Eine Themenbeilage der
Heise Medien GmbH & Co. KG

II
2016

SICHERHEIT & DATENSCHUTZ

Industrial Security und Kommunikationssicherheit

Verschlüsselung und Industrie 4.0:
Wie man Produktpiraten das Leben schwer macht

Cyberversicherungen:
Was die Reputation kosten darf

Industrial Security:
Worauf Anlagenbetreiber achten sollten

Mobile Devices:
Was ein effizientes EMM-Konzept ausmacht

B2B Security:
Warum Systemintegrität unverzichtbar ist

www.it-security-und-management.de

powered by: TeleTrusT Pioneers in IT security.

Ihr Einsatz ist gefragt

Liebe Leserinnen und Leser,

das Jahr 2016 neigt sich dem Ende entgegen. Es hat uns mit steigenden Bedrohungen durch Hackerangriffe, Verschlüsselungstrojaner und Datenlecks gezeigt, dass die Gefahren real sind. Kritische Infrastrukturen, wie etwa medizinische Geräte in Krankenhäusern, stehen zunehmend im Fokus von Hackern. Viele Verantwortliche wiegen sich in falscher Sicherheit, denn auch ohne Internetanbindung sind Anlagen gefährdet, was z.B. die in einem deutschen Atomkraftwerk gefundene Schadsoftware belegt. Cyberkriminelle erpressen nicht nur Geld von Unternehmen, sondern vermehrt auch von Privatpersonen. IT-Sicherheit ist daher längst nicht mehr nur ein Thema für Systemadministratoren. Der Grad der Digitalisierung des Alltags tangiert das Leben aller Bürger.

Auf staatlicher Ebene haben deutsche und europäische Gesetzgeber begonnen, dem gestiegenen Schutzbedarf Rechnung zu tragen und notwendige Rahmenbedingungen geschaffen. Mit dem deutschen IT-Sicherheitsgesetz und der neu gegründeten European Cyber Security Organisation (ECSO), die u.a. als Vertragspartner der EU-Kommission bei Public-Private-Partnership-Vereinbarungen auftritt, sind Weichen für die Zukunft gestellt.

Das Jahr 2017 wird dennoch auch politisch spannend bleiben. Wie wird sich die Regierung bezüglich der IT-Sicherheit und der fortschreitenden Digitalisierung aufstellen? Kommt der Breitbandausbau voran, was verändert sich beim Datenschutz und wie entwickelt sich z.B. der Referentenentwurf des eIDAS-Durchführungsgesetzes? Als Bundesverband IT-Sicherheit e.V. werden wir weiter alles daran setzen, bestmögliche Technologien voranzubringen und notwendige Informationen für die deutsche (IT-Sicherheits-) Wirtschaft bereitzustellen.

Die vorliegende Beilage „Sicherheit & Datenschutz“ will Ihnen Einblick in ausgewählte Themen der IT-Sicherheit verschaffen, die uns derzeit beschäftigen. Unsere Beiträge zielen dabei auf grundsätzliche Fragen ab, mit denen Sie sich als IT-Verantwortliche befassen sollten. Einen Schwerpunkt bildet diesmal das Thema „IT-Sicherheit und Industrie 4.0“ (S. 8, S. 21 und S. 23). Daneben werden auch Lösungsansätze für einen sicheren E-Mail-Transport (S. 14), zum Einsatz mobiler Geräte im Unternehmen (S. 12), zur Datenschutz-Zertifizierung von Cloud-Diensten (S. 25) und bei der Data Loss Prevention (S. 4) vorgestellt. Ein spezieller redaktioneller Beitrag zum Thema Cyberversicherungen (S. 16) rundet unseren Überblick ab.

Die Herausforderungen nehmen beständig zu. Dem steht jedoch eine starke, erfindungsfreudige Branche entgegen, die sich an neue Aufgaben dynamisch anpasst. 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“ wird auch weiterhin ein Garant für hohe Schutzstandards sein. Hier ist aber auch jeder Einzelne gefordert: Werden Sie aktiv, informieren Sie sich und setzen Sie notwendige Maßnahmen in der IT-Sicherheit um, damit Sie auch 2017 erfolgreich allen Sicherheitsrisiken trotzen können.

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

Inhalt

Alle Schotten dicht

Ein effizientes DLP-Konzept schützt vor dem Verlust sensibler Daten

In vielen Unternehmen und Behörden wird täglich mit Daten gearbeitet, die besonderen Schutz benötigen. Ungewollter Datenabfluss kann von außen, aber auch von innen ausgelöst werden. Deshalb müssen sämtliche potenziellen Datenlecks identifiziert, überwacht und abgesichert werden.

Daten sind der Rohstoff des 21. Jahrhunderts – und wecken Begehrlichkeiten. Längst hat sich eine Szene im Darknet etabliert, die gegen Zahlung den gezielten Datendiebstahl verspricht. Und anders als bei gestohlenen Autos lassen sich die Daten gleich mehrfach verkaufen – der Profit steigt. Die Gesetzgebung mag ausreichend sein, doch die Strafverfolgung ist nicht in der Lage, allen Delikten in allen Ländern nachzugehen. Der Schaden von einmal gestohlenen Daten kann, wenn diese bereits verkauft oder weitergegeben sind, nicht mehr geheilt werden, denn die Daten sind dann nicht mehr einzufangen.

Das einzig sinnhafte Konzept ist es deshalb, seine wichtigsten Daten selbst zu schützen. Sind die kritischen Daten identifiziert, gilt es, den adäquaten Schutz umzusetzen, denn nicht bei allen Daten gelten die gleichen Schutzziele. Manche müssen vor Innentätern geschützt werden, bei manchen ist es sinnvoll, die eigenen IT-Mitarbeiter vor dem Verdacht der unerlaubten Kenntnisnahme zu schützen. Mechanismen der Data Leakage/Loss Prevention (DLP), helfen dabei, ungewünschten Datenabfluss zu verhindern. Das eigene Risikomanagement definiert dann, wie robust der Schutzmechanismus jeweils sein muss.

Die gesamte Handlungskette sichern

Auch die Handlungskette bei der Datennutzung ist nur so stark wie ihr schwächstes Glied. Im ersten Schritt werden die Daten generiert. Im nächsten Schritt wird über Services, Netzwerke, Anwendungen oder Apps auf die Daten zugegriffen, um sie dem Nutzer zu präsentieren, der sie dann wiederum mithilfe anderer Anwendungen weiterverarbeitet, speichert, druckt, verschickt usw. Hat der Nutzer beliebige Freiheit bei der Verarbeitung, ist prinzipiell davon auszugehen, dass sich die Daten später elektronisch nicht wiedererkennen lassen, da sie verschlüsselt bzw. zu Bildinformationen oder in andere Formate gewandelt wurden. Für die Ziele der Integrität und Vertraulichkeit gilt es also, die gesamte Handlungskette so zu organisieren, dass ein adäquater Schutz in allen Lebenslagen für die Daten besteht. Das klingt noch relativ einfach, wenn man die wirklich sensiblen Daten in geeignet geschützten Datenräumen unterbringt und der Schutz mit hoher Robustheit durchgesetzt wird. Zur Absicherung der gesamten Handlungskette muss allerdings der vollständige Lebenszyklus betrachtet werden.

Eine erste Schwachstelle ist das Identity and Access Management (IAM). Angriffe auf die Passworteingabe mittels „über die Schulter schauen“ und Keylogger sind bekannt und können mit guten Awareness-Maßnahmen (auch gegen Kameras) und einigen Endpoint-Security-Lösungen verhindert werden. Der Angriff auf den Deutschen Bundestag im Jahr 2015 hat aber gezeigt, dass auch über andere Angriffe wie PassTheHash und Mimikatz die Identität eines Anwenders gestohlen werden kann, ohne dass man dessen Passwort und Username benötigt. Das Problem des Identitätsdiebstahls ist also viel komplexer, als dem Anwender seinen Besitz (Smartcard oder Zugangstoken) und sein Wissen (Passwort/PIN) zu stehlen.

Zugangskontrollen prüfen

Viele Sicherheitsberater gehen heute davon aus, dass man nicht jede Umgebung „sauber“ halten kann und in manche IT-Umgebungen wenig Vertrauen setzen sollte – insbesondere in solche, die über viele Services notwendigerweise mit dem Internet verbunden sind und dazu auch Nutzdaten austauschen. Wird dieselbe Kennung für diese unsicheren Umgebungen und gleichzeitig (ohne Zusatzschutz) für die sicheren Datenräume verwendet, kann von Sicherheit nicht mehr die Rede sein. Die Eingabe eines mehrfach nutzbaren Passwortes auf der Tastatur eines mobilen Endgerätes potenziert das Risiko. Wenn die Identität gestohlen ist, greifen alle nachfolgenden Sicherheitsmaßnahmen, die auf den Rechten Einzelner beruhen nicht mehr. Gleiches gilt natürlich für die unberechtigte Nutzung von Benutzerrechten durch schadhafte Anwendungen auf einem IT-System, mit dem der Anwender tatsächlich arbeitet.

Einem Benutzer sind aber meist mehrere Kennungen für unterschiedliche Datenräume nicht zuzumuten. Wichtig ist hier also die Vertrauensstellung der einzelnen Systeme untereinander. Ein System mit hoher Vertrauensstellung kann ein automatisches Login in ein niedrigeres System durchführen – umgekehrt darf das nicht passieren. Prinzipiell gilt also, dass die Tastatur zur Eingabe eines mehrfach verwendbaren Passwortes im Sicherheitsraum der genutzten Daten und Services liegen muss. Um lokale Angriffe zu vermeiden, müssen entsprechende Vorkehrungen bei der Kommunikation der Tastatureingaben getroffen werden.

Häufige Fehler bei DLP-Projekten

DLP-Projekte benötigen sehr viel Detailverständnis. Heutzutage sind IT-Projekte aber dazu gezwungen, bereits nach kurzer Zeit einen sichtbaren Nutzen zu erbringen und nicht als permanentes Groschengrab nur Ressourcen zu verbrauchen. Schnelle Erfolge lassen sich bei DLP-Projekten einfach erzielen: Das Monitoring der potenziellen Leckage-Punkte führt dazu, dass die notwendigen Schutzmaßnahmen erkannt und priorisiert werden können, ohne dabei den Betrieb zu behindern. Leckage-Punkte sind etwa Kommunikationsbeziehungen nach außen, wie E-Mail oder Browser-Upload, mobile Datenträger und spontane Kommunikation über Devices wie Bluetooth, WiFi etc., aber auch

Ausdrucke, Fotos von Bildschirmen und Informationen, die durch das „über die Schulter schauen“ gewonnen werden.

Wer zuerst versucht, alle vorhandenen Daten nach deren Kritikalität zu markieren – und dafür viel Zeit und Energie aufbringt – wird lange auf positive Resultate warten müssen. Das eigentliche Ziel, Daten vor unerlaubtem Abfluss zu schützen, wird man dann spät oder gar nicht mehr erreichen. Ignoriert man zusätzlich die systembedingten Ungenauigkeiten durch die unterschiedlichen Repräsentationen der gleichen Information (Sprachen, Sonderzeichen, OCR/Bild von Text, Formatierungen, Steganografie, Covert Channels …) in der Klassifikationsphase, werden viele „falsche Fehler“ (false positives und false negatives) dazu führen, dass man im Betrieb entweder häufig nachbessert und hohe administrative Kosten generiert oder die echten Schutzkriterien so lax einstellt, dass das Ergebnis den Aufwand nicht mehr wert ist.

Fallen identifizieren

Liegt der Fokus nur auf dem internen Datenabfluss, verstellt man den Blick auf Angriffe von außen, die erst im Ergebnis zum unerwünschten Datenabfluss führen. Häufig wird über Angriffe auf die Schwachstellen von Standardanwendungen (Browser-Exploit) oder Standardformate (Flash, PDF-Exploit) erst der unerwünschte Datenkanal nach außen geöffnet, der dann aufgrund stenografischer Verfahren nicht mehr erkannt werden kann. Der Angriff kommt aber von außen, weshalb es zu einer wesentlichen Aufgabe des DLP gehört, den „Import von schädlichen ausführbaren Objekten“ zu kontrollieren oder ganz zu verbieten, z.B. Javaskript in PDF, DLL-Download über Browser etc. Es ist also zwingend notwendig, ein Inventar aller zur Ausführung kommenden Programme zu halten und dieses sukzessive nach der Kritikalität für DLP zu bewerten. Dieser Schritt ist schon darum wertvoll, weil man alle Programme, Skripte, Makros etc. kennenlernt, die bisher nicht im Softwarekatalog oder dem offiziellen Inventar standen.

Best Practice für DLP

Einfache, weil im Betrieb unkritische Sicherheitsmaßnahmen (Quick Wins) sind zuerst an der Reihe. Das heißt, Maßnahmen wie Benutzersensibilisierung, Monitoring, Risikoinventarisierung und Alerting stellen die ersten Schritte dar und erlauben es, die Kritikalitätseinschätzung iterativ zu verfeinern. Die zyklische Untersuchung der statistischen Auswertung zeigt die realen Risiken und praktische Verstöße gegen die bestehenden Vorschriften auf. Bereits nach dieser Phase, die mit wenigen Arbeitsstunden erledigt ist, kann man klare Antworten auf die drängenden Fragen „Wie sicher sind wir?“ und „Wo ist unser dringendster Bedarf?“ geben. Das bildet die Grundlage für die regelmäßige Verfeinerung der technischen Sicherheitsmaßnahmen. Je nachdem identifizierten Datenmaterial, der verwendeten Applikation, dem Netzwerk, dem Datenträger, dem handelnden Benutzer und weiteren Parametern werden dann folgende Maßnahmen nahegelegt oder sogar erzwungen:

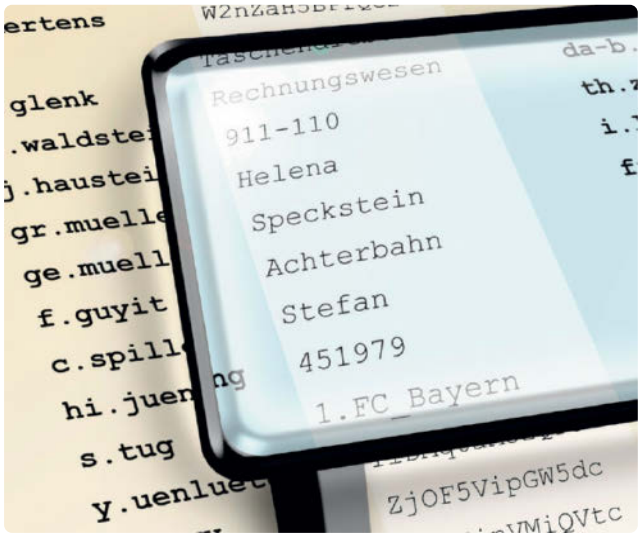
Bewusstseins- und wissensbildende *Informationen* über das konkret identifizierte Risiko an den Anwender in Echtzeit, evtl. mit elektronischer Willenserklärung für einen juristisch nachhaltigen Haftungsübergang; *Verschlüsselung* mit Unternehmensschlüssel oder persönlichem Schlüssel, je nachdem, ob der Anwender das Recht haben soll, diese Daten eigenständig, z.B. auf seinem privaten Rechner, zu nutzen (BYOD); revisionssichere *Beweiserhebung* und evtl. Alerting bei kritischen Aktionen; letztlich auch eine *Blockade*.

