|---|---|---|---|---|---|
| Bereich | Schutzbedarf | eingesetzte Maßnahme | Alternative(n) | Wirtschaft. Betrachtung | Auswahl und Begründung |
| | | | | | |

Quelle: Lawicki, Sachverständigen-Sozietät Dr. Schwerhoff

**Abb. 3: Ergänzung der Dokumentation eingesetzter und ausgewählter Maßnahmen**

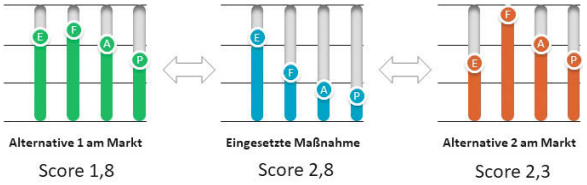
dem noch weitere Fragen mit Fokus auf den vorgesehenen Einsatzbereich und die erreichte Robustheit der Maßnahme im Vergleich Berücksichtigung finden.

Basierend auf dem Benchmark-Vergleich lässt sich die Dokumentation eingesetzter Maßnahmen ergänzen. Erst danach wird die wirtschaftliche Betrachtung mit anschließender Auswahl und Begründung der Auswahl dokumentiert (Abbildung 3).



*Anerkennung*: Bei der Bewertung der Anerkennung sollte berücksichtigt werden, inwiefern eine technische Maßnahme sich z. B. an international anerkannten Standards orientiert. Oft sprechen anerkannte Gremien oder Verbände Empfehlungen für den Einsatz bestimmter Maßnahmen (meist ohne Nennung von Produkten) aus.

*Praxisbewährung*: Die Praxisbewährung könnte angenommen werden, wenn eine Maßnahme am Markt verfügbar ist. Jedoch sollten zu-




Quelle: Lawicki, Sachverständigen-Sozietät Dr. Schwerhoff

**Abb. 2: Beispiel eines Benchmark-Vergleichs**

## Externe Unterstützung

Der Datenschutz genießt einen hohen Stellenwert. Durch die Vorgaben aus der DSGVO müssen die Verantwortlichen unternehmensweite Strategien am geforderten Sicherheitsniveau nachhaltig ausrichten. Das bedeutet, die IT-Sicherheit als wichtige Säule in der Sicherung des Datenschutzes zu sehen, sie fortlaufend zu überprüfen und gegebenenfalls nachzubessern.

Die Berücksichtigung und Einhaltung des Stands der Technik setzt wie beschrieben einen Vergleich von Maßnahmen voraus. Ein solcher ist jedoch oftmals nur schwer eigenständig durchzuführen. Daher ist es allenfalls sinnvoll, eine zielgerichtete und produktunabhängige Bewertung durch einen neutralen Dritten (z. B. Sachverständigen) vorzunehmen.

*Tomasz Lawicki*
*Sachverständigen-Sozietät Dr. Schwerhoff,*
*Leiter des Arbeitskreises "Stand der Technik" beim TeleTrusT*

# Ausbau der Kampfzone

## Bei gängigen IT-Lösungen zur Verschlüsselung sollte man auf die Details achten

Hundertprozentigen Schutz vor einem Hack gibt es nicht. Entsprechend gilt es, nicht nur auf Prävention zu setzen, sondern auch die Schadensbegrenzung im Auge zu behalten, wenn dann doch ein unbefugter Zugriff erfolgt. Was sollten also Unternehmen bei der Auswahl einer passenden IT-Lösung beachten?

Cyberangriffe zielen längst nicht mehr nur auf Großkonzerne ab. Das mussten zuletzt nicht nur Branchenriesen wie FedEx oder Equifax feststellen – auch mittelständische Unternehmen werden immer häufiger zum Angriffsziel. Laut einer Bitkom-Studie war in den Jahren 2016 und 2017 bereits jedes zweite Unternehmen betroffen. Und überdies bleiben solche Vorfälle oftmals erschreckend lange unbemerkt. Nicht zuletzt auch im Hinblick auf die neue Gesetzeslage ist diese Entwicklung besorgniserregend, denn mit Inkrafttreten der neuen EU-Datenschutz-Grundverordnung (DSGVO) drohen deutlich höhere Bußgelder als bisher.

### Assume the breach

In den letzten Jahren hat sich ein Paradigmenwechsel abgezeichnet, den Gartner 2014 mit seiner „Adaptive Security Architecture“ einläutete: weg von der Idee, man könne sich vor allen Angriffen präventiv schützen, hin zur Grundannahme, dass man zu jeder Zeit bereits kompromittiert sei. Unternehmen sollten sich deshalb nicht nur mit der Prävention von Cyberattacken beschäftigen, sondern auch damit, wie sie den Schaden minimieren können, falls Angriffe dennoch gelingen sollten.

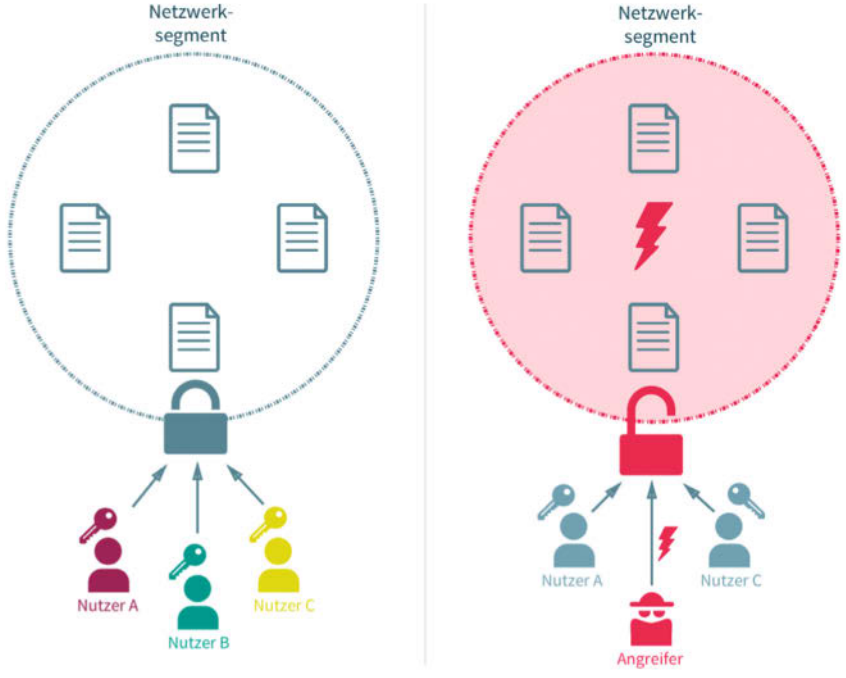
Das Konzept der asymmetrischen Verschlüsselung erlaubt es, direkt auf der Ebene einzelner Datensätze anzusetzen und so die Preisgabe von Daten bei Angriffen zu minimieren. Auch zentrale Vorgaben der DSGVO lassen sich so effektiv umsetzen. Doch bei der Auswahl der passenden Lösung müssen Unternehmen darauf achten, die Datenhoheit zu behalten und am Ende nicht selbst den Zugriff zu verlieren.

### Vom Netzwerk- zum Kryptoperimeter

Das altgediente Konzept des Netzwerkperimeters, das Schutzmechanismen an den Außengrenzen des Netzwerks vorsieht, wird dieser Zielsetzung nicht mehr gerecht. Zunehmende Mobilität und die Integration privater mobiler Endgeräte (Stichwort: BYOD) haben die Grenzen des Netzwerks längst aufgeweicht. Zudem werden die meisten Angriffe von innen heraus lanciert: Über raffinierte Social-Engineering-Methoden werden Mitarbeiteridentitäten gekapert, die dem Angreifer Zugriff zum Netzwerk verschaffen. Das eigentliche Ziel – und damit das schützenswerte Gut – sind aber die dort gespeicherten Daten (Abbildung 1). Entsprechend sollten auch die Schutzmaßnahmen genau dort greifen.

Ein vielversprechender Ansatz hierfür findet sich in der asymmetrischen Verschlüsselung. Dabei kommt je Nutzer ein Schlüsselpaar zum Einsatz, das aus einem öffentlichen und einem privaten Schlüssel besteht. Der öffentliche Schlüssel wird an andere weitergegeben; damit kann jeder Daten für den betreffenden Nutzer verschlüsseln. Nur dieser ist dann in der Lage, die Daten mit seinem geheimen privaten Schlüssel wieder zu entschlüsseln.

Die Vorteile eines solchen Kryptoperimeters sind vielfältig: Dringt ein Angreifer ins Netzwerk ein, so findet er nur verschlüsselte und damit für ihn wertlose Daten vor. Um diese lesbar zu machen, muss der Eindringling an den geheimen privaten Schlüssel eines berechtigten Nutzers gelangen. Da diese niemals im Klartext übertragen und daher unterwegs nicht abgefangen werden können, braucht er Zugriff auf das Endgerät des Nutzers, was in der Regel eine schwer zu überwindende Hürde ist – oder zumindest sein sollte. Doch selbst wenn ihm dies gelingt, sind nicht gleich alle Ressourcen im entsprechenden Netzwerk kompromittiert, son-




Quelle: Brabbler AG

**Abb. 1: Klassischer Netzwerkperimeter: Nutzer erhalten Zugriff auf ein gesamtes Netzwerksegment. Bei einem erfolgreichen Angriff ist dadurch auch potenziell das gesamte Netzwerksegment kompromittiert.**

Quelle: Brabbler AG

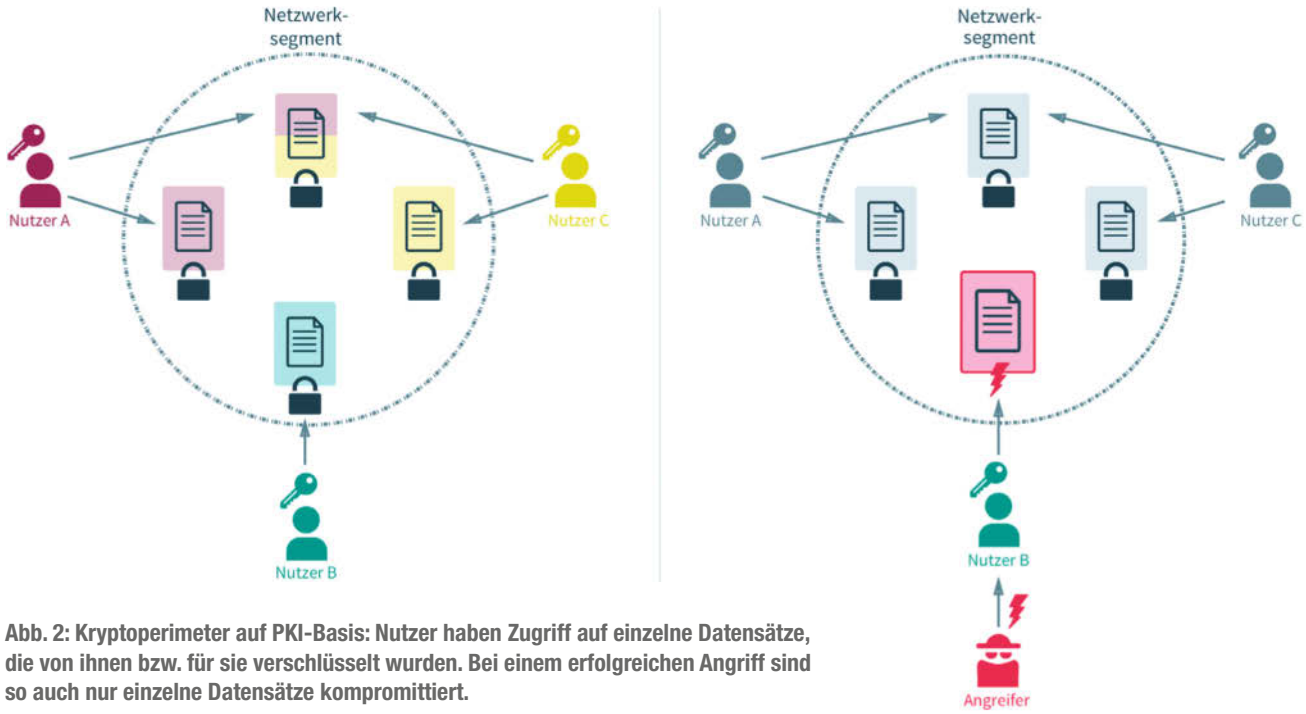



**Abb. 2: Kryptoperimeter auf PKI-Basis: Nutzer haben Zugriff auf einzelne Datensätze, die von ihnen bzw. für sie verschlüsselt wurden. Bei einem erfolgreichen Angriff sind so auch nur einzelne Datensätze kompromittiert.**

dern nur die, die von dem beziehungsweise für den betreffenden Nutzer verschlüsselt wurden (Abbildung 2).

Auch mit Blick auf die DSGVO bietet ein Kryptoperimeter klare Vorteile: Artikel 32 der neuen Datenschutz-Grundverordnung fordert „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau“ bei der Verarbeitung von Daten zu gewährleisten. Verschlüsselung ist dabei eine der wenigen Maßnahmen, die im Gesetzestext ganz konkret genannt werden. Das Schutzziel Vertraulichkeit ist damit nach verbreiteter Expertenmeinung erfüllt. Und sollte es tatsächlich zu einer Datenpanne kommen, gelten die abhanden gekommenen Daten bei angemessener Verschlüsselung nicht als verloren. Das bedeutet, dass in diesem Fall auch die Pflicht zur Information der betroffenen Personen und der Öffentlichkeit entfällt.

## Schwachpunkte gängiger Lösungen

An verfügbaren Lösungen mangelt es nicht, doch oftmals ist bereits die aufwendige Administration ein nicht zu unterschätzendes Ausschlusskriterium. Daher geht die Empfehlung zu Lösungen mit bereits

Quelle: Brabbler AG

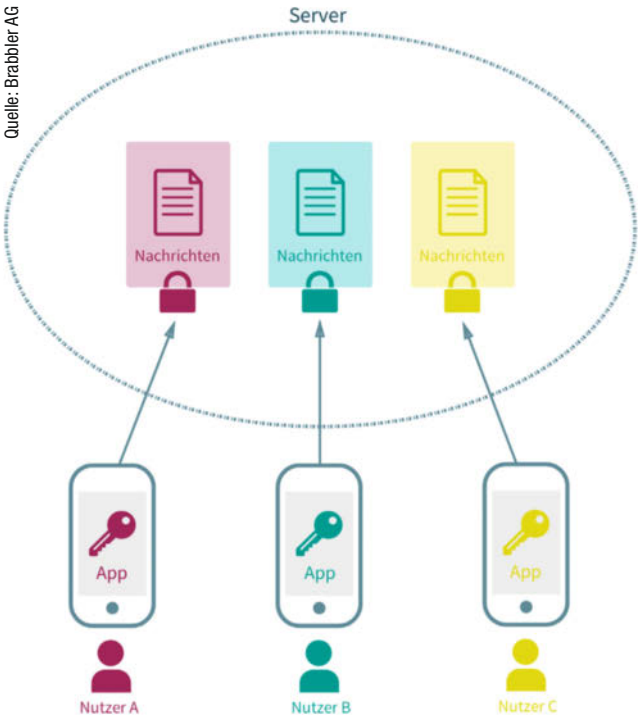



**Abb. 3: Bei vielen Lösungen werden die Schlüssel der Nutzer ausschließlich auf deren Geräten vorgehalten. Ein zentraler Zugriff auf die Daten durch das Unternehmen ist so nicht möglich.**

integrierter Verschlüsselung. Aber nicht jedes Angebot hält tatsächlich auch, was es verspricht.

So sollte sich etwa kein Unternehmen mit einer reinen Ende-zu-Ende-Verschlüsselung zufriedengeben. Dann kann zwar niemand brauchbare Daten bei der Übertragung abfangen, doch gerade bei der unweigerlich zunehmenden Mobilität stellen auch die Endpunkte einen Risikofaktor dar. Smartphones und Laptops gehen gerne mal verloren oder sie werden gestohlen. Damit auch dann keine Klartextinhalte in fremde Hände geraten, dürfen die ruhenden Daten auf diesen Geräten nur verschlüsselt abgespeichert werden.

Gleichzeitig sollte das Unternehmen selbst die uneingeschränkte Hoheit über die Daten behalten und bei Bedarf darauf zugreifen können. Aber auch hier liegt ein weiterer Schwachpunkt vieler Lösungen am Markt: Meistens wird der private Schlüssel eines Nutzers ausschließlich auf dessen Gerät vorgehalten. Das bedeutet, dass nur der Nutzer selbst die Daten entschlüsseln kann, nicht jedoch eine zentrale Kontrollinstanz im Unternehmen, etwa der Geschäftsführer oder der IT-Administrator (Abbildung 3).

## Datenhoheit zu treuen Händen

Will ein Unternehmen die Datenhoheit behalten, so braucht es die Hoheit über die Schlüssel. Dies lässt sich durch sogenannte Key-Escrow-Systeme realisieren. Der Begriff wird häufig im Zusammenhang mit staatlich erwünschten Hintertüren benutzt. In diesem Fall jedoch beschreibt er ein Grundkonzept, bei dem Backups der privaten Nutzerschlüssel zentral und ausschließlich für den unternehmensinternen Zugriff vorgehalten werden. Diese Backups sind wiederum mit einem Masterschlüssel verschlüsselt (Abbildung 4).