Bei der Wahl eines technischen Produktes ist es wesentlich, dass eigene algorithmische Prüfungen und solche von Drittprogrammen eingebunden werden können, sodass eine Sequenz von Prüfungen nach unterschiedlichen Kriterien entsteht. Mittelfristig sollte man die sensibelsten Daten in sicheren Datenräumen (Private Data Room) mit einfachen Richtlinien (Read up – No write down) sammeln und diese sicheren Datenräume nur über virtuelle Mechanismen einbinden.

Eine rein organisatorische Lösung ist nicht ausreichend, da der Mitarbeiter den Abfluss der Information oft gar nicht erkennen kann, z. B. wenn dieser durch Schadcode als Upload über den Browser stattfindet. Vielmehr muss zumindest ein Teil der Sicherheitsrichtlinie technisch umgesetzt werden. IT-Sicherheit gegen den Anwender durchzusetzen, ist sehr teuer oder gar unmöglich, deshalb sollten die Maßnahmen immer für die effiziente Abwicklung des Anwendungsfalls und damit für den Anwender – nicht gegen ihn – getroffen werden. Auch für das Umsetzen der Anforderungen aus den rechtlichen Auflagen, z. B. dem Datenschutz, hat sich ein software-gestütztes Risikomanagement bewährt. Die Ergebnisse der Überwachung der Leckage-Punkte bilden dann die Grundlage für das DLP-Risikomanagement und fließen in ein immer detaillierteres DLP-Konzept ein.

Verstöße vermeiden

Audit und revisionssichere Protokollierung bestimmter Aktivitäten dienen dazu, bestimmte Ereignisse für eine spätere Auswertung abzuspeichern, ohne dass diese Daten im Nachhinein modifiziert werden können. Die Audit-Funktionalität meldet in Echtzeit Sicherheitsvorfälle und ermöglicht so eine Alarmierung der Verantwortlichen und das Nachjustieren der technischen Richtlinien. Entsprechend der jeweiligen lokalen Gesetze sind die Log-Daten entweder völlig ohne Anwenderdaten zu erheben oder anonym bzw. pseudonymisiert zu speichern. Die Protokollierung von Risiken hat nichts mit der Überwachung von Anwendern zu tun, sondern eher mit dem Schutz der Anwender vor unsichtbaren Angriffen, die später so aussehen können, als wäre der Mitarbeiter selbst Innentäter.



Quelle: itWatch

Ausdrucke können sensible Daten enthalten.

Bei (unbewusst) versuchten Verstößen gegen die definierten Regeln bieten DLP-Tools ereignisabhängig abgestufte Reaktionsmöglichkeiten. Dazu gehören beispielsweise: die Anzeige eines *Hinweises* für den Benutzer, dass die geplante Transaktion gegen das Regelwerk verstoßen würde; die Abfrage einer expliziten *Zustimmung* des Benutzers, z. B. zur Protokollierung der Tätigkeiten; die *Freigabe* der Aktion unter bestimmten Auflagen; die Abfrage von *Gründen* für die Aktion; die *Blockade* der Aktion; die Protokollierung sowie die Freigabe durch *Dritte*, etwa einen Administrator oder Vorgesetzten.

DLP bei mobilen Daten

Das lokale Sammeln im Abfall wird bei Flash-Datenträgern noch kritischer, da diese den verwendeten Datenbereich nicht notwendigerweise wieder aufzeigen, sondern lebensverlängernde Maßnahmen durch versteckte Datenspeicher implementieren. Ein Verschlüsseln am Platz ist hier nicht möglich. Auf den ersten Blick genügt es, sensible Daten nur auf selbstverschlüsselnder Hardware zu speichern. Doch auch mit Datenträgern, die den gesamten zu speichernden Datenstrom verschlüsseln, löst man das DLP-Problem nur teilweise, denn der einfache und weit verbreitete Angriff mittels USB-Dumper oder erweiterten Werkzeugen bleibt hierbei wirksam. Bei der Verwendung eines vermeintlich sicheren Datenträgers auf einem jedoch unsicheren Fremdsystem kann der ganze Datenträger mittels PIN oder biometrischer Verfahren geöffnet werden.

Jede Anwendung auf dem Rechner kann alle Daten lesen, weil der Datenträger transparent entschlüsselt wird. So liest der USB-Dumper, weil er eine Anwendung auf dem Rechner ist, ohne Kenntnis des Nutzers alle Dateien aus und erhält diese im Klartext, denn der Datenträger ist ja geöffnet. Zudem wird gelegentlich übersehen, dass ein sicheres Löschen immer abhängig von der konkreten Bauart des Datenträgers ist und zudem in die Rechtestruktur eingebettet werden muss. Nicht zuletzt sind alle auf einem fremden System entstehenden temporären Dateien zu berücksichtigen, sodass diese nicht auf dem Fremdsystem verbleiben.

Dies alles sind Themenfelder, die man nicht dem Anwender überlassen kann, weil dieser sich ja auf sein Business und nicht das IT-Umfeld konzentrieren soll. Ein entsprechendes Sicherheitsprodukt muss daher automatisch temporäre Information auf dem Drittsystem löschen. Für das sichere Löschen auf mobilen Datenträgern gilt es, entsprechend der Eigenschaften des Datenträgers (Flash, magnetische oder optische Datenträger, Multiple Write oder WORM etc.) den richtigen Algorithmus auszuwählen, sodass zu schützenden Daten auch mit forensischen Werkzeugen nicht mehr rekonstruierbar sind. Bei „Write-Once-Read-Many"-Datenträgern (WORM) geht dies beispielsweise nur über den Hinweis, dass der Datenträger insgesamt einer physischen Zerstörung zugeführt werden muss – idealerweise informiert man in dieser Nachricht dann auch gleich über den Standort eines geeigneten Vernichtungsapparates oder liefert einen Link auf den vorgesehenen Vernichtungsprozess. Das sichere Formatieren vorhandener Datenträger (auch wiederbeschreibbarer optischer Medien) muss ebenfalls gewährleistet sein. Alle Verfahren sollten zudem internationalen Standards und Auflagen beziehungsweise den Empfehlungen des BSI folgen.

Auch wenn alle klassischen Schnittstellen gesichert sind, stellen Drucker häufig noch einen weiteren Leckage-Punkt dar. Ausdrucke las-

sen sich, wenn sie nicht geeignet kenntlich gemacht sind, einfach in andere Papiere oder Unterlagen integrieren und mitnehmen. Für die Sicherheitskontrolle am Ausgang ist es kaum möglich, die Kritikalität von Papieren einzuschätzen. Ohne fundierte Beweislage führt ein Vorfall schnell zu einem Generalverdacht auf alle Personen mit Leserecht und bringt dadurch unnötigen Unfrieden in die Organisation. Diese Sicherheitsherausforderung lässt sich nicht mit einem allgemeinen Druckverbot für bestimmte unternehmenskritische Dokumente lösen.

Eine adäquate Antwort darauf bietet nur ein Schutzkonzept, das die Sensitivität eines Dokuments in Echtzeit feststellt und entsprechend dem Schutzbedarf definiert, wer diese Information wann auf welchem Drucker wie ausdrucken darf und gegebenenfalls, welche Daten über die Umstände des Ausdrucks vom Anwender vor dem Ausdruck zu erfragen sind. Solche Informationen sollten dann auch auf dem Ausdruck mittels eines Wasserzeichens festgehalten und in einem revisionssicheren, elektronischen Archiv protokolliert werden. Die Angaben auf dem Dokument sind dabei notwendig, um den ermittelten Sensitivitätsgrad auch über den Medienbruch hinweg festzuhalten und in gedruckter Form dauerhaft mit der Information zu koppeln. Das Wasserzeichen kann maschinenlesbar oder lesbar für Menschen sein, je nachdem was bezweckt wird.

Sicherheitslösungen, die das Drucken sensitiver Daten kontrollieren, müssen naturgemäß alle Druckvorgänge überwachen und immer dort eingreifen, wo System oder Anwender die zu druckenden Informationen als kritisch einstufen. Für neu erstellte oder noch nicht klassifizierte Dokumente sollte unmittelbar eine Einstufung (ggf. durch den Anwender) erzwungen werden. Diese ermittelten oder in Echtzeit vom Anwender hinzugefügten Daten sollten zudem – zusammen mit dem vollständigen Inhalt des Ausdrucks jederzeit wiederherstellbar – revisionssicher abgelegt werden. Erst so ist dokumentiert, wer wann und warum welches Dokument mit welchem Inhalt in welcher Stückzahl und über welchen Drucker ausgegeben hat – und auch Auflagen der Langzeitarchivierung werden gleich mit erfüllt.

Fazit

Bei der richtigen Wahl des Vorgehensmodells und der eingesetzten Lösung(en) kann man auch bei dem komplexen Thema DLP Investitionsschutz, Skalierbarkeit, Zukunftsfähigkeit und Kosteneffizienz im Betrieb mit einem schnellen Projekterfolg kombinieren. Am besten natürlich technisch unterstützt mit einem Werkzeug, welches das Risikomanagement und die Schutzfunktionen in einem Produkt anbietet und dadurch die Lebenszyklen von Risiken und Daten vollständig abbildet. Wer seine sensibelsten Daten in sicheren Datenräumen segmentiert und zudem wirklich alle Leckage-Punkte und alle Stadien des Informations-Lifecycle berücksichtigt, besitzt ein ganzheitliches DLP-Konzept, und verhindert nachhaltig eine Gefährdung des Unternehmenskapitals, das in Form von gespeichertem Wissen und Informationen vorliegt.

Ramon Mörl,
Geschäftsführer itWatch GmbH

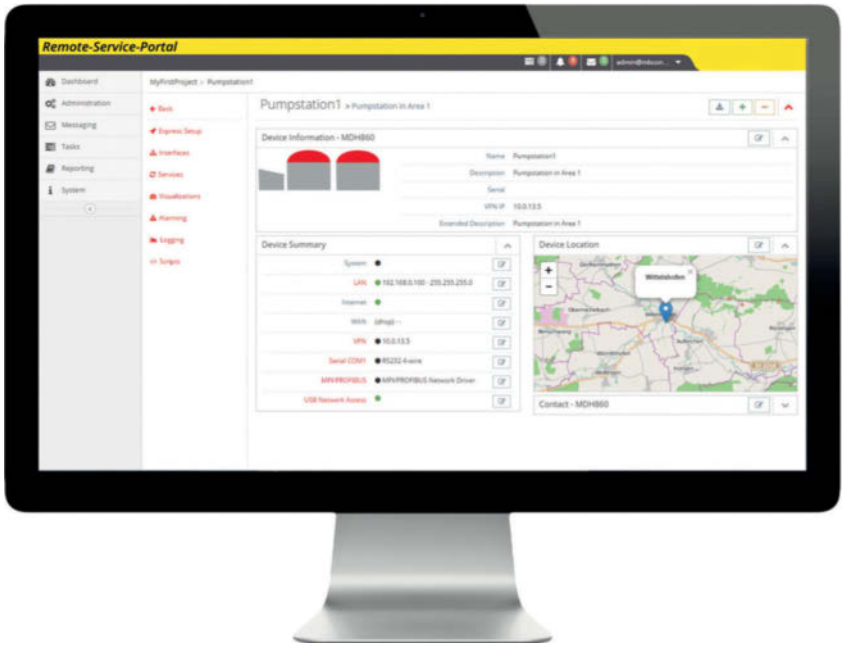
Sicherheit in der vernetzten Maschinenwelt

Industrial Security basiert auf der guten Zusammenarbeit von Anlagenbauern und -betreibern

Security war lange Zeit nur ein Thema für die klassische IT. Spätestens seit Stuxnet ist klar, dass auch Produktionsanlagen und Automatisierungssysteme gefährdet sind. Doch herkömmliche Security-Konzepte sind nicht ohne Weiteres mit der Automatisierungswelt kompatibel.

Die zunehmende Digitalisierung, gerade auch im Rahmen von Industrie 4.0, sorgt dafür, dass Informations- und Automatisierungstechnik immer mehr miteinander verschmelzen. Regelmäßige Meldungen über versuchte Denial-of-Service-Angriffe (DoS), gestohlene Kreditkartendaten oder manipulierte Finanztransaktionen treiben daher berechtigte Sorgenfalten auf die Stirn der Verantwortlichen.

Aus Sicht der Automatisierungstechnik sind die Vorteile und der Nutzen von Fernwartung und Zustandsüberwachung über das Internet unbestritten. Unabhängig davon, ob es sich um eine Anlagenstörung, um eine Umrüstung oder schlicht um eine Frage zur Bedienung handelt, das Servicepersonal des Maschinenbauers kann per Fernzugriff innerhalb von Minuten wertvolle Unterstützung anbieten. Was im Störungsfall eine tolle Sache ist, kann im Falle eines Missbrauchs allerdings zu großen Problemen führen. Verschafft sich jemand unberechtigt Zugang zu technischen Einrichtungen, einerlei ob Produktionsanlagen, Gebäudetechnik oder Infrastruktur, können Schäden in bedeutender Höhe entstehen – beispielsweise bei der Ausspähung von Rezeptur- und Produktionsdaten oder einer Manipulation der Anlage, die durch Übertemperatur oder mechanische Überlastung zu weitreichender Zerstörung führt.



Quelle: MB connect line GmbH

Alle Konfigurations- und Verwaltungsaufgaben werden über eine webbasierte Benutzeroberfläche erledigt (Abb. 1).