**Abb. 4: Key-Escrow-System: Backups der Nutzerschlüssel werden zentral abgelegt. Sie sind mit einem Masterschlüssel verschlüsselt, den nur eine Kontrollinstanz im Unternehmen bei Bedarf nutzen kann.**

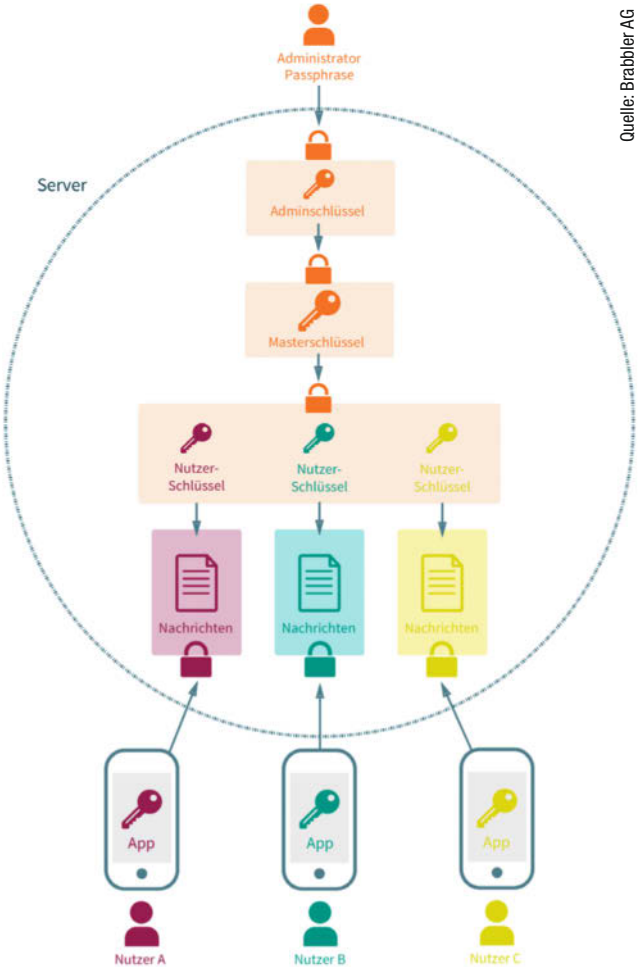
Freilich gilt es, die Rechte des Administrators so einzuschränken, dass Missbrauch ausgeschlossen ist. Ein Administrator soll zwar Daten entschlüsseln können, darf aber nie direkten Zugriff auf die Nutzerschlüssel im Klartext erhalten. Damit wird Identitätsdiebstahl verhindert. Noch mehr Kontrolle bietet darüber hinaus ein Vier-Augen-Prinzip bei datenschutzrelevanten Operationen.

## Mehrwert für die Sicherheitsstrategie

Man sollte also bei der Auswahl passender Lösungen genau hinschauen. Der Aufwand lohnt sich, denn durchdachte Produkte mit integrierter Verschlüsselung liefern vielfältigen Mehrwert für die Sicherheitsstrategie eines Unternehmens: Sie nehmen Druck von der Sicherheit des Netzwerkes und unterstützen – die starke Verschlüsselung ruhender Daten auf den Endgräten vorausgesetzt – auch die klassische Endpoint Security. In vielen Bereichen ersetzen sie die aufwendige Implementierung eigener Verschlüsselungskonzepte und leisten damit nicht zuletzt auch einen wichtigen Beitrag zur effizienten Umsetzung der DSGVO-Anforderungen.

*Daniel Eyring*
*Teamlead Software Engineering, Brabbler AG*

Quelle: Brabbler AG



# Sicherheitsexperten für KMU

## Neue Ausbildungsstandards sollen die mittelständische IT-Sicherheit stärken

Das kleine und mittelständische produzierende Gewerbe bildet das Rückgrat der deutschen Wirtschaft. Bei der Betrachtung von IT-Security werden diese Unternehmen jedoch oftmals außer Acht gelassen. Eine Forschungsinitiative will hier Abhilfe schaffen.

Kleine und mittlere Unternehmen steuerten im Jahr 2014 laut IfM Bonn rund 55 % zur gesamten Nettowertschöpfung deutscher Unternehmen bei. Gerade die KMU im Bereich des herstellenden Gewerbes sind aber mit besonderen Herausforderungen konfrontiert, wenn es um die Umsetzung effektiver IT-Sicherheitsmaßnahmen geht. Dies gilt umso mehr, als im Zuge von Industrie 4.0 eine immer stärkere Vernetzung von Steueranlagen stattfindet und die vormals bestehende Trennung des Produktionsnetzes vom Büronetz immer weiter aufgehoben wird.

Daneben wird IT-Security zunehmend interdisziplinärer: So sind nicht nur technische, sondern ebenso rechtliche wie betriebswirtschaftliche, teils sogar psychologische Kenntnisse gefordert, wenn es um die Abwehr von Gefahren beispielsweise durch Social Engineering, geht. Insbesondere im Hinblick auf KMU führt diese zunehmende Spezialisierung der Mitarbeiter, oftmals verbunden mit einem Mangel an wirtschaftlichen Ressourcen und unzureichenden personellen Kapazitäten, zu einer Realisierungslücke im IT-Sicherheitsmanagement: Entweder sind die geltenden Anforderungen gar nicht bekannt oder es fehlen die Mittel zu ihrer Umsetzung. Dies hat zur Folge, dass Maßnahmen der IT-Security entweder überhaupt nicht, nicht flächendeckend und nur als Insellösungen oder aber nicht in der notwendigen Implementierungstiefe realisiert werden.

### Die CertComp-Initiative

An dieser Stelle soll der durch das Forschungsvorhaben „Kompetenz durch Zertifizierung“ (CertComp) zu entwickelnde aktive Maßnahmenkatalog einfließen. Erforscht werden soll eine interdisziplinäre IT-Sicherheitslösung, die im Gegensatz zu vorherrschenden rein technischen, computerbasierten Ansätzen den Menschen als den originär für die IT-Sicherheit Verantwortlichen in den Mittelpunkt der Betrachtung stellt. Die Grundlage hierfür wird zunächst eine umfassende Studie bilden, die den Kenntnis- und Ausbildungsstand von IT-Sicherheitsverantwortlichen in Deutschland sowie potenzielle Diskrepanzen zwischen Ist- und Sollzustand ermittelt und bewertet.

Das auf dieser Basis im Folgenden durch CertComp zu erstellende Lehr- und Lernkonzept entwirft ein neues Berufsmodell des IT-Sicherheitsverantwortlichen: Zielgerichtet als Entscheidungsträger durch eine multimodale Wissensvermittlung berufsqualifizierend ausgebildet und zertifiziert werden selbst solche Mitarbeiter im Unternehmen, die bisher über keine berufliche Vorbildung im Bereich des IT-Sicherheitsmanagements verfügen, in die Lage versetzt, informationstechnische Bedrohungslagen zu erkennen und erfolgreich abzuwehren sowie Prävention zu betreiben. Insbesondere soll durch CertComp dem Umstand Rechnung getragen werden, dass die IT-Anlagen im produzierenden Gewerbe insgesamt ähnliche technische Strukturen aufweisen (BSI, ICS-Security-Kompendium, 2013). So ist es gleichgültig, ob ein Lebensmittelhersteller, ein Automobilzulieferer oder ein Chemieproduzent tätig wird, denn in nahezu allen Fällen wird der Produktionsprozess durch eine Industriesteuerungsanlage – nicht selten vom gleichen Typ – geführt.

### Kompetente Partner

CertComp wird in seiner Forschung ausschließlich auf kleine und mittelständische Unternehmen fokussieren, die explizit nicht dem Sektor kritischer Infrastrukturen im Sinne des IT-Sicherheitsgesetzes (IT-SiG) zugeordnet sind. Der Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE e. V.) als Transferpartner von CertComp verfügt über einen umfassenden Zugang zu KMU im produzierenden Gewerbe und ist bereits seit Jahren in der IT-sicherheitstechnischen Normung und Standardisierung aktiv. Die VdS Schadenverhütung GmbH ist als weltweit etablierte Institution für Unternehmens- und IT-Sicherheit Anwendungspartner von CertComp.

Kompetenzpartner des Forschungsvorhabens ist die Universität Bremen mit dem Technologiezentrum Informatik und Informationstechnik (TZI), dem Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) sowie der AG DiMeB (Digitale Medien in der Bildung), die sich bereits seit Jahren mit aktuellen Fragen der IT-Sicherheit, des Datenschutzes und der computerbezogenen Bildung befassen. Die einzelnen Institute werden in interdisziplinärer Zusammenarbeit die technischen, rechtlichen sowie vor allem auch die didaktischen Voraussetzungen einer praxisnahen und effektiven, berufsbegleitenden Ausbildung zum IT-Sicherheitsverantwortlichen erforschen. Hierbei sollen Konzepte des Blended-Learning, also der Kombination aus E-Learning und Präsenzlehre, zum Einsatz kommen. Dadurch wird vor allem auch der Anforderung Rechnung getragen, dass die häufig bestehende umfassende berufliche Einbindung der Zielgruppen gleichermaßen passgenaue wie flexibilisierte Schulungskonzepte erfordert.

### Zertifizierte Standards

CertComp kann in seiner Zwecksetzung damit einen wesentlichen Faktor nicht nur zum Schutz der wirtschaftlichen und geistigen Ressourcen des Mittelstandes, sondern ebenso einen Beitrag zur Förderung und zukunftsgerichteten Definition der IT-Standorte Deutschland und Europa leisten, indem es erstmals das Ziel verfolgt, die Ausbildung zum IT-Sicherheitsverantwortlichen an den Anforderungen der KMU-Praxis orientiert zu vereinheitlichen, zu standardisieren und zu zertifizieren.

*Dr. Dennis-Kenji Kipker*
*Universität Bremen (IGMR)*

# Wider den Dominoeffekt

## Der Trend zu Detect-and-Response-Systemen bei der Malware-Abwehr birgt Risiken

Im Internet gibt es nur Opfer und potenzielle Opfer. Das gilt für einzelne Anwender und Großunternehmen gleichermaßen. Die sich weiterdrehende Komplexitätsspirale erfordert permanent Aufmerksamkeit, aber oft fehlt die Priorisierung bei der Abwehr von Malware-Attacken.

Die immens gestiegene Nachfrage nach Sicherheitslösungen hat die IT-Sicherheit zu einer Boomwirtschaft gemacht. Auf der Suche nach wirksamen Methoden haben etliche Lösungen allerdings ungewollt zu neuen Herausforderungen geführt und dabei den eigentlichen Zweck verfehlt. Malware ist bei fast allen Datenschutzvorfällen in der einen oder anderen Form beteiligt, aber eine reine Post-Execution-Strategie zur Malware-Behandlung birgt hohe Risiken.

### Von Pre- zu Post-Execution

Die rasante Weiterentwicklung und schnelle Verbreitung von Malware treibt die Kosten in die Höhe und den Markt an. Sicherheitslösungen, Tools und Dienstleistungen zur Wiederherstellung und Schadensbegrenzung, zu Speicher- und Verhaltensanalysen – die Zahl der Layer wächst. Getreu der Ansicht, dass man einen Angriff ohnehin nicht gänzlich vermeiden kann, geht der Fokus auf präventive Methoden und Technologien verloren. Die Mehrzahl der Sicherheitsanbieter reagiert auf die wachsende Zahl von Angriffen mit einer Malware-Analyse ‚*nachdem* der Schadcode ausgeführt wurde. Dazu überwachen Softwaremodule und Sensoren kontinuierlich alle Endpunkte, um dann möglichst schnell auf einen Angriff zu reagieren. Ist das das Gebot der Stunde?

Schließlich gelangt die Malware erst in den Einflussbereich der Post-Execution, wenn die präventiv arbeitenden Lösungen sie nicht stoppen können. Kommt es zur Malware-Ausführung auf einem Endgerät, ist das immer mit hohen Risiken verbunden. Ziel vieler Security-Anbieter ist es, die Malware nun anhand des Verhaltens aufzudecken, Folgeschäden in Grenzen zu halten und ein Worst-Case-Szenario zu verhindern. Post-Execution-Monitoring analysiert und protokolliert das Anwendungs- und Systemverhalten. In den meisten Fällen werden dafür auch große Teile des Netzwerkverkehrs analysiert und fortlaufend massenhaft gespeichert.

### Reaktive Sicherheit vs. Datenminimierung

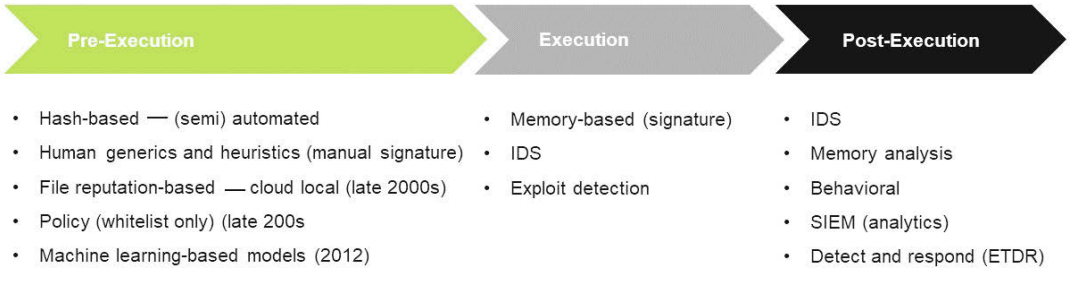
Um das Dilemma zu verstehen, das die Ausführung einer Malware am Endpunkt und die anschließende Analyse hervorrufen, muss man die Frage beantworten: Was genau sollen diese Lösungen eigentlich überwachen? Protokollieren sie Netzwerk- und Betriebssystemdaten sowie das Verhalten auf Anwendungsebene, so sammeln sie riesige Datenmengen. Zur Illustration dient ein kleines Rechenexempel: Nehmen wir an, die Systeme sammeln 1 MByte pro Stunde und Host multipliziert mit 24 Stunden. Für 1000 Hosts bedeutet das eine Zahl von 24 Millionen Ereignissen oder 24 GByte an Daten pro Tag. Nach 90 Tagen haben sich 2,1 Milliarden Datensätze oder 2,1 TByte Daten angesammelt. Datenvermeidung sieht anders aus!

Dabei entsteht eine ganze Reihe versteckter Kosten etwa für die Verwaltung oder die Analyse von immer mehr Sicherheitsvorfällen. Die kontinuierliche Überwachung aller Endpunkte kann überdies zu Leistungsengpässen führen. So zahlt der Sicherheitsanbieter zwar für Cloud-Storage, aber das Unternehmen für die Bandbreite. Lokales Hosting, um große Datenmengen vor Ort zu verwalten, treibt indes beides in die Höhe: Komplexität und Kosten. Dazu kommen datenschutzrechtliche Bedenken. Am Ende sammeln solche Lösungen mehr Informationen als notwendig, erwünscht oder gestattet. Und trotzdem reichen die Informationen über verdächtige Dateien oft nicht aus, um eine Malware zu erkennen bevor der Schadcode ausgeführt wird. Es existieren genügend Beispiele für Malware, die über Wochen, Monate oder sogar Jahre hinweg unentdeckt bleiben konnte.

### Wie spät ist zu spät?

Erlaubt man einer Malware ihren Schadcode auszuführen, erweitert das eher ihre Möglichkeiten statt sie einzuschränken. Detect-and-Response-Systeme haben eine Reihe von Nachteilen. Analysiert man die Malware nach dem Ausführen des schädlichen Codes, beobachtet man den Verdächtigen quasi in seiner natürlichen Umgebung. Nur so kann man die relevanten Ereignisse erkennen, protokollieren und blockieren. Aber selbst unter andauernder Beobachtung ist es schwer zu prognostizieren, wann eine Malware wie etwa Rombertik ihr hässliches Gesicht zeigt.

Kann eine Überwachungstechnologie dann bereits das initiale Ereignis, etwa die Installa-




Quelle: Cylance

**Drei-Phasen-Modell für Strategien der Angriffserkennung**

tion eines Treibers, als potenziell schädliches Ereignis erkennen? In den meisten Fällen wahrscheinlich nicht. Aber wenn bereits ein bösartiger Kernel-Treiber läuft, ist es vermutlich zu spät, die Systemintegrität zu wahren. Meist gibt es zwar verschiedene Anzeichen einer erfolgten Kompromittierung, doch dann lässt sich die Malware kaum noch blockieren. Besonders, wenn dieses Verhalten nicht rechtzeitig und nicht jedes Mal erkannt wurde. Das altbekannte Katz-und-Maus-Spiel: kein Schutz ohne vorheriges Wissen. Erkennt man eine Malware nicht rechtzeitig, entstehen irreversible Schäden:

*Parasitäre Infektion.* Lässt man eine parasitäre Infektion laufen, die kritische Dateien infiziert, steigen die Kosten für die Wiederherstellung. Der Datenbestand kann dauerhaft beschädigt sein, sodass ein System komplett neu aufgebaut oder aus dem Backup wiederhergestellt werden muss.

*Datenvernichtung.* Wir haben eine Reihe von groß angelegten Angriffen erlebt, die ein Detect-and-Response-Ansatz nicht verhindern konnte. Bei den Attacken auf Saudi Aramco und Sony Pictures wurde in beiden Fällen ein signierter kommerzieller Kernel-Treiber verwendet, um die Daten auf den Zielrechnern zu löschen.

*Erkennen von Sicherheitslösungen und „feindliche Invasion".* Die Rombertik-Malware ist ein Paradebeispiel für das, was eine Malware anrichten kann, wenn der Schadcode ausgeführt wird. Rombertik versucht nicht nur die Kontrollmechanismen der Sicherheitslösungen zu umgehen, sondern die Rechner zu zerstören, auf denen die Analysesoftware installiert ist.