Unterschiedliche Anforderungen

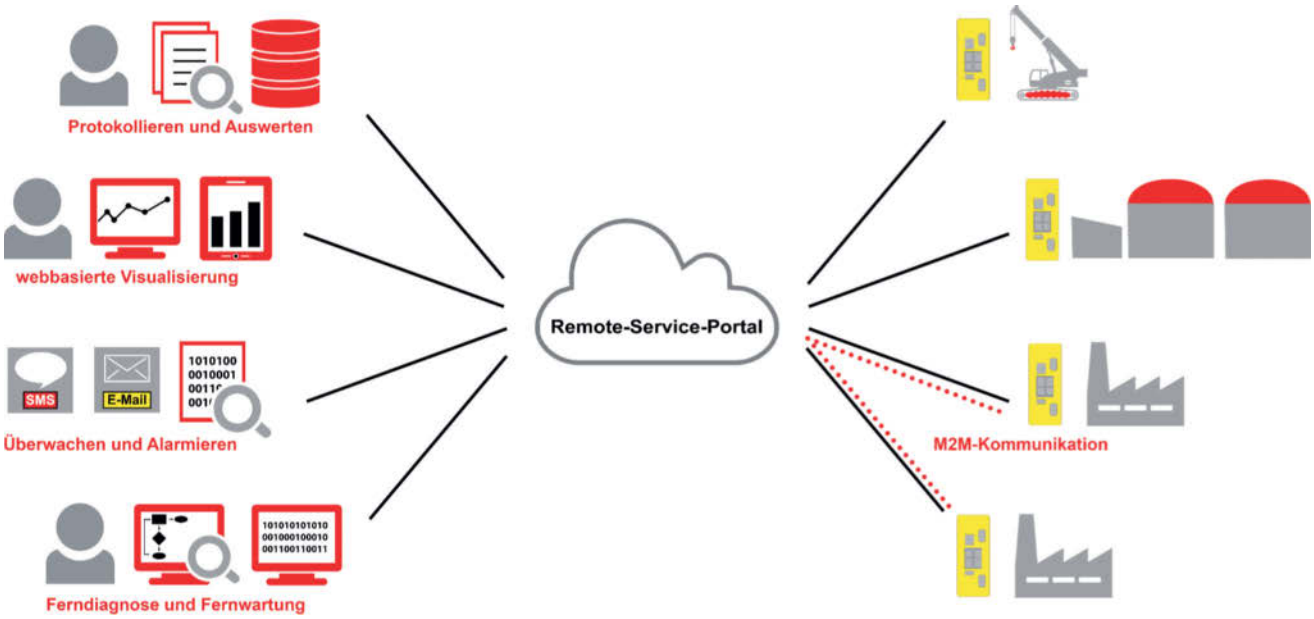
Die Themen Zugriffsschutz und Security fallen in der Regel in die Zuständigkeit der jeweiligen IT-Abteilungen. Dort sollte die Sicherheit an erster Stelle rangieren, letztlich also noch vor der Funktionalität und der Verfügbarkeit. Im Gegensatz dazu steht an einer Produktionsanlage die Verfügbarkeit über allem. Das lässt sich an einem einfachen Vergleich verdeutlichen: Eine Papiermaschine, in der das Papier mit fast 2000 m/s durch die Anlage läuft, muss innerhalb von Millisekunden auf Probleme reagieren können. An einem Büro-PC spielt es dagegen kaum eine Rolle, wenn der Benutzer einmal fünf Sekunden auf einen Virenscan warten muss.

Auch in einem weiteren Punkt unterscheiden sich IT und Automatisierungstechnik gravierend: Bestehende Steuerungen und andere Automatisierungskomponenten wie Umrichter oder Regler verfügen im Normalfall über keine eigenen Sicherheitsfunktionen. Wer auf ein solches Gerät Zugriff hat, kann dort Daten auslesen und einzelne Parameter oder ganze Programme ändern, ohne dass er sich authentifizieren muss und ohne dass dies protokolliert wird. Das hat u.a. historische Gründe: In den Anfangszeiten der Automatisierung funktionierte jede Steuerung wie eine autarke Insel, die Sicherheit nach außen war durch einen aufmerksamen Werkschutz garantiert.

Zentrale Service-Plattformen

Soll nun jedoch eine Vernetzung und Fernwartung stattfinden, ist eine Lösung gefordert, welche sowohl den Anforderungen der IT als auch der Automatisierungstechnik entspricht. Als nicht akzeptabel gelten Konzepte, bei denen

Quelle: MB connect line GmbH



Das Remote-Service-Portal ist eine universelle Lösung für die Datenerfassung, Fernwartung und M2M-Kommunikation (Abb. 2).

NICHT NUR KRITIS SIND SICHERHEITSKRITISCH

Die im Frühjahr 2016 beschlossene BSI-KRITIS-Verordnung soll Betreiber kritischer Infrastrukturen in die Lage versetzen, anhand definierter Kriterien zu prüfen, ob sie unter den Regelungsbereich des IT-Sicherheitsgesetzes fallen. Das Bundesinnenministerium hatte die Bundesländer, aber auch Verbände um eine Stellungnahme zum Entwurf gebeten. Die Reaktionen fielen überwiegend positiv aus. So schrieb zum Beispiel der DVGW (Deutscher Verein des Gas- und Wasserfaches e.V.), dass die „Vorschläge des Verordnungsgebers zur Ermittlung der kritischen Infrastrukturen im Sinne des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz-BSIG) zu begrüßen sind“, und machte verschiedene Anmerkungen zur weiteren Konkretisierung. Auch die Fachgremien von TeleTrusT Bundesverband IT-Sicherheit e.V. äußerten grundsätzliche Zustimmung, sahen aber gewissen Nachbesserungsbedarf.

Denn nach der Veröffentlichung des IT-Sicherheitsgesetzes machten Fragen wie „Sind wir eine kritische Infrastruktur?“ die Runde. Laut einer PwC-Umfrage sind sich 18 % der Unternehmen unsicher, ob sie dem Gesetz unterliegen. Dieser Prozentsatz scheint aber die Untergrenze zu sein, wenn man an die zahlreichen Fragen der Unternehmen in den letzten Monaten denkt.

Das BSI selbst definiert kritische Infrastrukturen (KRITIS) als: „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten.“ Zudem hat das BSI eine Tabelle zum IT-Sicherheitsgesetz veröffentlicht, in der Unternehmen nachsehen können, ob und wie sie von dem Gesetz betroffen sind. Abgesehen davon, dass die ebenfalls vom IT-Sicherheitsgesetz betroffenen Betreiber von Web-Angeboten, zum Beispiel Online-Shops, in der Tabelle nicht genannt werden, da sie nicht zu KRITIS gehören, darf eines nicht vergessen werden: Sicherheitskritisch sind nicht nur kritische Infrastrukturen.

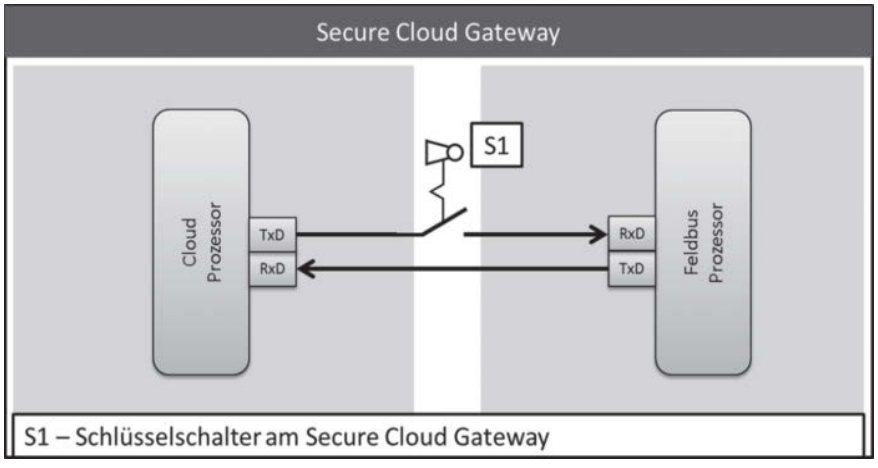
Für Online-Shops zum Beispiel gelten seit Inkrafttreten des IT-Sicherheitsgesetzes erhöhte Anforderungen an die technischen und organisatorischen Maßnahmen zum Schutz ihrer Kundendaten und der von ihnen genutzten IT-Systeme. Die Betreiber solcher Web-Angebote brauchen nicht auf die finale KRITIS-Verordnung zu warten, sondern müssen bereits seit mehreren Monaten aktiv geworden sein. Zudem darf man nicht vergessen, was zum Beispiel der Bundesverband der Deutschen Industrie (BDI) bereits vor Längerem betont hat: „Vermutlich werden die betroffenen Unternehmen die Sicherheitsanforderungen an ihre Zulieferer und Dienstleister weitergeben.“

Feststeht: IT-Sicherheit ist nur dann zu gewährleisten, wenn die Sicherheit aller IT-Systeme in einer Lieferkette oder in einem geschäftlichen Kunden-, Mitarbeiter- und Lieferantennetzwerk gewährleistet ist. Aus gutem Grund bezeichnet zum Beispiel die Studie „Threat Horizon 2016“ des Information Security Forums (ISF) die Sicherheitsmängel bei IT-Dienstleistern als bedeutendes IT-Sicherheitsrisiko. Die Erfahrung lehrt: Angreifer suchen sich das schwächste Glied in der Kette, das gilt auch und insbesondere für kritische Infrastrukturen. Aus diesem Grund muss jedes Unternehmen in der Liefer- oder Servicekette einer kritischen Infrastruktur die IT-Sicherheit deutlich ernster nehmen – ob sie nun in der KRITIS-Verordnung genannt werden oder nicht.

Oliver Schonschek
News Analyst, MittelstandsWiki

über das Internet von außen auf Maschinen oder Anlagen zugegriffen werden soll. Dieser Ansatz würde zu einem erheblichen technisch-administrativen Aufwand führen. Für jedes zusätzlich installierte Gerät müsste die Konfiguration der Firewall manuell angepasst werden. Neben dem Arbeitsaufwand muss auch das Sicherheitsrisiko betrachtet werden. Bei der manuellen Konfiguration der Firewall passiert schnell einmal ein Fehler, der die Schutzfunktion empfindlich beeinträchtigen kann.

In der Praxis haben sich Lösungen bewährt, die auf einer zentralen Remote-Service-Plattform basieren (Abbildung 1). Sowohl das Servicepersonal als auch die Maschinen und Anlagen sind mit dieser Remote-Service-Plattform verbunden. Der große Vorteil dabei ist, dass Verbindungen von innen nach außen ohne Änderungen an bereits vorhandenen Firewalls funktionieren. Eingehende Verbindungsanfragen an die Maschinen kommen prinzipbedingt nicht vor. Bei den Kunden bereits eingeführte Sicherheitsstrategien bleiben davon unberührt.



Quelle: MB connect line GmbH

Ein sicheres Cloud Gateway hat eine integrierte Hardware-Datendiode, die Kommunikation ausschließlich in eine Richtung zulässt (Abb. 3).

Die Übertragung der Daten sollte natürlich verschlüsselt erfolgen, beispielsweise über gesicherte VPN-Verbindungen. Als Verschlüsselungsprotokoll hat sich TSL (SSL) bewährt. Diese hohen Sicherheitsstandards ermöglichen einen Einsatz auch in geschäftskritischen Anwendungen.

Rollenbasierte Rechteverwaltung

Die zentrale Plattform hat auch den Vorteil, dass der Anlagenbetreiber weder dem externen Servicepersonal noch den eigenen Mitarbeiten einen direkten Zugriff auf das Produktionsnetzwerk erlauben muss. Direkten Zugriff auf alle Maschinen hat nur die Plattform, die eine rollenbasierte Rechteverwaltung für alle Beteiligten bietet. Sie erlaubt eine feine Abstufung der Rechte der einzelnen Benutzer – bis hin zur Beschränkung der Zugriffsrechte auf einzelne Ports oder Protokolle. Damit sind verschiedene Sichtweisen auf die Maschinen und Anlagen möglich. Den Produktionsleiter interessieren beispielsweise nur die wesentlichen Zahlen einer Anlage, während für den Bediener wichtig ist, ob die Anlage richtig läuft und alle Parameter im grünen Bereich sind. Für das Servicepersonal wiederum sind Produktionsdaten und Rezepturen tabu, sie können jedoch eingreifen, wenn Anlagenparameter oder SPS-Programme angepasst werden müssen (Abbildung 2).

Cloud oder nicht?

Ist der Zugriff auf die Daten geregelt, stellt sich noch die Frage nach Art und Ort der Datenspeicherung. Seit Snowden und der NSA-Affäre überlegt man genau, wem man seine Daten anvertraut: Wo steht der Server? Wie ist dieser gesichert? Welche nationalen Gesetze gelten am Serverstandort? Zu empfehlen ist allemal eine Lösung, die auf der Serverinfrastruktur des Anwenders betrieben wird, beispielsweise auf Basis einer gängigen Virtualisierungstechnik. Kein Tunnelendpunkt befindet sich damit außerhalb des eigenen Hoheitsgebiets. Und auch weitere Vorteile einer virtualisierten Umgebung wie Skalierbarkeit, Verfügbarkeit, Performance, Datensicherung und schnelle Wiederherstellung sind nutzbar. Über verschiedene Lizenzmodelle kann die Leistungsfähigkeit der Plattform mit den Kundenanforderungen wachsen. Und dank regelmäßiger Sicherheitsupdates des Herstellers ist die Kundenplattform stets auf dem aktuellen Stand. Die Antwort auf die Frage, ob Cloud oder nicht, lautet deshalb: Ja zur Cloud, aber innerhalb der eigenen Infrastruktur.

Sichere Feldbusanbindung

Als viele der heute eingesetzten Geräte und Feldbusse entwickelt wurden, waren IoT, Industrie 4.0 und Big Data noch unbekannt. Diesen Systemen fehlen daher jegliche Sicherheitsmerkmale für eine direkte Vernetzung, wie Zugangsschutz mit Passwort oder signierte Firmwareupdates. Um Bestandsanlagen Industrie-4.0-tauglich zu machen, eignen sich Gateways, die hardwaretechnisch die Kommunikation nur in eine Richtung zulassen, vom Feld ins sichere Netz. Es sollte technisch unmöglich sein, sich von außen mit der Anlage zu verbinden, um Daten zu stehlen oder zu manipulieren. Erreicht wird das, indem der Rückkanal elektrisch getrennt ist und nur per Schlüsselschalter zu Konfigurationszwecken aktiviert werden kann (Abbildung 3). Durch die echte hardwarebasierte Trennung sind auch übliche Schwachstellen der Security-Hardware ausgeschlossen: fehlerhafte Konfiguration durch den Anwender oder Sicherheitslücken in der Gerätesoftware.