*Daten-Exfiltration.* Im Laufe der Jahre sind wir unterschiedlicher Point-of-Sale Malware begegnet. Zum Beispiel Framework POS, die einen DNS-Mechanismus benutzt hat um Kreditkartendaten abzuziehen. Oder die berüchtigte BlackPOS-Malware, mit der es z. B. die US-amerikanische Handelskette Target zu tun bekam.

*Direkte Angriffe auf Sicherheitslösungen.* Das Ausführen von Malware hat einige bösartige Programme in die Lage versetzt, Sicherheitslösungen und Endpoint-Agenten direkt anzugreifen. Die Vawtrak-Malware versucht elegant die Sicherheitssoftware mithilfe der Richtlinien zur Beschränkung von Softwareinstallationen zu deaktivieren.

## Zurück in die Zukunft

Was haben Anbieter und Anwender in fast einem Jahrzehnt aus all dem gelernt? Ganz offensichtlich reicht es nicht aus, sich auf rein reaktive Ansätze, manuelle Analysen und das Erstellen von Signaturen zu verlassen. Dennoch sind vorausschauende Ansätze zunächst aus dem Fokus von Herstellern und Anwendern verschwunden. Das beginnt sich nun zu ändern. Unter anderem, weil maschinelles Lernen und künstliche Intelligenz in der Informationssicherheit angekommen sind.

Die größte Herausforderung einer Pre-Execution-Umgebung besteht darin, das Programm zu analysieren und zu entscheiden, ob es sich um eine harmlose Datei handelt oder um eine potenzielle Schaddatei. Diese Entscheidung wird aufgrund von Informationen und Merkmalen der betreffenden Datei getroffen. Sehr vielen Merkmalen. Und es ist nötig, große Zahlen von Samples zu analysieren. Allein schon deshalb, weil Malware heutzutage automatisch generiert und verteilt wird. Angreifer können mit geringem Aufwand eine Malware verändern und neue Mutationen erzeugen.

Manuell generierte Signaturen (oder heuristische und emulationsbasierte) halten mit der Masse automatisch erzeugter Varianten nicht Schritt. Mithilfe von maschinellem Lernen lassen sich jedoch Modelle erstellen, die vorhersagen, ob ein Programm bösartig ist oder nicht. Das gilt auch für neuartige und bis dato ungesehene Malware. Diese zu erkennen, bevor sie ausgeführt wird, ist natürlich kein Allheilmittel. In der Praxis geht es darum, das Risiko präventiv zu senken, und genau das tun Lösungen, die Modelle maschinellen Lernens zur Codeanalyse nutzen.

## Gegen die Datenflut

Post-Execution-Ansätze sind nicht nur ineffektiv, sondern produzieren immens viele Daten und damit gleichzeitig einen wachsenden Bedarf für Sicherheitsanalysen. Gibt man den Versuch auf, eine Bedrohung präventiv zu stoppen ist das eine mindestens riskante Haltung. Dazu kommen die Anforderungen der am 25. Mai 2018 verbindlich werdenden EU-Datenschutz-Grundverordnung. Mit ihr müssen Unternehmen nun endlich ihrer Datenflut Herr werden. Sicherheitsstrategien und -ansätze, die im Gegensatz zu den traditionellen Detect-and-Response-Modellen vorausschauend arbeiten, haben im Licht der DSGVO betrachtet noch einen weiteren Vorteil, weil Unternehmen weniger Daten sammeln müssen. Ein Pre-Execution Environment stärkt also in mehrfacher Hinsicht die Datensicherheit im Unternehmen.

*Sascha Dubbel*
*Senior Systems Engineer DACH, Cylance*

# Ist das datenschutzkonform – oder muss das weg?

## Bei der IT-Konsolidierung gibt es in Zeiten der Datendämmerung einiges zu beachten

Die EU-DSGVO hält für IT-Experten und Entscheider etliche Herausforderungen bereit. Sei es beim Design neuer Software- und Datenbanklösungen oder bei der datenschutzkonformen Anpassung bestehender Systeme – was müssen Entwickler und Leiter in Fachabteilungen über brauchbare Lösungen wissen?

Die Erfüllung der Anforderungen aus der EU-Datenschutz-Grundverordnung (DSGVO) ist eine ganzheitliche betriebliche Aufgabe. Sie betrifft alle Unternehmensbereiche und -prozesse, in denen personenbezogene Daten verarbeitet werden – egal ob analog oder digital. Beteiligte müssen geeignete und kontinuierlich geprüfte Verfahren bereitstellen, um einen datenschutzkonformen und transparenten Umgang mit personenbezogenen Daten zu gewährleisten. Demzufolge stellt sich für IT-Führungskräfte die Frage, wo sie primär ansetzen müssen, um diese Aufgabe nachhaltig zu lösen, und wie sie verhindern, dass der damit verbundene Berg an Herausforderungen wächst.

### Umsetzung von DSGVO-Projekten

Schon während des Designs einer Software- oder Datenbanklösung treten Faktoren zu Tage, die auf das Datenschutzkonto einzahlen. Mit folgenden Empfehlungen halten Entwickler und Administratoren den (Mehr-)Aufwand bei der Implementierung DSGVO-relevanter Punkte überschaubar.

Wichtig ist eine klare Trennung von Informations-, Einwilligungs- (Opt-in) und archivierungspflichtigen Daten. Für datenschutzkonforme Systementwicklungen zeichnet es sich als notwendig ab, Daten redundant zu speichern und sie mindestens in die Kategorien Informationsdaten, widerrufliche Einwilligungsdaten und Archivierungsdaten einzuteilen.

Bei *Informationsdaten* handelt es sich um Informationen zu einer Person, die nicht der gesetzlichen Archivierungspflicht unterliegen. Sie müssen umgehend nach Erfüllung des Erhebungszwecks gelöscht werden. Als Beispiel dient die Löschung von Kreditkartendaten nach dem Bezahlvorgang.

*Widerrufliche Einwilligungsdaten*, oder Opt-in-Daten, sind Informationen, die bis zum Widerruf zu einem bestimmten Zweck vorgehalten werden, um die Umsetzung eines wiederkehrenden Wunsches zu ermöglichen. Beispiele hierfür sind die E-Mail-Adresse für den Newsletter oder das Geburtstagsdatum für jährliche Glückwünsche. Für werbliche Maßnahmen wie einen Newsletter-Versand dürfen Anwender ausschließlich Daten verwenden, deren Eigentümer ihre explizite, temporäre Zustimmung hierfür abgegeben haben. Sobald Datenschutzbehörden nachweisen, dass eine Kontaktaufnahme zu Personen erfolgte, die nicht explizit über Opt-in zustimmten, können sie diese mit erheblichen Geldstrafen belegen. Entscheidend ist Transparenz für die Dateneigentümer, damit sie überblicken können, wie ihre Daten verwendet werden, und sie gegebenenfalls die einmal erteilte Zustimmung jederzeit zurückziehen können. Unternehmen sollten darauf achten, Antworten und Aktionen sorgfältig zu dokumentieren, damit Audits gelingen. Empfehlenswert ist zudem das Design eines Datenbankbereichs für Textbausteine. Dies können zum Beispiel Einwilligungsvorlagen oder juristische Texte sein.

*Archivierungsdaten* stellen eine Sammlung an Informationen dar, die beispielsweise für die gesetzlichen Aufhebungsfristen im medizinischen Bereich oder in der Buchhaltung benötigt werden, um Vorgänge nachvollziehen zu können. Das sind unter anderem Rechnungsdaten zum Kauf von Produkten und Dienstleistungen. Erst nach Ablauf der gesetzlichen Aufbewahrungspflicht dürfen diese Archivierungsdaten gelöscht werden – ein Löschvorgang, der mit Inkrafttreten der DSGVO bindend ist. Diese Daten dürfen von den Unternehmen nicht mehr verarbeitet werden.

### Archivierungspflichten

Im Design neuer Software- und Datenbankentwicklungen sollte für nahezu jedes Datenfeld eine Tabelle mit den dazugehörenden gesetzlichen Archivierungspflichten hinterlegt sein. Beispiele für Datenfelder sind Rechnungsnummer, Rechnungsdatum und der Nettobetrag. Mitarbeiter müssen Belege entsprechend der Abgabeverordnung (AO) nach Steuerrecht zehn Jahre, Belege gemäß Handelsgesetzbuch (HGB) sechs Jahre archivieren. Wesentlich für Neuprojekte sind jedoch branchenbezogene Spezifika in puncto Archivierungsauflagen.

So müssen Unternehmen bei der Verarbeitung von Daten wie einer Arztrechnung, in Verbindung mit Patientendaten nach Strahlenschutzbeziehungsweise Röntgenverordnung, eine Frist von bis zu 30 Jahren berücksichtigen. Gleiches zählt auch für Aufzeichnungen nach dem Transfusionsgesetz. Gelten für personenbezogene Daten mehrere und dabei divergierende Auflagen zur Archivierung, so empfiehlt es sich, nicht nur die maximale Archivierungszeit, sondern alle Fristen anzulegen. Denn wenn Entwickler lediglich die Maximalzeit berücksichtigt haben, müssen sie bei Veränderungen erneut Hand an die Software legen.