Industrielle Sicherheit umfasst nicht nur den gefährdungs- und unfallfreien Betrieb von Maschinen und Anlagen, sondern auch den Schutz von Know-how und die Sicherstellung der Systemintegrität. Das beginnt mit einer Segmentierung der Netzwerke in einzelne Automatisierungszellen und setzt sich darin fort, die Datenzugriffe nur einem begrenzten Teilnehmerkreis zugänglich zu machen. Was oft unterschätzt wird, ist die Bedrohung von innen. Etwa dadurch, dass Mitarbeiter Daten von kompromittierten Internet-Seiten oder E-Mails herunterladen oder Schadsoftware über USB-Sticks einschleusen.

Awareness und Wissensaustausch

Industrial Security ist also keine rein technische Angelegenheit. Auch organisatorische Gesichtspunkte und der Faktor Mensch spielen eine wichtige Rolle. Allgemein bekannte Abteilungspasswörter gehören ebenso der Vergangenheit an wie kleine Haftnotizen, auf denen die Passwörter gewissermaßen öffentlich ausgehängt werden. Die Anforderungen an Qualifikationen und Ausbildung der Mitarbeiter müssen also steigen. Während im Produktionsumfeld und in der Automatisierungstechnik grundlegende Kenntnisse in Sachen Security erforderlich sind, sollten sich Verantwortliche der IT-Sicherheit auch mit den Anforderungen der Produktionstechnik befassen. Und nicht zuletzt muss dem Management klar sein, dass es Sicherheit nicht zum Nulltarif gibt.

Siegfried Müller,
Geschäftsführer MB connect line GmbH

Smartphones als Risikofaktor

Bei der Einführung von Mobilgeräten im Unternehmen gilt es, vorab wichtige Kernfragen zu klären

Mobile Geräte beinhalten immer mehr sensible Informationen, sei es aus dem beruflichen oder dem privaten Bereich. Diese Daten müssen sowohl während des Betriebs vor unbefugtem Zugriff geschützt werden als auch bei einem möglichen Verlust des Geräts sicher gespeichert sein.

Gerade durch die ständige Verfügbarkeit mobiler Endgeräte neigen Nutzer dazu, sichere und unsichere Anwendungen auf der gleichen Plattform zu betreiben. Zudem sind Mobile Devices viel eher gefährdet, gestohlen oder verloren zu werden. Aus diesem Grund ist es wichtiger denn je, die gespeicherten und verarbeiteten Daten zu schützen.

Sicherheitslücken by Design

Während das Risiko, das Gerät zu verlieren, auch bei Laptops eher gering ist, ist dies bei Smartphones sehr wohl gegeben. Dazu kommt häufig ein sorgloser Umgang mit dem Gerät, was insbesondere durch die Installation von beliebigen Apps eine Gefährdung der gespeicherten Informationen darstellt. Und im Gegensatz zu stationären Geräten gehen Smartphones selten im ausgeschalteten Zustand verloren. Ein Schutz, der beispielsweise nur auf den Bootvorgang abzielt, kann hier also nur begrenzte Sicherheit bieten.

Ein häufig unterschätztes Risiko stellen insbesondere die Sensoren eines Smartphones dar. Am Beispiel GPS lässt sich dies einfach verdeutlichen: Mit den gesammelten Daten kann problemlos ein Bewegungsprofil erstellt werden. Die Koordinaten können auch implizit beim Teilen von Bildern als zusätzliche Meta-Informationen oder beim Absetzen von Social-Media-Nachrichten verbreitet werden. Je nach Aufgabe des Mitarbeiters sind das Profil und der aktuelle Standort nicht nur für ihn selbst schützenswert, sondern auch für das Unternehmen. So könnten sich darüber Informationen zu Vertragsverhandlungen oder Meetings ablesen lassen. Dem gegenüber steht jedoch häufig das Bedürfnis des Anwenders, die Standortinformationen zu nutzen, beispielsweise zur Navigation. Hier gilt es für das Unternehmen, eine Risikoabwägung zu treffen. Neben einer technischen Kontrolle ist auch eine organisatorische Vorgabe denkbar.

Generell sind bei der Einführung mobiler Endgeräte mit Zugriff auf die firmeneigene Infrastruktur eine Reihe von Anforderungen zu beachten. Hierbei hilft jedoch kein allgemeingültiges Regelwerk von der Stange – eine individuelle Betrachtung und Bewertung des Einsatzumfeldes und der den Nutzern eingeräumten Freiheiten ist entscheidend. Dennoch gibt es drei Kernthemen, die vor dem Beginn eines Deployments untersucht werden sollten: die Separation der Arbeitsbereiche, die Verwaltung der Geräte sowie die Sicherung des Zugriffs auf das eigene Netzwerk.

Getrennte Arbeitsbereiche

Bei betrieblich bereitgestellten und exklusiv für dienstliche Zwecke genutzten Geräten ist der Umgang mit den verarbeiteten Daten meist klar geregelt. Bei Smartphones besteht jedoch aufgrund der Tatsache, dass sie ständig mitgeführt werden, oftmals der Wunsch nach einem Mischbetrieb aus privater und dienstlicher Nutzung. Für solche Fälle ist – unabhängig davon, ob der Mitarbeiter sein eigenes Gerät dienstlich (Bring Your Own Device; BYOD) oder ein dienstlich bereitgestelltes Smartphone auch privat (Corporate Owned Personally Enabled; COPE) einsetzt – eine strikte Trennung der Arbeitsbereiche unabdingbar. Hierfür stehen zwar bei der App-Entwicklung bereits Möglichkeiten bereit, etwa ein Verhindern der Erstellung von Bildschirmfotos und der Nutzung der Zwischenablage. Dies setzt jedoch voraus, dass betriebliche Daten ausschließlich in speziell dafür entwickelten Apps verarbeitet werden. Bei Standardfunktionalitäten wie dem E-Mail-Versand oder dem Zugriff auf berufliche Kontakte ist das aber nicht wirklich zielführend.

Im Wesentlichen gibt es zwei Optionen für die Separation von Arbeitsbereichen im mobilen Bereich. Der erste Ansatz ist eine Trennung auf Rechteebene. Ein prominentes Beispiel dafür ist Android for Work. Hier werden, aufbauend auf bereits auf Hardware-Ebene vorhandenen Mechanismen wie der ARM TrustZone, zwei verschiedene Benutzerprofile zur gleichen Zeit ausgeführt. Für den Anwender ist dieser Ansatz nicht invasiv, denn es ist nicht zwangsweise ein separates Login für den Zugriff auf die Firmendaten notwendig. Betriebliche Apps erhalten ein spezielles Icon und sind so leicht von anderen Apps zu unterscheiden. Sie lassen sich jedoch vollständig durch die firmeneigene IT verwalten, inklusive einer Fernlöschung aller Daten.

Ein zweiter Ansatz, der nicht direkt im Betriebssystem verankert ist, ist der Einsatz einer Container-App. Die zu schützenden Daten werden verschlüsselt in dieser App gespeichert, der Nutzer öffnet den Container bei Bedarf und entschlüsselt damit die Daten. Dies geschieht zur Laufzeit, sodass auf ruhende Daten nicht zugegriffen werden kann. Aus Unternehmenssicht bietet diese zweistufige Authentifizierung einen zusätzlichen Schutz. Nachteil aus Nutzersicht ist hier jedoch, dass eine der Anmeldung am Gerät nachgelagerte Authentifizierung notwendig ist.

Bei der Festlegung der Policies sollte man darüber hinaus auch über verschiedene Profile für verschiedene Anwendungsfälle und Einsatzgebiete nachdenken. Müssen z. B. vom Mitarbeiter unterwegs Daten gesammelt und geschäftliche Dokumente angepasst werden, ist der Schutzbedarf des mobilen Gerätes wohl höher einzustufen als im Falle eines Mitarbeiters, der ausschließlich Mails und Termine verwaltet.

Enterprise Mobility Management

Egal, ob rein dienstlich oder mit privater Nutzung – die zentrale Verwaltung der Endgeräte ist ein Muss. Sowohl bei der Durchsetzung der eigenen Richtlinien als auch bei der (teilweisen) Fernlöschung im Falle eines Verlustes ist ein solcher Mechanismus unabdingbar.

Hierfür kommt meist eine Auswahl oder Kombination von drei Komponenten infrage.

Während das Mobile Device Management (MDM) die Verwaltung der Profile und Berechtigungen auf dem Gerät selbst übernimmt, verwaltet ein Mobile Application Management (MAM) die auf dem Gerät verwendeten und zugelassenen Apps. Ein Mobile Information Management (MIM) kümmert sich um die auf dem Gerät verarbeiteten und gespeicherten Daten. Zusammengefasst spricht man häufig von einem Enterprise Mobility Management (EMM). Die Verwaltung eines Gerätes sollte immer eine Konfiguration der Sensoren und Schnittstellen umfassen, zugelassene Verbindungen festlegen und eine Passwort-Policy für die Bildschirmsperre beinhalten.

Ein weiterer zentraler Punkt bei der Einführung eines EMM ist der Enrolment-Prozess der Geräte. Diese können vorpersonalisiert an die Nutzer ausgehändigt werden. Bei einer hohen Anzahl von auszugebenden Geräten erfordert diese Aufgabe allerdings einen immensen Ressourceneinsatz, sodass sie in solchen Fällen an den Nutzer delegiert werden sollte. Diesem können mit seinem Gerät Registrierungsdaten übermittelt werden, mit denen er sein Gerät am Managementserver anmelden kann, wo er dann ein für ihn vorbereitetes Profil erhält.

Netzwerkzugriff

Neben der Datenhaltung und -verarbeitung auf den Mobilgeräten muss auch der Transportweg vom und in das Firmennetzwerk gesichert werden. Hierfür eignen sich klassische Maßnahmen wie VPN und Client-Zertifikate. Für beide Varianten bieten alle gängigen Betriebssysteme Unterstützung.

Auch hier sind wiederum verschiedene Ansätze denkbar. Eine Option ist, den kompletten Datenverkehr des Gerätes, inkl. sämtlicher Internetzugriffe, über die Infrastruktur zu leiten. Diese Variante erlaubt die Filterung der Inhalte wie auf stationären Geräten. Allerdings belasten in diesem Szenario auch sämtliche Softwareupdates und andere großen Datenübertragungen, möglicherweise parallel, die Infrastruktur. Alternativ kann der geschützte Bereich so konfiguriert werden, dass nur Anwendungen, die hier abgelegt sind, auf das interne Netz zugreifen können. Dadurch bleiben Verbindungen aus dem privaten Bereich des Gerätes unberührt. Dies ist mit beiden genannten Separierungsmechanismen möglich, in der App-Container-Variante jedoch mit einem Overhead in Form einer höheren Anzahl an Verbindungen. Dafür lässt sich gezielter steuern, welche Anwendung mit welchen Systemen der eigenen Infrastruktur kommunizieren darf.

Bei der Konstruktion der Netzwerkinfrastruktur und der Anbindung der mobilen Geräte ist auf die Positionierung des MDM-Servers besonderes Augenmerk zu legen. Ist der Server für die Geräte nur aus dem internen Netz und über VPN erreichbar, muss eine entsprechende Verbindung vor dem Enrolment hergestellt werden. Dies kann beispielsweise durch einen Administrator in Form einer Vorinitialisierung vor der Übergabe an den Nutzer sichergestellt werden. Alternativ können hier auch organisatorische Prozesse zum Einsatz kommen, die ein Enrolment nur unter der Nutzung eines eigenen WLAN-Netzwerkes oder APNs zulassen.

Zudem ist sicherzustellen, dass kein Abfluss von sensiblen Daten stattfindet. Häufig erfolgt beispielsweise ein automatisiertes Backup der auf dem Gerät gespeicherten Daten in die Cloud, ohne dass sich die Nutzer der möglichen Auswirkungen bewusst sind. Besonders bei der Verarbeitung personenbezogener Kundendaten auf mobilen Endgeräten kann ein solcher Synchronisationsmechanismus auch juristische Konsequenzen nach sich ziehen.

Analysieren und handeln

Unabhängig davon, ob ein Unternehmen BYOD zulässt oder doch lieber auf COPE setzt: Sicher ist, dass zumindest in der Anfangsphase die Organisation der mobilen Datenverarbeitung komplexer wird. Bei allen Überlegungen ist zu berücksichtigen, welchen Wert die Daten haben, die auf dem Gerät gespeichert sind, und wie schnell der Verlust eines Gerätes bemerkt wird. Falls beispielsweise nur ein Remote-Zugriff auf Daten besteht und keinerlei Information auf dem Gerät nach der Nutzung verbleiben, könnte eine schnelle Sperrung des Zugriffs dieses Gerätes den potenziellen Schaden sehr gering halten.

Die Vielzahl an Möglichkeiten und Einschränkungen führt dazu, dass ein Unternehmen in jedem Fall eine Risikoanalyse durchführen muss, damit das für ihren Anwendungsfall angemessene Sicherheitsniveau bestimmt werden kann. Die Kernthemen der Umsetzung und die damit verbundenen Fragestellungen bleiben allerdings, unabhängig von den Ergebnissen der Analyse, im Wesentlichen identisch. IT-Verantwortliche sollten bei ihren Überlegungen keinen der Bereiche außer Acht lassen.

Dr. Jörn-Marc Schmidt und Lukasz Kubik,
secunet Security Networks AG

Sichere E-Mails für alle

Eine Technische Richtlinie fördert den Datenschutz im E-Mail-Verkehr

Trotz wachsender Konkurrenz durch alternative Kommunikationstechniken ist die E-Mail nach wie vor eines der am häufigsten genutzten Verfahren im privaten, geschäftlichen und behördlichen Bereich. Die konsequente Anwendung von IT-Sicherheitsmechanismen spielt dabei oft aber nur eine nachgeordnete Rolle.