Auch sollten Verantwortliche rollenbasierend den Terminus „Ansichtsfristen“ pro Feld hinterlegen. Was bedeutet das? Archivierungsdaten für Rechnungen sind nur fünf Jahre für die „Rolle A“ einsehbar, für die „Rolle B“ in der ganzen Laufzeit. Bei besonders schützenswerten Informationen wie Gesundheitsdaten ist ein Einblick für Administratoren ohne Betriebsrat und/oder Datenschutzbeauftragte zu unterbinden, sprich: Beide stellen ihren Schlüssel zur Einsichtnahme zur

Verfügung. Eine auf das Datenfeld basierte Verschlüsselung, die für bestimmte Informationen das Verfallsdatum bereits einbaut, eignet sich hierfür am besten.

## Datenschutz-Booster für bestehende Systeme

Was passiert mit Datenbanken, deren Speicher zum Bersten gefüllt sind, während niemand weiß, welche personenbezogenen Daten darin lagern? Bei vielen Anwendungen existiert keine Transparenz darüber, wo diese Daten liegen und wer im Unternehmen für die allgemeine Speicherung verantwortlich zeichnet. Dies beschreibt eine Situation, in der sich aktuell viele Firmen, Behörden und Institutionen befinden. Berücksichtigen IT-Beauftragte Datenschutz und Entwicklungseffizienz, dann ist es unmöglich, auf diese Situation aufzubauen, neue Daten unter DSGVO-Gesichtspunkten zu behandeln und den bestehenden Datenpool zu ignorieren.

In einem großen Unternehmen jedoch alle personenbezogenen Daten zu identifizieren und sie zuzuordnen, scheint, vorsichtig formuliert, ehrgeizig. Diese umfangreichen und komplizierten Prozesse stellen für alle Beteiligten eine der größten Herausforderungen auf dem Weg zur Datenschutzkonformität dar. Nicht erkannte, frei flottierende und unsachgemäß gespeicherte Datenbestände bergen ein hohes Risiko für Sicherheitsverletzungen und können eine Haftung nach DSGVO mit sich tragen. Konzentrierte Anstrengungen, diese nicht verwendeten Daten zu finden und zu löschen, reduzieren die Strafen im Ernstfall erheblich.

Hier empfiehlt es sich für IT-Verantwortliche, analog zu Neuprojekten zu verfahren. Erschwerend kommt hinzu, dass es schwierig ist herauszufinden, wo sich relevante Informationen befinden und von wem und wie diese prozessiert werden. Dieses Mammutprojekt ist leider nur teilweise mit Software abbildbar, da es sich zumeist um gelebte Prozesse handelt.

## Software-Einsatz

Was müssen Entwickler und Leiter in Fachabteilungen über brauchbare Lösungen wissen? Sie benötigen zum Start eine Beschreibung des Löschprozesses personenbezogener Daten in den operativen und dispositiven Systemen des Unternehmens. Bei der Entwicklung und dem Einsatz von Software muss eine datenschutzkonforme Löschung dieser Daten oberste Priorität haben.

Derzeit gibt es nahezu keine Standardsoftware, mit der Nutzer konform Daten löschen können. Diesen Punkt sehen Anwendungsentwickler in der Konzeption von Software meist nicht vor. Um den Anforderungen der DSGVO gerecht zu werden, müssen sie nun nachträglich flächendeckend Softwareänderungen durchführen. Um eine aufwendige und fehleranfällige manuelle Löschung zu vermeiden, bietet sich die Entwicklung automatischer Löschroutinen an. Auch bei der Erstellung von Übersichten über Personendaten sollten Entwickler die Prozesse softwareseitig unterstützen, um die enormen Aufwände und die Fehleranfälligkeit einer manuellen Auswertung zu vermeiden.

Nach welchen Kriterien sich eine Anpassung lohnt und wann eine neue Softwarelösung sinnvoll ist, zeigt sich als klassische Güterabwägung. Tendenziell empfiehlt es sich, Refactoring den Vorzug zu geben, statt alte, unzeitgemäße Systeme in die neue Welt hinüberzuretten.

## Mindestprüfungen und Small Data

Bei bestehenden IT-Systemen müssen Entwickler etablierte Prozesse wie Audits und Penetrationstests adaptieren; Projekte, die teilweise mit großen Herausforderungen verbunden sind. Es gibt hierbei jedoch Mindestanforderungen an Überprüfungen bestehender Systeme. Unter der Voraussetzung, dass mindestens drei Umgebungen (Dev=Entwicklung, Test und Prod=Produktion) vorhanden sind, sollten Administratoren, Entwickler und IT-Sicherheitsmitarbeiter idealerweise folgende Prüfverfahren automatisch vornehmen: 1. Schwachstellenanalyse (Vulnerability Scans); 2. Schadsoftware-Überprüfungen (Malware Scans); 3. Compliance Scans wie Härtungen, bei denen IT-Komponenten auf Sicherheitsaspekte hin verändert werden; 4. Historisierung der Codes innerhalb der Softwareentwicklung (idealerweise bei jedem Commit), Einführung eines Versionskontrollsystems (beispielweise mit GIT).

Diese Mindestprüfungen müssen Anwender ausführen und die Ergebnisse in der Deployment-Pipeline lückenlos dokumentieren. Ein praxisnahes Konzept zeigt auf, wie IT-Beauftragte anfallende Daten verarbeiten und worauf sie gesondert achten müssen: Zu Beginn erfassen Projektverantwortliche alle anfallenden Daten und klassifizieren sie. Im Klassifizierungsprozess spielt auch eine Rolle, dass neben der DSGVO noch weitere Gesetze, Regularien und Behördenauflagen existieren. Dazu zählen die Abgabenordnung (AO) als elementares Gesetz des deutschen Steuerrechts; das IT-Sicherheitsgesetz (IT-SiG), weithin auch unter KRITIS bekannt; diverse E-Health-Gesetze wie die EU-Verordnungen zu Medizinprodukten und In-vitro-Diagnostika. Interessanterweise widersprechen sich diese Verordnungen zum Teil und erfordern eine permanente und gründliche Prüfung aller Parameter, die für die eigenen Daten greifen. Festhalten lässt sich, dass bei unterschiedlichen Zeiträumen zur Datenspeicherung und Archivierung immer die längste Zeitspanne zählt.

## Datenschutz in der Cloud

Als nächstes sollten Projektverantwortliche prüfen, wie personenbezogene Daten, die sich auf Geschäftsaktivitäten beziehen, in datenschutzkonformem Umfang gesammelt werden können und / oder wie eine Pseudonymisierung der Daten gelingt. Diese Pseudonymisierung meint die „Verarbeitung personenbezogener Daten in einer Weise, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“ (Kapitel 1 Art. 4 DSGVO).

Nach dem neuen Gesetz „Clarifying Lawful Overseas Use of Data Act“ (CLOUD) sind amerikanische Internet-Unternehmen, also auch Cloud Service Provider aus den USA, dazu verpflichtet, amerikanischen Sicherheitsbehörden Zugriff auf Nutzerdaten zu ermöglichen, die außerhalb der USA gespeichert sind. Daraus folgt der zwingende Rat an Entwickler, auch unter Berücksichtigung der DSGVO, sich mit der Verschlüsselung „on Rest“, „in Transit“ und „in Use“ vertraut zu machen und so schnell wie möglich mit der Implementierung zu beginnen.

## Fazit

Zusammenfassend lässt sich festhalten, dass vor allem eine exakte Bestandsaufnahme aller datenverarbeitenden Prozesse und ihrer IT-Systeme im Unternehmen die Basis aller Entscheidungen pro und contra Neuentwicklung bildet. Darauf bauen Überlegungen zu Security-by-Design-Projekten, zu ihrem Umfang, dem personellen Einsatz und den eingesetzten Methoden auf.

*Pierre Gronau*
*Gronau IT Cloud Computing*

# Sicherheit aus dem Container

## So lassen sich Sicherheitsrisiken auf mobilen Endgeräten minimieren

Smartphones und Tablets sind Achillesfersen der IT-Sicherheit, erst recht, wenn es sich um private Geräte handelt. Container-Lösungen schirmen Unternehmensdaten in einem verschlüsselten Bereich wirksam ab. Damit lassen sich auch die Vorgaben der EU-DSGVO problemlos erfüllen.

Die Nutzung mobiler Endgeräte ist geradezu ein Musterbeispiel für Consumerization: Einmal auf den Geschmack gekommen, wollen viele Anwender auch im Job nicht auf ihre privaten Smartphones und Tablets verzichten – nicht auf das überlegene Bedienungskonzept, nicht auf die vielfältigen Kommunikationsmöglichkeiten, nicht auf Kompaktheit und Flexibilität. Dagegen sehen herkömmliche Desktops einfach ziemlich alt aus. Anfangs verhinderten noch die Bedenken der Unternehmen den breiten Einsatz mobiler Systeme. Doch es zeigt sich immer wieder, dass sich echter Bedarf nicht einfach durch Vorschriften ausbremsen lässt. Mittlerweile haben die meisten Unternehmen in dieser Frage die weiße Flagge gehisst. Und schließlich bedeutet Bedienkomfort ja auch Produktivität und Effizienz.

### Mobile Risiken

Die Bedenken speziell der IT-Abteilungen sind damit freilich nicht aus der Welt geschafft, die Herausforderungen für Management, Datenschutz und Sicherheit bleiben bestehen. Mobile Systeme werden anders als Desktops in ungeschützten Umgebungen benutzt – im Hotel, auf dem Bahnsteig, im Bus – und da sind die Risiken naturgemäß groß, etwa durch unsichere WLANs. Dies gilt besonders, wenn es um mobile Geräte geht, die gar nicht dem jeweiligen Unternehmen gehören, also um private Smartphones und Tablets, die von den Mitarbeitern – nebenbei – für berufliche Zwecke genutzt werden (Bring Your Own Device – BYOD).

Die IT hat auf diese Geräte nur einen eingeschränkten Zugriff, sie muss diesen immer auch mit dem Eigentümer teilen, sodass es nicht ohne Weiteres möglich ist, einheitliche Sicherheitseinstellungen, Richtlinien und Zugriffsrechte zu definieren und zu realisieren. Da sich auf den Geräten regelmäßig auch private Daten befinden, die unter strengem gesetzlichen Schutz stehen, kann eine IT-Abteilung hier nicht einfach durchgreifen und z. B. Daten auf einem verloren gegangen Gerät aus der Ferne löschen.

Dabei sind die Risiken, die für Unternehmen aus dem Einsatz von Smartphones und Tablets entstehen, überaus real: Die Marktforscher von IDC schätzen, dass 2017 in etwa zwei Drittel der Unternehmen in Deutschland, die mit mobilen Endgeräten arbeiten, auch entsprechend Sicherheitsvorfälle zu verzeichnen waren. Da zahlreiche Angriffe gar nicht erst entdeckt werden, kommt noch eine hohe Dunkelziffer dazu.

So wichtig Lösungen für MDM (Mobile Device Management), die mobile Geräte zentral verwalten, grundsätzlich sein mögen, für die Sicherung der auf mobilen Geräten befindlichen Daten und Anwendungen reichen sie keinesfalls aus. Dafür müssen unmittelbar auf dem jeweiligen mobilen Gerät die privaten und die dienstlichen Daten und Anwendungen strikt voneinander getrennt werden. Nur wenn das mobile Gerät gewissermaßen aus zwei virtuellen Systemen besteht, kann es auch mit hinreichender Sicherheit betrieben werden.

### Sicherheit auf beiden Seiten

Realisieren lässt sich das mit einer Container-Lösung. Ein solcher Container ist ein automatisch verschlüsselter Bereich, in dem Unternehmensdaten, E-Mails, Kontakte, Kalender, Notizen, Aufgaben und Dokumente gespeichert werden. Im Falle eines Diebstahls oder Verlusts bleiben die Daten auf diese Weise vor Missbrauch geschützt. Der Container verhindert auch, dass Mitarbeiter aus dem sicheren Unternehmensbereich auf eine private App zugreifen und so Daten etwa mit Copy-and-Paste in den privaten Bereich übernehmen. Andere Anwendungen erhalten grundsätzlich keinen Zugriff auf die Inhalte des Containers. WhatsApp beispielsweise kann daraus keine Kontaktdaten übernehmen.

Die Container-Lösung verfügt über ein Management-Portal, in dem Administratoren Sicherheitsregeln festlegen können, zum Beispiel Vorgaben für die Länge von Passwörtern, Regeln für das Sperren von Geräten und für den Zugriff auf Intranet-Anwendungen oder Fileshare. Die Verschlüsselung erstreckt sich nicht nur auf die Inhalte des Containers auf dem mobilen Endgerät, sondern ebenfalls auf den Datenaustausch, sodass auch keine Man-in-the-Middle-Angriffe möglich sind.

Eine Container-Lösung schützt nicht nur die Daten und Anwendungen des Unternehmens, sondern im BYOD-Fall zugleich auch die Privatsphäre der Eigentümer. IT-Administratoren haben keinen Zugang zum Gerät, sondern steuern immer nur den Container, die gesetzlichen Anforderungen für den Schutz der Privatsphäre werden eingehalten. Andererseits können Unternehmen damit auch die rechtlichen Vorgaben für den Schutz der Unternehmensdaten einhalten, etwa bezüglich personenbezogener Daten von Kunden, Lieferanten, Geschäftspartnern und Mitarbeitern. Denn: Unternehmen sind gesetzlich für die Einhaltung des Datenschutzes bei der Verarbeitung personenbezogener Daten verantwortlich, auch wenn Mitarbeiter private mobile Endgeräte dafür benutzen.

### Datenschutz auch unterwegs

Mit einer Container-Lösung sind Unternehmen schließlich auch bei den Anforderungen der EU-DSGVO auf der sicheren Seite. Die technisch realisierte Trennung von beruflichen und privaten Apps und Daten erlaubt es, geltende Compliance- und rechtliche Vorgaben sowie unternehmensweite IT-Sicherheitsrichtlinien auch auf mobilen Systemen umzusetzen und deren Einhaltung zu überwachen. Damit lassen sich die drohenden hohen Bußgelder, die Aufsichtsbehörden aufgrund unzureichender organisatorischer und technischer Sicherheitsmaßnahmen verhängen können, vermeiden.

*Günter Junk*
*CEO Virtual Solution AG*

# Malware überlistet Sandbox

## Aufmerksame Fraunhofer-Forscher finden eine neue Sicherheitslücke

Schadsoftware plagt Privatleute und Unternehmen gleichermaßen. Sie späht Nutzer und Firmennetze aus, stiehlt vertrauliche Daten oder beschädigt die Hardware. Daher gehören nicht nur Anti-Viren-Software, sondern auch Sandboxen zur IT-Grundausstattung vieler Unternehmen – doch wie sicher sind sie?

Eine Sandbox ist eine speziell abgesicherte Umgebung, in der ein frisch heruntergeladenes Programm laufen kann, ohne Verbindung zum Rest des Systems zu haben. Gleichzeitig überwacht die Sandbox das Verhalten der Software und protokolliert ihr Verhalten. Deshalb werden sie von Sicherheitsexperten genutzt, um Funktionsweise und Gefährlichkeit von Schadsoftware zu untersuchen.

Zwischen den Herstellern von IT-Sicherheitslösungen und den Malware-Autoren herrscht ein ständiger Wettlauf. Beide Seiten versuchen, ihre Gegenspieler mit immer neuen Kniffen auszutricksen. Nun haben Wissenschaftler des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) eine bislang unbekannte Schwachstelle von Sandboxen entdeckt. Sie fanden eine Methode, mit der Software das Konzept der Sandbox aushebelt, indem sie die Analyse-Reports manipuliert. Malware, die nach dieser Methode vorginge, würde der Sandbox falsche Aktivitäten vorgaukeln und auf diese Weise der Entdeckung entgehen.

### Unbekannte Schwachstelle

Anfang Oktober 2017 schrieb das Fraunhofer-Team um Viviane Zwanger und Dr. Elmar Padilla ein internes Tool zur Überwachung, Beobachtung und Änderung von speziellem Programmcode und den dazugehörigen gerätebezogenen Programmteilen. Dahinter stand die Idee, die Aktionen der untersuchten Malware anpassen zu können, um Aktion und Reaktion auch unter künstlichen Bedingungen untersuchen zu können.

Das Ergebnis war verblüffend. „Das Tool funktionierte wie vorgesehen, aber da es in einer Sandbox ausgeführt wurde, stellten wir fest, dass der Bericht falsch war“, schreiben Zwanger und Padilla in ihrem Aufsatz. Im Report der Sandbox fanden sich die ursprünglich programmierten Aktionen wieder. Aber die Wissenschaftler wussten, dass das nicht stimmen konnte. Sie selbst hatten durch eine Modifikationsroutine die Aktionen in der Zwischenzeit verändert. Außerdem hatten sie die Folgen ihrer Änderungen beobachtet, etwa eine Verbindung zu einem von ihnen kontrollierten Server oder zu einer auf der Festplatte erzeugten Datei.

### Wie die Schwachstelle wirkt

Bei dieser neuen Form der Sandbox Evasion führt die Malware zunächst eine „Fake-Aktion“ durch. Während die Sandbox die Aktion aufzeichnet, verändert sie die Malware so, dass die Sandbox eine gutartige Aktion protokolliert. Die Fake-Aktion kann dabei alles mögliche sein, beispielsweise Dateien senden oder empfangen, schreiben oder verändern. Bei einer anfälligen Sandbox bekämen die Nutzer nichts davon mit.