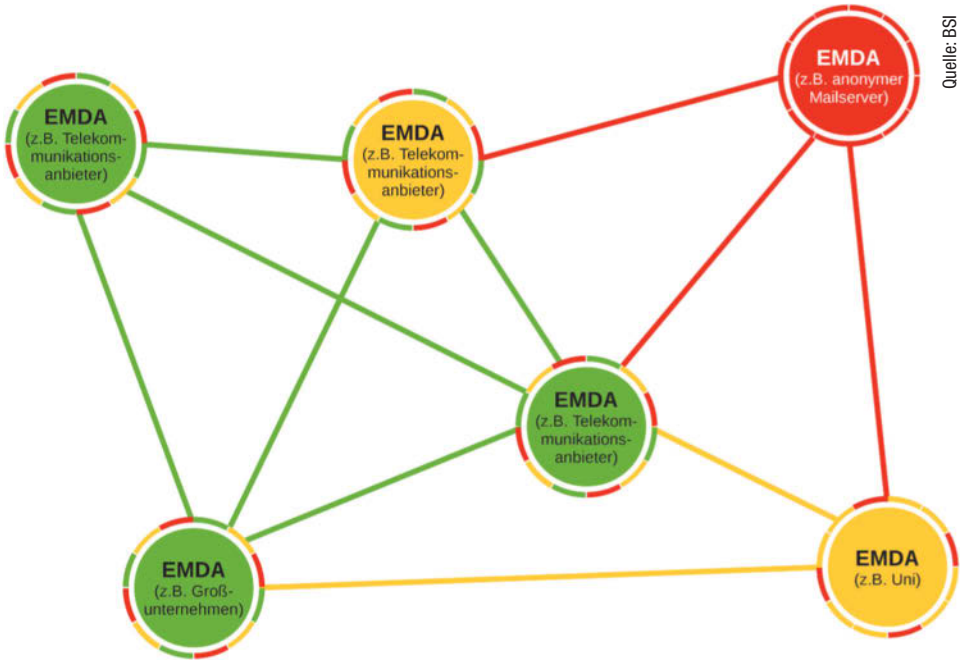
Im Fokus von E-Mail-Nutzern wie auch -Diensteanbietern steht in erster Linie der schnelle und unkomplizierte Versand einer Information vom Sender zum Empfänger. Mehr und mehr zeigt sich aber, dass die Nutzer durchaus ein unverkennbares Interesse an Sicherheits- und Datenschutzaspekten demonstrieren, etwa wenn sie sich bewusst für E-Mail-Diensteanbieter entscheiden, die ihren Server-Standort in Deutschland haben und mit einem hohen Maß an IT-Sicherheit werben. Zusätzliche Maßnahmen zur Erhöhung der IT-Sicherheit auf Nutzerebene, wie z. B. die Ende-zu-Ende-Verschlüsselung, fristen hingegen ein Nischendasein und werden häufig als zu kompliziert empfunden.

Neue Richtlinie nach bewährten Mustern

Die „Technische Richtlinie 03108 Secure E-Mail-Transport“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) berücksichtigt dies, indem ausschließlich IT-Sicherheitsmaßnahmen gefordert werden, die ohne das Zutun oder eine fachliche Expertise des Nutzers vom E-Mail-Diensteanbieter umgesetzt werden können. Darüber hinaus wurde keine neue in sich geschlossene Infrastruktur geschaffen, sondern die besonderen Eigenschaften der weltweiten E-Mail-Kommunikation berücksichtigt. Diese findet heterogen statt: Es gibt sowohl E-Mails, die Ende-zu-Ende verschlüsselt oder zwischen allen Knotenpunkten transportverschlüsselt sind, als auch solche, die als frei lesbarer Text übermittelt werden. Und beide Arten von E-Mails landen letztlich in den gleichen Postfächern (Abbildung 1).

Mit der neuen Technischen Richtlinie TR-03108 wird nun das Ziel verfolgt, durch die Definition eines einheitlichen Sicherheitsniveaus für E-Mail-Dienste, das auch bereits etablierte internationale Standards berücksichtigt, auf eine geschützte Aufbewahrung und Übertragung von E-Mails hinzuwirken. Dadurch soll zumindest ein Teil unserer digitalen Kommunikation insgesamt sicherer gemacht werden.

Um dies zu erreichen, setzt das BSI auf einen modularen Katalog von IT-Sicherheitsanforderungen, der durch übergreifende Anforderungen, wie ein taugliches Sicherheitskonzept und die Einhaltung des Datenschutzes, flankiert wird. Es werden sowohl der Betrieb als auch die einzelnen Schnittstellen des E-Mail-Dienstes adressiert. Hinsichtlich der Sicherheitsanforderungen wurde auf bereits in der Praxis erprobte nationale und internationale Standards zurückgegriffen. Neben der Verwendung sicherer Kryptografie (BSI TR-03116-4) zählen gesicherte DNS-Abfragen (DNSSEC), obligatorische Verschlüsselung (DANE/TLSA) und die Verwendung vertrauenswürdiger Zertifikate (BSI TR-03145) zur Palette der Leistungsmerkmale. Die Anforderungen wurden so gestaltet, dass sie vom E-Mail-Diensteanbieter auch schrittweise umgesetzt werden können und jeweils schon für sich genommen zu einer Erhöhung der IT-Sicherheit beitragen (Abbildung 2).



Quelle: BSI

Heterogene E-Mail-Kommunikation: Ende-zu-Ende-verschlüsselte, transportverschlüsselte und offene E-Mails nutzen die gleichen Infrastrukturen (Abb. 1).

Standardisierte Technologien

Eine von der Technischen Richtlinie geforderte Schlüsseltechnologie ist die DNS-Based Authentication of Named Entities (DANE). Diese relativ junge Technologie ermöglicht es Internet-Diensten, ihre für die Authentisierung und Verschlüsselung notwendigen Schlüssel oder Schlüsselinformationen durch die Veröffentlichung auf DNS-Servern bekannt zu geben. Auf diese Weise kann jeder authentisiert und ver-

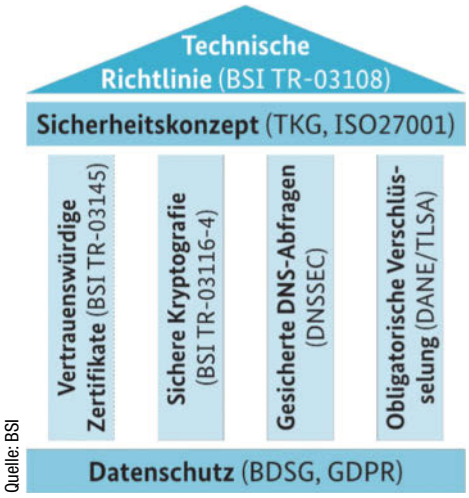
schlüsselt mit einem E-Mail-Dienst kommunizieren. Tatsächlich geht DANE an dieser Stelle sogar noch einen Schritt weiter, denn die Nutzung von DANE ist gleichzeitig ein Statement dafür, dass der E-Mail-Dienst standardmäßig in der Lage ist, eine verschlüsselte Verbindung anzubieten, und dass ungesicherte Verbindungen eher unerwünscht sind. Damit ist DANE eine Technologie, die obligatorisch sichere Verbindungen skalierbar in die Fläche bringt.

Internet-Verbindungen, die mit Hilfe von Transport Layer Security (TLS) abgesichert werden, finden im Gegensatz zu DANE schon seit längerer Zeit in der Praxis zunehmende Verbreitung. Sicherheitsschwächen wie BEAST oder Poodle haben in der Vergangenheit aber gezeigt, dass hierbei vor allem der Einsatz zeitgemäßer und geprüfter Kryptoverfahren von essenzieller Bedeutung ist. Das BSI veröffentlicht aus diesem Grund jährlich und anlassbezogen entsprechende Empfehlungen, die auch in der Technischen Richtlinie TR-03108 Anwendung finden. Durch die Kombination von DNSSEC zur sicheren Abfrage beim DNS-Server, DANE zum Abruf von Schlüsseln oder Schlüsselinformationen und dem Einsatz von sicheren Algorithmen bei TLS wird mithilfe von Standardtechnologien ein einheitlich hohes Sicherheitsniveau erreicht.

Die Auswahl der IT-Sicherheitsanforderungen fand bereits für die Erstellung der ersten Version der Technischen Richtlinie gemeinsam mit E-Mail-Diensteanbietern in einer eigens zu diesem Zweck vom BSI gegründeten Arbeitsgruppe statt. Auch in Zukunft wird in dieser Arbeitsgruppe über die Fortentwicklung der TR-03108 diskutiert. Die Berücksichtigung neuer, in der Praxis etablierter Technologien ist also durchaus vorstellbar.

Einfache Zertifizierung

Wie alle Technischen Richtlinien des BSI hat auch die TR-03108 lediglich Empfehlungscharakter. Sie enthält Kriterien und Methoden zur Konformitätsprüfung, um die eigenen IT-Systeme besser abzusichern. Derzeit befindet sich im BSI jedoch auch ein Zertifizierungsverfahren im Aufbau. Dieses soll es den E-Mail-Diensteanbietern ermöglichen, die Einhaltung der Anforderungen der Technischen Richtlinie auch gegenüber Dritten nachzuweisen. Auf diese Weise entsteht vor allem für Nutzer der E-Mail-Dienste eine höhere Transparenz. Das Zertifizierungsverfahren kann, da die Schnittstellenprüfungen lediglich die ohnehin vom E-Mail-Dienst angebotenen Schnittstellen betreffen, nahezu vollständig remote durchgeführt werden. Die einzelnen Prüffälle, welche in der Prüfspezifikation zur TR-03108 veröffentlicht sind, erfolgen störungsfrei im Wirkbetrieb.



Quelle: BSI

Konzeptionelle Übersicht der Anforderungen der Technischen Richtlinie 03108 Secure E-Mail-Transport (Abb. 2).

Ausblick

Allen anders lautenden Voraussagen zum Trotz bleibt die E-Mail wohl auch in Zukunft eine wichtige Kommunikationstechnik, sowohl im privaten wie auch im geschäftlichen und behördlichen Bereich. Da über dieses Verfahren aber auch besonders schützenswerte Daten transportiert werden, muss der E-Mail-Verkehr den Sicherheitsanforderungen, die auch für andere Formen des Datenaustausches gelten, wirksam angepasst werden.

Die Technische Richtlinie TR-03108 wurde schon früh mit den internationalen Partnerbehörden des BSI abgestimmt und kann sich seit der Veröffentlichung des Entwurfs vor einem Jahr eines steigenden Interesses erfreuen. Geplant ist, in Zukunft die Akzeptanz international noch weiter zu fördern und national, neben den E-Mail-Diensteanbietern, auch solche Stellen für die TR-03108 zu gewinnen, bei denen der E-Mail-Dienst nicht zum Kerngeschäft, dennoch aber zum Tagesgeschäft gehört (z. B. Versicherungen, Großunternehmen, Behörden und öffentliche Einrichtungen). Somit hat die Technische Richtlinie das Potenzial, die Sicherheit der digitalen Kommunikation via E-Mail Schritt für Schritt national und international deutlich zu erhöhen.

Florian Bierhoff,
Referat S11, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Besser ausdrücklich vorgesorgt

Bei den Policen für IT-Schadensfälle ist es oft ratsam, genau nachzufragen

Das Risiko, Opfer eines Cyberangriffs zu werden, ist zuletzt stark gestiegen. Datendiebstahl, Betriebsunterbrechungen oder Erpressungen können zu Verlusten in Millionenhöhe führen. Welche Leistungen bieten Cyberversicherungen, wer kann sich versichern und was sollte man vor Abschluss unbedingt wissen?

Cyberkriminelle entwenden vertrauliche Daten, schleusen Schadsoftware in Netzwerke ein oder legen ganze Produktionsanlagen lahm. Wie schwer die Folgen bei den Betroffenen unter Umständen sind, konnte man an Beispielen wie dem Sony Playstation Network, dem Deutschen Bundestag oder dem zerstörten Hochofen sehen, dessen Fall das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem „Bericht zur Lage der IT-Sicherheit in Deutschland 2014“ dokumentiert hat. Und auch mittelbare Schäden wie der Missbrauch des eigenen Firmennamens für Betrugsmaschen können ein Unternehmen teuer zu stehen kommen.

Risikolandschaft Deutschland

Gemessen an der Wirtschaftsleistung sind diese Schäden nirgends so hoch wie in Deutschland. Das geht aus einer weltweiten Untersuchung des Centers for Strategic and International Studies hervor. Das bestätigt auch die E-Crime-Studie 2015 der Wirtschaftsprüfungsgesellschaft KPMG: 40 % der befragten Unternehmen waren in den letzten zwei Jahren von Cyberkriminalität bzw. E-Crime betroffen – Tendenz steigend. Das Risiko, dass deutsche Unternehmen zum Opfer werden, schätzen 98 % der Studienteilnehmer als hoch oder sehr hoch ein. Den Gesamtschaden durch E-Crime in den vergangenen zwei Jahren veranschlagt die KPMG mit circa 54 Milliarden Euro. Die bittere Erkenntnis: Ein vollständiger Schutz vor Cyberangriffen ist für technologieabhängige Unternehmen nicht erreichbar.

Dennoch, so schätzen die Versicherer, sichern sich lediglich bis zu 10 % der deutschen Unternehmen gegen das Risiko eines Cyberangriffs mit einer entsprechenden Versicherung ab. Wie sind diese Zahlen zu interpretieren? Eine Erklärung könnte sein, dass das Thema Cyberrisiken bei deutschen Unternehmenslenkern noch nicht vollständig angekommen ist. Immerhin hat ein Viertel der deutschen CEOs noch nie an einer Sitzung mit Führungskräften oder Vorstandskollegen zum Thema Cyber Security teilgenommen. Das ist im weltweiten Vergleich der höchste Wert (Durchschnitt: 5 %).

Die Frage ist: Kennen die Unternehmensführungen die Möglichkeiten von Cyberversicherungen? Eventuell fehlt der Dialog, um die Potenziale einer Versicherung auf die eigenen Cyberrisiken übertragen zu können – vorausgesetzt, diese sind im Unternehmen überhaupt bekannt. Vielleicht sehen Unternehmen auch die kumulierten Schadenssummen als viel zu hoch an, als dass diese kaufmännisch sinnvoll versichert werden könnten. Zumindest Konzerne kommen im Gespräch mit den Versicherern in Einzelfällen zu diesem Schluss.

Eine durchschnittliche Gesamtschadenssumme von circa 370 000 Euro mit Ermittlungs- und Folgekosten von rund 70 000 Euro über verschiedene Deliktstypen hinweg spricht allerdings für ein breites Spektrum kaufmännisch sinnvoll versicherbarer Schäden – insbesondere wenn man berücksichtigt, dass einige Deliktstypen 50 Mal und häufiger innerhalb von zwei Jahren auftreten, wie die E-Crime-Studie belegt.

Versicherungen nach IT-Abhängigkeit

Im Gegensatz zu anderen Versicherungsprodukten unterscheiden sich Cyberversicherungen vor allen Dingen in ihrem ganzheitlichen, spartenübergreifenden und sachschadenunabhängigen Ansatz. So werden sowohl Eigen- als auch Drittschäden (Haftpflichtkomponente) mitversichert. Ebenso wenig spielt die Herkunft des Täters (unternehmensintern oder -extern) eine Rolle. Zudem bieten Cyberversicherungen die Möglichkeit, sich zusätzliche Expertenunterstützung durch IT-Forensik-Sachverständige oder Kommunikationsmanager einzukaufen.