Zwanger und Padilla weiteten die Untersuchung aus. Sie baten das Zentrum Cyber-Sicherheit der Bundeswehr (ZCSBw) um Unterstützung, denn dort standen viele verschiedene Sandbox-Systeme zur Verfügung. Sie prüften acht Sandbox-Lösungen mit Blick auf ihre Anfälligkeit. Der Test umfasste Systeme der Hersteller BlueCoat/Symantec, VM-Ray, Lastline, Huawei, ThreatTrackSecurity/Vipre, VxStreams und JoeSandbox. Als einzige nichtkommerzielle Sandbox unterzogen sie Cuckoo einer genaueren Prüfung.

Vier der Sandboxen waren verwundbar, eine nur zum Teil. Die restlichen drei ließen sich nicht beeinflussen. Das bedeutet, so Zwanger und Padilla in ihrer Dokumentation, dass in vier Fällen der Sandbox-Bericht über Aktionen informiert, die nie stattgefunden haben, jedoch über keine von denen, die die Malware in Wirklichkeit ausgeführt hat. Dementsprechend fällt das Fazit der Fraunhofer-Experten aus: „Das Gegenteil einer funktionierenden Sandbox."

### So funktionierte der Test

Zwanger und Padilla lösten zuerst einen frei gewählten API-Aufruf der Anwendung aus. API steht für „Application Programming Interface“, also eine Schnittstelle, die die vom Betriebssystem bereitgestellten Funktionen abstrahiert und Programmen in vereinfachter Form zur Verfügung stellt. Einer ihrer Tests war die Funktion „connect ()“ aus der Winsock-Bibliothek. Darin wurden zunächst ein falscher Port und eine gefälschte IP-Adresse verwendet. Während der Verarbeitung des Aufrufs änderte die Modifikationsroutine beide Parameter auf eine reale IP-Adresse und einen realen Port.

War die getestete Sandbox anfällig, schrieb sie nun einen Analyse-Report über den Aufruf der falschen IP und des falschen Ports, während der Aufruf der echten Ziele nicht auftauchte. Weil jeder Hersteller seine eigenen Lösungen anbietet, testeten die Fraunhofer-Wissenschaftler auch die verschiedenen Sandbox-Techniken.

Eine Usermode-basierte Sandbox läuft als normaler Prozess auf dem System. „Sie kann auch als normaler Prozess gesehen, gelesen, umgeschrieben und ausgeschaltet werden“, so Viviane Zwanger. Kernelmode-basierte Sandboxen arbeiten im Betriebssystemkern als Kerneltreiber. Sie laufen zwar in einem dem Kernel zugewiesenen Bereich, bleiben dort aber verwundbar. Hypervisor-basierte Sandboxen sind eines von mehreren Gastsystemen auf einem Hostsystem. Ein Hypervisor verwaltet die Zuteilung von Systemressourcen an die einzelnen Gastsysteme. Die Sandbox nutzt hier ihr Interface mit dem Hypervisor, um zu kommunizieren.

Hinzu kommen Emulator-basierte Sandboxen. Ein Emulator stellt eine bestimmte Systemumgebung, etwa ein Betriebssystem oder ein Hardware-Gerät wie ein Handy nach. So können auf einem Computer andere Systeme nachgebildet werden. In diesen sind dann Programme

lauffähig, die eigentlich für eine andere Umgebung konzipiert sind. So kann ein Software-Entwickler ein Programm für ein bestimmtes Gerät in einem Emulator testen, ohne das echte Gerät nutzen zu müssen. Analog läuft die Sandbox in einer eigenen virtuellen Umgebung, die ein komplettes System mit angeschlossenen Geräten nachbildet. Dabei stoßen Emulatoren schnell an Komplexitätsgrenzen.

Die meisten verfügbaren Sandbox-Lösungen sind Hybride. „Die verschiedenen Ansätze haben ihre Vor- und Nachteile, keiner ist perfekt", so Viviane Zwanger. Jedoch bleiben die Eingriffe der Malware auf der Usermode-Ebene. Zwanger stuft sie als „minimal-invasiv" ein. Eine genaue Diagnose war nicht möglich, weil sie und Padilla keinen Zugriff auf die proprietären Codes der Sandboxen hatten. Den haben nur die Hersteller.

## Erste Gegenmaßnahmen

Gefälschte Sandbox-Berichte waren für Zwanger und Padilla ein echtes Novum, weil die Anwender diesen Berichten vertrauten. „Es war also für uns als Malware-Analysten eine kleine Überraschung, als wir herausfanden, dass die Berichte ohne großen Aufwand gefälscht werden können und nicht unbedingt die Wahrheit widerspiegeln", schreiben sie in ihrer Studie. Im Oktober 2017 teilten sie den verschiedenen Sandbox-Herstellern ihre Ergebnisse mit. Aber bisher hat nur einer auf die entdeckte Sicherheitslücke reagiert. Er veröffentlichte im Februar 2018 einen Patch. Es könnte sein, dass die anderen Hersteller das Problem stillschweigend behoben haben. Für die Open-Source-Sandbox Cuckoo arbeiten die Fraunhofer-Forscher gerade selbst an einem Patch.

Allerdings ist nicht klar, ob es tatsächlich Malware gibt, die die neue Methode zur Sandbox Evasion anwendet. „Anhand der Tatsache, dass es uns möglich war, zufällig darauf zu stoßen, halten wir es aber für denkbar", sagt Viviane Zwanger. Das wäre dann ein großes Problem. Denn wenn Anwender und Sandbox-Analysten tatsächlich durch falsche Sandbox-Berichte getäuscht werden, hätte Malware, die die von Zwanger und Padilla beschriebene Technik ausführt, freie Bahn.

## Informationen online

Sicherheitsverantwortliche von Unternehmen, die Sandbox-Systeme nutzen, sollten prüfen, ob ihre Sandbox verwundbar ist. Um das zu erleichtern, haben die Wissenschaftler ihren ausführlichen Bericht und weitere Hilfsmittel online gestellt: Unter der URL *https://www.fkie.fraunhofer.de/de/Pressemeldungen/aushebeln-sandbox.html* findet sich nicht nur ihr Bericht mit einer ausführlichen technischen Beschreibung ihres Vorgehens. Außerdem stehen ein Prüfungstool sowie ausführbare Dateien, wie sie Zwanger und Padilla selbst bei ihren Tests verwendet haben, zur Verfügung. Sicherheitsexperten können damit selbst feststellen, ob ihre eigene Sandbox betroffen ist und falsche Berichte schreibt.

*Friedrich List*

**Impressum**
**Themenbeilage Sicherheit & Datenschutz**

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

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

**Autoren dieser Ausgabe:**
Dr. Amir Alsbih, Sascha Dubbel, Daniel Eyring, Pierre Gronau, Günter Junk, Dr. Dennis-Kenji Kipker, Tomasz Lawicki, Friedrich List, Dr. Holger Mühlbauer

**DTP-Produktion:**
Matthias Timm, Hinstorff Media, Rostock

**Korrektorat:**
Ninett Wagner, Hinstorff Media, Rostock

**Titelbild:**
© shutterstock, Sentavio

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

**Geschäftsführer:**
Ansgar Heise, Dr. Alfons Schräder

**Mitglieder der Geschäftsleitung:**
Beate Gerold, Jörg Mühle

**Verlagsleiter:**
Dr. Alfons Schräder

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

**Leiter Vetrieb und Marketing:**
André Lux

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

# UNABHÄNGIG IN JEDER HINSICHT:
## c't als Heft und digital auf jedem Gerät lesen

In jedem Browser & auf jedem Gerät c't lesen

Videos & Tabellen direkt aufrufen


Lesezeichen & Kommentare synchronisieren

Optimale Darstellung für mobile Endgeräte

**Testen Sie jetzt c't online und stöbern Sie 3 Monate lang in allen verfügbaren Ausgaben.**

**Mit Willkommensgeschenk:** z.B. ein Kino- und Snack-Gutschein

JETZT TESTEN!

**Zum Angebot: ct.de/digital-erleben**

Bitte bei Bestellung über Telefon oder E-Mail angeben: 1CEA1713

ct.de/digital-erleben  +49 541/80 009 120  leserservice@heise.de

c't THEMEN & TESTS **MIT LEIDENSCHAFT.**

**heise.de/select/ct**

it sa 2018

Die IT-Security Messe und Kongress

HOME OF IT SECURITY

# MEIN UNTERNEHMEN EXPANDIERT MIT SICHERHEIT*

DANIEL CASE, CISO

## * NETWORKING@IT-SA

Seien Sie Teil der it-sa 2018 und starten Sie mit Ihrem Unternehmen sicher in die Zukunft. Nur auf Europas führender Fachmesse für IT-Security trifft sich jährlich das Who is Who der Branche.

Nürnberg, Germany
**9.-11. Oktober 2018**

**it-sa.de**

NÜRNBERG MESSE