Trotzdem sind sich die meisten Versicherungsunternehmen einig, dass Unternehmen ihre bisherigen Versicherungspolicen beibehalten sollten. Sie begründen es damit, dass die Cyberversicherung lediglich eine Erweiterung des Versicherungsschutzes als Reaktion auf eine wachsende Bedrohungslage ist und ihn nicht ersetzt. Dennoch empfehlen einige Versicherer ein Überprüfen und gegebenenfalls Anpassen des Versicherungsportfolios gegen Beitragsminderungen von anderen Policen. Hierbei ist zu beachten, dass die Cyberpolice zumeist vorrangige Deckung vor anderen Versicherungen hat. Oft sind die tatsächlichen Überschneidungen aber geringer als allgemein angenommen.

Das Abschließen einer Cyberpolice lohnt sich nach Ansicht der Versicherer grundsätzlich für jedes Unternehmen. Am meisten profitieren Industrieunternehmen, Dienstleister oder Firmen IT-naher Branchen, deren Umsätze stark von Informationstechnik abhängen.

Eine Branche im Aufwind

Seit 2011, als die erste Cyberversicherungspolice auf den deutschen Markt kam, haben solche Angebote kontinuierlich zugenommen. Mittlerweile bieten etliche Versicherer Cyberpolicen für Geschäftskunden in Deutschland an. Der Blick über die Ländergrenzen zeigt, dass Cyberversicherungen in den USA und in Großbritannien bereits zu den Trendprodukten der Branche gehören.

Grundsätzlich kann eine Cyberversicherung durch Standardangebote bis hin zu Individuallösungen ein großes Spektrum an Risiken ab-

HISCOX

AUSSERGEWÖHNLICH VERSICHERT

MAN KANN NICHT ALLE GEFAHREN RIECHEN

Wir versichern Ihr Unternehmen gegen unsichtbare Gefahren wie Hackerangriffe und Datenverlust. Unsere umfassenden Assistance-Leistungen in den Bereichen Prävention und Risikobekämpfung räumen Risken aus und helfen, Schäden zu vermeiden.

16745 11/16

Cyber Risk Management by Hiscox **hiscox.de**

CYBERVERSICHERER* UND POLICEN

Versicherer	Policen
ACE	ACE Data Protect PLUS
AIG	AIG Cyber-Edge 2.0
Allianz	Allianz Cyber Protect
AXA	ByteProtect
DUAL	DUAL Cyber Defence
exali	Cyber-Versicherung
HDI Global SE	HDI Cyber+ (Smart)
Hiscox	Cyber Risk Management
W&W	Die Cyber-Police
Zürich DE	Zurich Cyber & Data Protection

* alphabetisch sortiert

bilden. Die Angebote unterscheiden sich im Umfang der abgesicherten und ausdrücklich ausgeschlossenen Risiken zum Teil deutlich. Zum Standard gehört, dass die Anbieter aber die Kosten für das Abwehren unberechtigter und das Begleichen berechtigter Schadensersatzansprüche Dritter übernehmen sowie die Haftpflicht infolge von Hackerangriffen, Denial-of-Service-Attacken, Datenschutzverletzungen oder nicht funktionierender digitaler Kommunikation.

Ebenso verhält es sich mit dem Übernehmen der direkten Schäden durch Denial-of-Service-Attacken, der Kosten für die Aufrechterhaltung des Geschäftsbetriebs sowie der Verdienst- und Ertragsausfälle bei Betriebsstörungen. Gleichermaßen einheitlich ist die Regulierung von Schäden durch gefälschte, ausgespähte und abgefangene Daten, Computersabotage und das Erschleichen von Zugangsdaten.

Eine Ausnahme bildet die Sabotage der Steuerungs-IT von Maschinen und Anlagen. Einen daraus resultierenden Schaden würden nicht alle Versicherungsanbieter begleichen. Zudem würden nur wenige die Kosten für Ersatzleistungen, Reparaturen oder Neuanschaffungen erstatten. Fragen Sie also vor Abschluss einer Versicherung nach, was die Übernahme von Schäden durch Sabotage im Detail bedeutet!

Geschäftsrisiken im Einzelfall

Bemerkenswert ist an dieser Stelle, dass der Missbrauch unternehmenseigener Computer durch Cyberkriminelle nicht von allen Versicherungsanbietern gedeckt ist. Wie verhält es sich aber, wenn dieser Missbrauch zum Ausspähen von Daten oder eben zur Sabotage genutzt wird? Wie ist diese Regelung in Bezug auf die widerrechtliche Nutzung eines Unternehmensservers zum Speichern und Streamen von (kinder-)pornografischem oder verfassungsrechtlich bedenklichem Material auszulegen? Hieraus können sich drastische strafrechtliche Konsequenzen sowie enorme Reputationsschäden ergeben. Solche Schäden schließen einige Anbieter ausdrücklich aus oder verweisen auf entsprechende Zusatzprodukte.

Die Kosten für das Wiederherstellen gestohlener, zerstörter, beschädigter oder blockierter Daten, Programme und Netzwerke nach einer Cyberattacke übernehmen die Versicherungsanbieter in der Regel. Hierbei sollten Unternehmen aber mit ihrem Anbieter für ihre spezifischen Geschäftsrisiken klären, was das im Einzelfall heißt. Unternehmen, deren Geschäftsmodell beispielsweise größtenteils aus der Nutzung von Kundenkontaktdaten besteht, sollten sich bestätigen lassen, ob darunter der Einkauf komplett neuer Kundenkontaktdaten fällt. Im Zweifelsfall könnte die Regelung auch nur bedeuten, dass die Kosten für die Entschlüsselung unautorisiert verschlüsselter Daten übernommen werden. An dieser Stelle ist darauf hinzuweisen, dass nicht alle Versicherungsanbieter die Schäden durch den Diebstahl von Datenträgern inklusive Folge- und Nebenschäden tragen.

Hilfe bei Erpressung

Bei fast allen Anbietern sind auch die Schäden und Aufwendungen bei Erpressungen über das Internet zumindest theoretische Regulierungsfälle – insbesondere Lösegeldzahlungen unter Umständen allerdings explizit ausgeschlossen. Dabei sind Erpressungsversuche durch Ransomware nicht gerade selten. Selbst wenn die Kriminellen den Schlüssel tatsächlich herausrücken, ist nicht unbedingt gesichert, dass alles klappt. Zahlt die Versicherung auch zusätzlich zum Lösegeld die Folgeschäden, wenn ein Entschlüsseln nicht zustande kommt? Diese Frage wäre auf alle Fälle zu stellen.

Beim klassischen Internetbetrug oder der Urkundenfälschung zahlen nicht alle Anbieter. Letztere ist ein klassisches Mittel, um bei sogenannten Fake-President-Betrugsmaschen beispielsweise die Freigabe von Zahlungsanweisungen durch Geschäftsführer vorzutäuschen. Gerade solche Vorfälle, bei denen Mitarbeiter – bewusst oder unbewusst – zu Mittätern werden, erfordern das Einbinden externer Sachverständiger, die die Vorfälle objektiv aufklären und aufarbeiten. Oft reagieren Unternehmen jedoch genau gegenteilig und versuchen, die Cybervorfälle eigenständig aufzuarbeiten, selbst wenn sie nicht über ausreichend interne Kapazitäten und Fachwissen verfügen. In der Regel führt das zu höheren Schäden, da es die Aufklärung verzögern kann. Zumeist findet in diesen Fällen keine tiefere Ursachenermittlung statt, das heißt, man läuft Gefahr, dass sich solche Vorfälle wiederholen, weil Schwachstellen, Täter und Motivationen nicht ermittelt wurden.

Diesem finanziellen Risiko begegnen die Versicherer bewusst durch das Übernehmen der Kosten für die Schadensermittlung, das Einbinden

Reputationsschäden sind schwer zu beziffern, können das Unternehmen aber empfindlich treffen.

externer IT-forensischer Sachverständiger sowie IT-forensische Untersuchungen.

Was die Reputation kosten darf

Versicherer tragen in der Regel zudem die Kosten für einen externen Krisen- und Kommunikationsmanager, der die Reputation des Unternehmens schützt, und von Juristen für die Rechtsverteidigung sowie -verfolgung. Die Versicherer weisen vereinzelt darauf hin, dass es sich nicht um einen aktiven Rechtsschutz handelt. Unternehmen sollten also nach der freien Auswahl eines Sachverständigen, Krisenmanagers oder Rechtsanwaltes fragen und sich über eine Deckelung der Honorarsätze oder des Gesamthonorars informieren. Häufig stellen Versicherer Kontakte zu Experten her, deren Beauftragung und Kostendeckung bereits abgestimmt und freigegeben sind. Dies erleichtert auch schnelles Reagieren im Ernstfall.

Unterschiede zwischen den Versicherungen ergeben sich im Hinblick auf die Behandlung von Schäden durch interne Täter – nach wie vor eines der am meisten unterschätzten IT-Risiken. Dennoch übernehmen fast alle Versicherer die Schäden infolge des Löschens und Manipulierens von Daten durch Bedienungsfehler. Eine vergleichbare Konstellation findet sich bei der Deckung von Schäden durch das unbeabsichtigte Verbreiten von Malware, etwa durch Weiterleiten befallener E-Mail-Anhänge oder verseuchte Websites. Auch diese Schäden sind durch fast alle Versicherungsanbieter gedeckt.

Ganz ähnlich handhaben die Versicherer die Problematik interner Täter, die vorsätzlich handeln: Gedeckt sind Schäden, die auf Mitarbeiter zurückzuführen sind, die Schwachstellen in Informations- und Kommunikationstechnologien sowie Kontrollmaßnahmen ausnutzen. Auch Schäden durch vorsätzliche Programm- und Datenänderungen durch Mitarbeiter sowie die widerrechtliche Nutzung von IT-Systemen werden von fast allen Versicherungsanbietern reguliert.

Dauer des Versicherungsschutzes

Die Versicherungsdauer, während der der Schutz besteht, variiert je nach Anbieter. Während bei manchen die Regelung existiert, dass das versicherte Ereignis innerhalb der Vertragslaufzeit erfolgen muss, gibt es bei anderen eine unbegrenzte Rückwärtsdeckung und eine automatische Nachhaftung von fünf Jahren. Fast alle Versicherer wenden das Claims-made-Prinzip an, das heißt, dass unabhängig vom Zeitpunkt des Schadeneintritts (etwa dem Erstzugriff durch einen Cyberkriminellen) der Zeitpunkt der Anspruchserhebung gegen den Versicherer (das Feststellen des Angriffs) ausschlaggebend ist. Sie ist also das Ereignis, das innerhalb der Versicherungsdauer liegen muss.

Generell deckt das Angebot Unternehmen jeder Größe – gemessen am Umsatz – und sämtlicher Branchen ab. Dabei konzentrieren sich die Versicherungsunternehmen zum Beispiel auf kleinere Unternehmen ausgewählter Branchen wie der produzierenden Industrie oder Transport und Verkehr mit einem Umsatz von unter 10 Millionen Euro. Ein anderer Schwerpunkt liegt auf Unternehmen mit einem Umsatz von bis zu 3 Milliarden Euro und einer übergreifenden Branchenabdeckung oder auf Finanzdienstleistungsunternehmen. Einige Versicherer konzentrieren sich auf die produzierende Industrie ab einem Umsatz von 5 Millionen Euro. Aber auch Unternehmen jeder Branche ab einem Umsatz von 100 Millionen Euro sind eine Zielgruppe. Angesprochen werden dabei überwiegend der deutsche und der europäische Markt.

Fragen vor einem Abschluss

Sollte man sich als Unternehmen dafür entscheiden, eine Cyberversicherung abzuschließen, kann man je nach Bedarf zwischen standardisierten Deckungsbausteinen und individuellen Lösungen wählen. Die Deckungssumme ist bei allen Versicherern nach oben und oft auch nach unten hin begrenzt. Die größte Flexibilität wird bei ausbleibender Minimalgrenze der Deckungssumme und einer Maximalgrenze bei 100 Millionen Euro erreicht. Individuelle Regelungen sind jedoch immer möglich. Der Eigenanteil des Versicherungsnehmers – auch im Hinblick auf vorab definierte Ausfallzeiten – ist mit den meisten Versicherern individuell verhandelbar. Untergrenzen liegen häufig bei 1000 Euro beziehungsweise vier Stunden. Dies ist jedoch wie bei anderen Versicherungsformen stark abhängig vom gewählten Deckungsumfang.

Bevor Versicherer eine Police abschließen, unterziehen sie das zu versichernde Unternehmen einer Risikoprüfung. Art und Umfang dieser Prüfung hängen von der Deckungssumme, der Größe des Unternehmens und den exponierten Risiken ab. Das Spektrum ist breit und beginnt bei der Selbstauskunft durch Ausfüllen eines Fragebogens. Eine weitere Variante wäre ein Risikodialog zwischen internen Sachverständigen des potenziellen Versicherungsnehmers sowie IT-(Sicherheits-) und Forensik-Experten über den Gefährdungsgrad (Welche Risiken bestehen konkret und wie groß wäre der mögliche Schaden?) und den vorhandenen Schutz (Welche spezifischen Schutzmaßnahmen sind implementiert?). Schließlich sind auch sogenannte Penetrationstests durch externe Sachverständige denkbar.

Der Versicherungsbeitrag und die tatsächlich festgesetzte Versicherungssumme ergeben sich vor allem aus dem Reifegrad der IT- und Informationssicherheit im Unternehmen, dem Selbstbehalt und dem Risiko von Dritt- und Eigenschäden. Das mögliche Ausmaß Letzterer leitet sich sowohl von den Sicherheitsmaßnahmen ab, die einen Cybervorfall verhindern sollen (Intrusion Prevention), als auch von denjenigen zum Erkennen (Intrusion Detection) eines Vorfalls sowie ersten Reaktionen darauf (Incident/Cyber Response). Immer mehr an Bedeutung gewinnt in diesem Zusammenhang die Fähigkeit von Unternehmen, über die eigentliche Abwehr und Schadensbegrenzung hinaus entscheiden zu können, welcher Vorfall forensische Reaktionsmaßnahmen im Sinne einer gerichtsfesten Beweisdatensicherung und -analyse erfordert, und entsprechende interne und externe Spezialisten umgehend zu mobilisieren.

Um den Versicherungsbeitrag zu reduzieren und die Versicherungssumme zu erhöhen, können Unternehmen einen aktiven Beitrag in Form von Zertifizierungsnachweisen und externen IT-Audits leisten. Generell ist die Vorbereitung auf einen Schadensfall durch das Erstellen von Notfall-, Management- und Wiederanlaufplänen mit definierten Verantwortlichkeiten und regelmäßig durchgeführten Penetrationstests, Notfallübungen und Systemupdates zu empfehlen. Einige Versicherungsanbieter bieten auch präventive Maßnahmen an. Unternehmen sollten ihren Versicherungsanbieter oder Makler darauf ansprechen.

Wenn der Schadensfall eintritt

Kommt es zum Schadensfall, ist die Erstreaktion besonders kritisch. Unklare Zuständigkeiten sowie Fehler in der Beweissicherung und der Kommunikation haben oft irreparable Auswirkungen. Auch die Versicherer weisen im Falle eines Schadens auf die Wichtigkeit der sofortigen Kontaktaufnahme mit dem dafür vorgesehenen Notfall-Service und gegebenenfalls internen IT-Sicherheitsexperten hin. Konkret besteht dieser Service in einer Notfall-Hotline, meist ergänzt von einer umfangreicheren Cyber-Assistance durch IT-Forensik-Experten. Diese stellen mit ihrer Erfahrung und globalen Netzwerken sicher, dass die Beteiligten schnell, koordiniert und angemessen auf die Situation reagieren, selbst wenn zeitgleich an mehreren Unternehmensstandorten Reaktionsmaßnahmen erforderlich sind. Sie unterstützen bei der Schadenseindämmung, Beweisdatensicherung und -analyse, Aufarbeitung sowie Bewältigung des Schadens. Sie geben Empfehlungen zum Beheben des Cybervorfalls oder für das Einbinden weiterer Spezialisten, beispielsweise Anwaltskanzleien. Zumeist handelt es sich dabei um Wirtschaftskanzleien, spezialisiert auf Datenschutzrecht, Arbeitsrecht und Strafrecht. Für Unternehmen ist es wichtig zu berücksichtigen, dass Cybervorfälle keiner technisch orientierten Reaktion und Aufarbeitung bedürfen.

In der Regel sind nicht nur beim eigentlichen Cyberangriff personenbezogene Daten von Kunden oder Mitarbeitern des Unternehmens betroffen. Auch bei der nachfolgenden Untersuchung können Persönlichkeitsrechte der Betroffenen verletzt werden. Die Gestaltung der Sonderuntersuchung könnte ein Mitbestimmungsrecht des Betriebsrats begründen, das in der Regel mit einer vollumfänglichen Beteiligung der Arbeitnehmervertretung einhergeht. Darüber hinaus stellt sich gerade beim Aufarbeiten des Vorfalls die Frage, ob und inwieweit das Datenleck durch ein strafbares Verhalten eines Mitarbeiters entstand und ob dieses Fehlverhalten strafrechtlich und arbeitsrechtlich sanktioniert werden kann.

IT-Forensiker arbeiten überdies eng mit PR-Beratern zusammen. Sie stellen die komplexen technischen Sachverhalte einfach und verständlich dar und ermöglichen somit klare Aussagen nach innen und außen. Sie wissen auch im Bedarfsfall, für welche ausgewählten Einzelfragen weitere technische Spezialisten, beispielsweise für Fragen zu proprietärer Software, einzubeziehen sind.

Nach Beurteilung der Versicherer nehmen die IT-Forensik-Experten eine Schlüsselrolle im Schadensfall ein. Ergänzend zur Weiterführung der Geschäfte (Krisenmanagement, Business Continuity Management, Disaster Recovery) sichern sie den Bestand der Daten und Beweise während und nach einer Krise. Im Bedarfsfall definieren sie auch Kriterien für ein vertieftes Monitoring kritischer Daten und Systeme für einen Übergangszeitraum, um ein erneutes Aufflammen komplexer Vorfälle zu verhindern. In Zeiten, in denen man davon ausgehen kann, dass früher oder später jedes Unternehmen von Sicherheitsvorfällen betroffen sein wird, trägt die professionelle Reaktion im Ernstfall auch dazu bei, Reputationsschäden zu reduzieren.

Was die Zukunft bringt

Vor allem Unternehmen, deren Geschäftsbetrieb in hohem Maße von IT abhängig ist und die einen großen Bekanntheitsgrad genießen, dürften sich zunehmend an die Cyberversicherer wenden. Aus Sicht der Autoren wird der Aspekt der Standardisierung der Cyberversicherung einhergehen mit einer verfeinerten Methodik, die messbare Reaktionsfähigkeit von Unternehmen auf Cybervorfälle in Beziehung zu Versicherungsbeitrag und -summe zu setzen. Zwangsläufig ist dafür eine breitere Basis von ausgewerteten Schadensfällen und Vergleichsinformationen zum Reifegrad der Unternehmen notwendig. Mit der Standardisierung wird auch der Bedarf der Versicherungsanbieter verbunden sein, sich mit ihrem Produkt von dem der Konkurrenz zu unterscheiden – idealerweise aber nicht vorrangig durch den Preis. Versicherer werden im Zuge des individuellen Vertragsabschlusses dann zunehmend auf Unternehmen treffen, die ganz genau wissen, welche ihre spezifischen Cyberrisiken sind und wie sie ihnen wirksam begegnen.

Thomas Fritzsche und Alexander Geschonneck,
Cyber Forensic Team, KPMG AG

UNSCHÄRFEN BEI VERBUNDENEN DRITTEN

Besonders aufzupassen gilt es bei den Regelungen zu Cyberangriffen auf verbundene Dritte, zum Beispiel Cloud-Anbieter oder Geschäftspartner, die Unternehmensdaten nutzen oder bereitstellen. Hier bietet sich bei den Versicherern ein äußerst heterogenes Bild. Letztendlich verdeutlicht das die Notwendigkeit einer intensiven Diskussion darüber, wie verbundene Dritte zu definieren sind. Sind davon auch Konzerngesellschaften betroffen? Wie sind Minderheitsbeteiligungen geregelt? Ist die Möglichkeit der Einflussnahme auf verbundene Dritte erheblich?

Ausdrücklich nicht abgesichert werden bei fast allen Versicherern beispielsweise Personen- und Sachschäden. Strafzahlungen nach Verurteilungen sind bei einem Großteil ebenfalls explizit nicht gedeckt. Dafür übernehmen einige Anbieter auch die Kosten für Auswertungen elektronischer Dokumente und Daten im Zusammenhang mit Rechtsstreitigkeiten oder regulatorischen beziehungsweise behördlichen Anfragen (E-Discovery).

Die Beispiele zeigen, dass die Regelungen der Anbieter versuchen, alle abgedeckten sowie alle ausdrücklich ausgeschlossenen Schadensfälle hinreichend zu definieren. Dennoch besteht für Versicherungsnehmer die Notwendigkeit, konkrete Risikoszenarien für das eigene Unternehmen zu definieren und diese im Risikodialog mit dem Versicherer anhand des jeweiligen Bedingungswerks zu prüfen.

Keine Chance für Produktpiraten

Der industrielle Anwendungsbereich verlangt nach verlässlichen Sicherheitskonzepten

Die beste Verschlüsselung taugt nur dann, wenn die Schlüssel auch sicher aufbewahrt werden. Das gilt nicht nur für den Nachrichtenaustausch, sondern auch auf der Prozess- und Anwendungsebene im industriellen Bereich. Doch gerade hier wird es Datendieben oftmals noch viel zu leicht gemacht.

Nach wie vor prallen beim Konzept Industrie 4.0 zwei völlig unterschiedliche Welten aufeinander: Auf der einen Seite die IT-Branche, deren Lizenzverträge gerne die Klausel „Mir ist bekannt, dass die Software Fehler enthalten kann“ beinhalten. Auf der anderen Seite stehen die Industrieunternehmen, also der Praxiseinsatz, der möglichst fehlerfrei ablaufen sollte. Durch das Internet haben beide Welten schon längst zueinandergefunden, was bei der Kommunikationssicherheit und der Angreifbarkeit von Industrieanlagen für Betreiber ebenso wie für Hersteller einige Herausforderungen mit sich bringt.

Erste positive Entwicklungen sind bereits erkennbar, gerade für die IT-Sicherheit im industriellen Umfeld. So hat das Bundesministerium für Wirtschaft Anfang des Jahres die Studie „IT-Sicherheit für die Industrie 4.0“ veröffentlicht, die nicht nur einen Überblick über die derzeitige Lage in deutschen Industrieunternehmen beinhaltet, sondern auch klare Handlungsempfehlungen für die unterschiedlichen Disziplinen der IT-Sicherheit gibt. Allerdings: Bei der Betrachtung des Referenzarchitekturmodells RAMI 4.0 wird das Thema IT-Sicherheit nur peripher adressiert. Zudem divergieren in manchen Bereichen die Schutzziele zwischen Industrie und IT-Branche extrem.

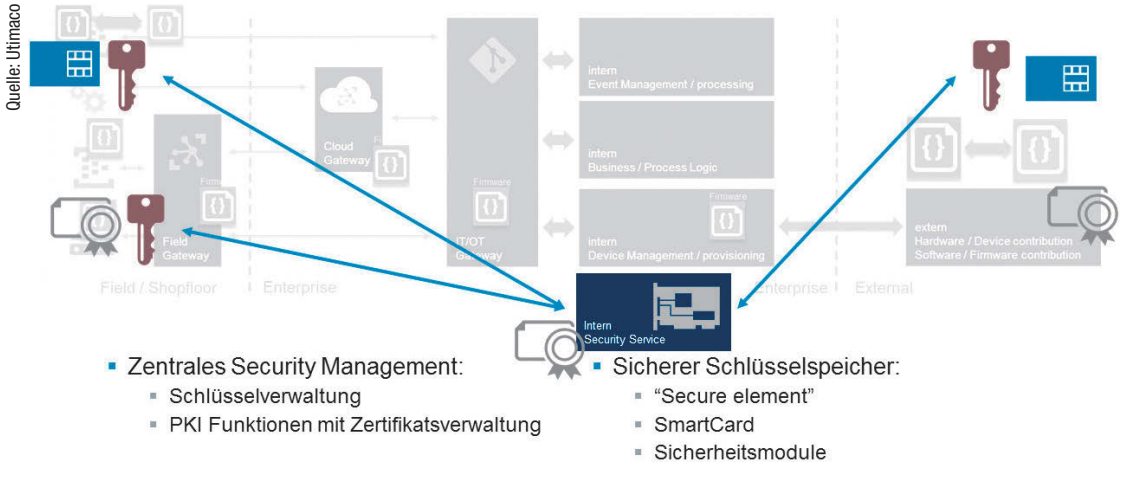
IT-Sicherheit in allen Bereichen

Mit der zunehmenden industriellen Automatisierung steigen die Anforderungen an die IT. Neben den bestehenden Kriterien an die funktionale Sicherheit rückt vor allem die Datensicherheit in den Fokus. Ein erster Schritt ist, die bewährten Sicherheitstechniken aus der IT in Unternehmensnetzwerken auch im industriellen Bereich anzuwenden. Damit ist es jedoch längst nicht getan. Um den Erfolg der 4. Industriellen Revolution nicht zu gefährden, ist es höchste Zeit, geeignete Sicherheitstechniken und angewandte Kryptografie in die industriellen IT-Systemarchitekturen zu integrieren.

Betrachtet man die unterschiedlichen Protokolle, Systemkonzeptionen und Architekturen im Industrieumfeld etwas genauer, so stellt man fest, dass IT-Sicherheit immer ein Bestandteil der Konzeptionen und deren Abhandlungen ist. Doch diese Sicherheit beschränkt sich bisher stark auf das Thema Kommunikation, also konkret auf den Einsatz von VPN, SSL/TLS. Dies macht aber auch in der IT-Welt nur einen kleinen Teil eines umfassenden Sicherheitskonzeptes aus. Im industriellen Bereich sieht es nicht anders aus.

Kryptografie gegen Produktpiraterie

Ein Grund, warum der Kommunikationssicherheit so große Aufmerksamkeit geschenkt wird, liegt darin, dass die Big Player der Kommunikationsbranche wie Cisco, Juniper oder auch Oracle mit millionenschweren Marketingbudgets in die Absatzmärkte gehen. Produkte wie Firewalls oder VPN-Gateways sind zweifelsohne wichtige Elemente eines umfassenden Sicherheitskonzeptes, doch die Datensicherheit innerhalb des Anwendungskontextes ist ebenfalls ein wesentlicher Bestandteil für die Gesamtsicherheit.



Digitaler Schlüsseltresor: Hardware-Security-Module sorgen dafür, dass kryptografische Codes sicher aufbewahrt sind.

VERSCHLÜSSELUNG IST KEIN SICHERHEITSRISIKO

Nicht nur das FBI hat bei verschlüsselten Verbindungen spezielle Hintertüren für staatliche Ermittlungen gefordert. Entsprechende Begehrlichkeiten gibt es auch in der EU und in Deutschland. Aus gutem Grund mahnt z.B. TeleTrusT, der Bundesverband für IT-Sicherheit e.V., ein besonnenes Vorgehen in der Debatte um ein Verschlüsselungsverbot an.

Niemand wird bestreiten, dass Verschlüsselung auch von Kriminellen und Terroristen genutzt werden kann, um ihre Kommunikation abzusichern. Der Verschlüsselung geht es nicht anders als jeder anderen Schutzmaßnahme – sie kann missbraucht werden. Es liegt aber auf der Hand, dass nichtcodierte Kommunikation den Kriminellen mehr helfen würde als verschlüsselte Kommunikation. Daher stehen verschiedene Stellen auf dem Standpunkt: Verschlüsselung ja, aber mit Hintertür. Die Internet-Nutzer und Unternehmen dürften dann verschlüsseln, solange Ermittlungsbehörden an den Schlüssel kämen.

Diese Vorstellung verkennt allerdings die Tatsache, dass jede Hintertür eine Schwachstelle ist. Und Schwachstellen können von kriminellen Dritten ausgenutzt werden. Man kann davon ausgehen, dass legalisierte Lauschangriffe nicht die einzigen bleiben. Kriminelle Lauschangriffe werden früher oder später den gleichen Weg nutzen.

Wer Backdoors fordert, übersieht, dass nur eine echte Ende-zu-Ende-Verschlüsselung wirklich schützen kann. Und er verkennt zum anderen die Folgen, die eine Verschlüsselung mit Hintertür für die gesamte Kommunikation hat: Wenn klar ist, dass staatliche Stellen Zugriff auf die Daten haben, verlieren Unternehmen die letzte Motivation, sich um mehr Datensicherheit zu bemühen.

Oliver Schonschek,
News Analyst, MittelstandsWiki

In der Industrie ist das aber noch längst nicht immer der Fall. Dabei sollten sich besonders Industrieunternehmen gegen Produktpiraterie und Know-how-Verlust wappnen. Wurde das geistige Eigentum erst einmal entwendet, kann das die gesamte Existenz eines Unternehmens gefährden. Daher ist es elementar, die Software soweit abzusichern, dass keine externe, unbefugte Person bzw. Maschine schützenswerte Informationen und wertvolles Wissen auslesen kann. Die gute Nachricht: Die Verantwortlichen können mit einfachen Mitteln der Kryptografie den Datendieben einen Riegel vorschieben.

Durch die Anwendung symmetrischer Verschlüsselungsverfahren, bei denen die Daten mittels eines Schlüssels ver- und entschlüsselt werden, bleibt die Tür für Cyberkriminelle verschlossen – oder ist zumindest nur schwer zu öffnen. Dieses Verfahren lässt sich relativ einfach auf Softwaresysteme anwenden und sichert so die gesamte Verteilerkette vom Erzeuger bis zum Endgerät. Wie aber verteilt man Schlüssel, die doch geheim sind? Wie kann man sicherstellen, dass der Absender vertrauenswürdig ist? Und wie erkennt man trotz Verschlüsselung, ob der Inhalt nicht eventuell doch schädlich ist?

Datentransparenz trotz Verschlüsselung

Schon lange ist das Problem bekannt, dass verschlüsselte Datenpakete, Transaktionsnachrichten oder auch Dateien zum Teil Klartextinformationen beinhalten müssen. Sie dienen zur Angabe von Empfängerinformationen oder Routing-Nachrichten oder auch als Identifikationsmerkmale. Ein sehr probates und auch einfaches Mittel ist die partielle Verschlüsselung. Dabei bleiben unkritische Informationen innerhalb der Datei im Klartext erhalten, nur der Nutzerdatenblock wird verschlüsselt. So erkennt das Betriebssystem beispielsweise nach wie vor das Dateiformat, also etwa ein Word-Dokument, obwohl die eigentlichen Inhalte nicht lesbar sind.

Doch wie kann einfach sichergestellt werden, dass der Absender des Datenpaketes vertrauenswürdig ist? Diese Frage stellt sich zunehmend gerade im IoT-Zeitalter, wird aber oft nur unter dem Aspekt der Identitäten behandelt. Mit einem Identitätscheck allein ist es aber leider nicht getan. Um die Vertrauenswürdigkeit des Absenders zu überprüfen, helfen bewährte Mittel wie Zertifikate und PKIs (Public-Key-Infrastrukturen). Wichtig ist, dass innerhalb einer komplexen Verteilerkette – von der Erstellung bis hin zum Endgerät – die Überprüfung der Identität jederzeit gewährleistet sein muss. An dieser Stelle gibt es keine Antwort, die alle Eventualitäten abdeckt. Daher sollten Mittel und Verfahren immer individuell und bedarfsgerecht abgewogen werden.

Geheimes bleibt geheim

Ein wichtiger Aspekt beim Identitätsschutz ist die zweite Variante der Verschlüsselung, das asymmetrische Verfahren. Grundlage dafür sind zwei verschiedene Schlüssel: ein öffentlicher (Public Key) und ein geheimer. Hierbei handelt es sich um ein Schlüsselpaar, das immer korrespondiert und den wesentlichen Teil der oben genannten Identität darstellt. Hat der öffentliche Schlüssel die Aufgabe, Daten zu verschlüsseln und elektronische Signaturen zu verifizieren, kommt dem geheimen Schlüsselteil die Aufgabe der Signaturerstellung zu.

Nur mit der elektronischen Signatur lässt sich die Authentizität der Datei nachweisen. In Kombination mit einem Hashwert wird ebenso die Integrität der Daten verifiziert. Damit bleibt nur noch zu klären, wie die geheimen Schlüssel auch wirklich geheim gehalten werden. Die Antwort: Mithilfe von Sicherheitsspeichern, sogenannten Tokens, oder auch Hardware-Security-Modulen (HSM) sowie Secure Elements, die entweder auf Chipebene Funktionen zum Verwalten der Schlüssel bieten oder als eigenständiges Gerät mit einer hohen Leistungsfähigkeit angeboten werden. Sicherheitsmodule gibt es in unterschiedlichen Bauformen und Bezeichnungen, etwa als USB-Token, als Chipkarte oder als 19-Zoll-Serverkomponente. Sie alle haben Verfahren und Mechanismen implementiert, die den Schutz der kryptografischen Schlüssel vor Angriffen von außen gewährleisten.

Fazit

Eine durchgehende Ende-zu-Ende-Verschlüsselung, wie sie in vielen Publikationen und Konzepten gefordert wird, lässt sich nicht allein durch das Absichern der Kommunikation erreichen. Damit der Erfolg von Industrie 4.0 weiterhin anhält und das Potenzial dahinter ausgeschöpft werden kann, müssen IT-Sicherheit und Kryptografie auch Einzug in die Anwendungsebenen halten. Ebenso wichtig ist ein Umdenken in der IT-Branche: Die Anbieter sind gefordert, Geräte und Baugruppen bereitzustellen, die den Anforderungen der Industrie gewachsen sind. Dazu gehört auch, dass diese in die bestehende Steuerung und Prozessautomatik integriert werden können. Nur so lässt sich das Risiko, dass Unternehmens- und Produktionsdaten in die Hände von Cyberkriminellen gelangen, auf ein Minimum reduzieren.

Andreas Philipp,
Vice President Business Development, Utimaco GmbH

Sichere Kommunikation in der Industrie 4.0

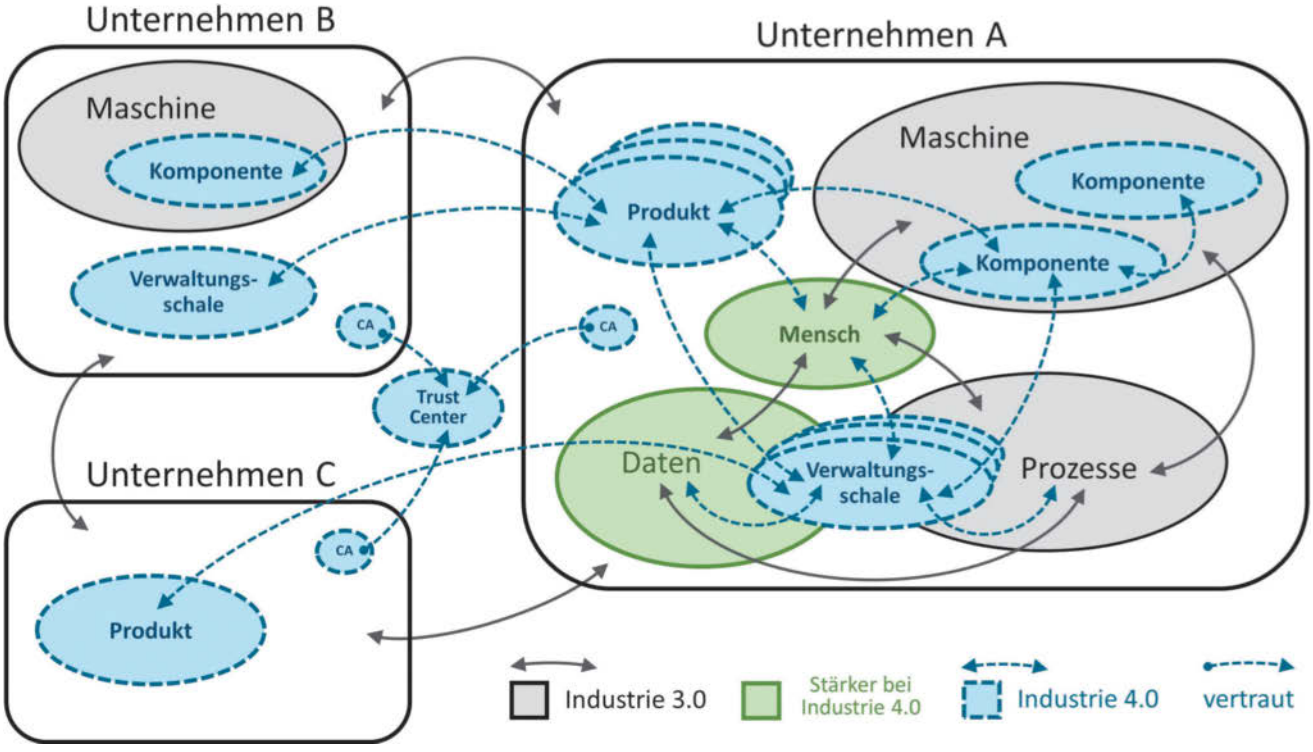
Die Vernetzung automatisierter Produktionssysteme erfordert umfassende Sicherheitskonzepte

Der Aufbau unternehmensübergreifender Wertschöpfungsnetzwerke basiert auf einer leistungsfähigen, zuverlässigen digitalen Infrastruktur. Gut geschützte Übertragungswege, gesicherte Integrität und Authentisierung sowie hohe Verfügbarkeit nehmen dabei die Schlüsselrollen ein.

Die Digitalisierung der Automatisierung durchzieht in der Industrie 4.0 den gesamten Lebenszyklus industrieller Produktion und industriell gefertigter Produkte. Erwartet werden Verbesserungen in vielen Dimensionen, unter anderem bei Effizienz, Flexibilität und Resilienz. Ein wesentlicher Baustein ist dabei die unternehmensübergreifende Kommunikation. Hierbei wird nicht mehr nur auf interner Ebene kommuniziert, vielmehr findet direkte Kommunikation zwischen einzelnen Komponenten und Systemen unternehmensübergreifend statt. Die Anwendungsgebiete beginnen bei Fernwartung und Predictive Maintenance und gehen über Betreibermodelle bis hin zu zukünftigen, noch zu entwickelnden Geschäftsmodellen in dynamischen Wertschöpfungsnetzwerken.

Die Umsetzung dieser neuen Konzepte setzt einen angemessenen Schutz von Informationen und Daten sowie Systemen und Prozessen voraus. Die Grundlagen des entsprechenden Risikomanagements und der Klassifizierung sind bekannt und beschrieben, wobei die ISO 27000 für die IT bereits länger etabliert ist. Die auf die Automatisierung zielende Norm IEC 62443 setzt auf der ISO 27000 auf, ergänzt um spezifische Themenfelder. Durch eine ganzheitliche Sicht auf Betreiber, Integratoren bzw. Maschinenbauer sowie Komponentenlieferanten geht sie sogar über die Sicht der ISO 27000 hinaus. Leider sind in der industriellen Praxis viele Aspekte bisher nicht umgesetzt, wie u.a. eine aktuelle BSI-ZVEI-Umfrage zeigt. Neue Herausforderungen entstehen in den agilen Wertschöpfungsnetzwerken von Industrie 4.0,

Quelle: Plattform Industrie 4.0



Kommunikations- und Vertrauensbeziehungen bei Industrie 4.0

da individuelle vertragliche Vereinbarungen an Relevanz verlieren. Die Bewertungsmaßstäbe müssen also unternehmensübergreifend vereinheitlicht werden.

System- und Informationsintegrität

Im Mittelpunkt aller unternehmerischen Aktivitäten stehen die Geschäftsprozesse, die geschützt werden müssen. Die Verfügbarkeit von Geschäftsprozessen steht schon heute im Fokus produzierender Unternehmen. In unternehmensübergreifenden Netzwerken entstehen zusätzliche Anforderungen an die Verfügbarkeit von Kommunikationsverbindungen. Wer zum Zeitpunkt einer Online-Transaktion, z. B. einer Auftragsvergabe, nicht verfügbar ist, muss mit Geschäftseinbußen rechnen.

Elementare Voraussetzung ist auch die Integrität der beteiligten Systeme. Kompromittierte Systeme können versagen oder den Schutz von Informationen und Daten nicht mehr gewährleisten.

In der Automation nimmt die Integrität eine sehr wichtige Rolle ein. Aus fehlerhaften Daten könnten fehlerhafte Produkte folgen oder Aufzeichnungen, etwa zur Qualitätssicherung, wären nicht konsistent. In solchen Fällen wird die Produktion gestoppt, die Integrität also sehr hoch bewertet. Produktionsverantwortliche gehen dann aber zumeist von einem Verfügbarkeitsproblem aus. Und auch die Vertraulichkeit von Know-how, Rezepturen, Konstruktionsdaten usw. spielt in der Automation eine große Rolle, da diese Daten eng mit der Wettbewerbsfähigkeit eines Unternehmens verbunden sind.

Zentrale Anforderungen

Ziel der Kommunikation ist der Austausch von Informationen, um neues Wissen und so neuen Wert generieren zu können. Die zugrunde liegenden Daten müssen entsprechend des jeweiligen Bedarfs geschützt werden. Dafür lassen sich einige wesentliche Aspekte festhalten:

Die *sichere Übertragung* von Daten muss alle Anforderungen an den Schutz von Unternehmenswerten erfüllen, wobei miteinander in Konflikt stehende Herausforderungen zu bewältigen sind.

Für die *vertrauliche Kommunikation* über Unternehmensgrenzen hinweg muss der Dienstanbieter die Sicherheit garantieren. Zusätzlich ist eine verschlüsselte Kommunikation entsprechend etablierter Standards (z. B. VPN) einzusetzen. Für Kommunikation in Unternehmen hinein könnte eine Ende-zu-Ende-Verschlüsselung verwendet werden, die aber keine Überwachung der Kommunikation erlaubt, wie dies hingegen bei der Verwendung von Gateways möglich ist.

Die *Integrität* der Kommunikationswege wird grundsätzlich von den gleichen Protokollen ermöglicht, die auch Verschlüsselung erlauben. In den meisten Implementierungen sind aber Verschlüsselung und Integritätsschutz (Message Authentication Code) zwangsweise gekoppelt, sodass ein reiner Integritätsschutz auf Protokollebene Eingriffe erfordert.

Für die *Verfügbarkeit* von Verbindungen ist der Dienstanbieter verantwortlich. Dabei ist eine Zusage über die dauerhaft zur Verfügung stehende Bandbreite und Dienstgüte auch unter Last notwendig. Entsprechende Anforderungen an den Ausbau der digitalen Infrastruktur sind auf politischer Ebene zu adressieren.

Da absolute Sicherheit nicht möglich ist, sind *Detektion und Reaktion* elementare Bestandteile jeder Security-Strategie. Die Überwachung verschlüsselter Kommunikation ist jedoch nicht möglich, sodass viele Betreiber industrieller Anlagen verschlüsselte Ende-zu-Ende-Verbindungen verbieten. Bereits heute sind Gateways und Sprungserver im Einsatz, die aber aufgrund schlechter Eignung der verwendeten Protokolle nicht gut skalieren. Hier sind in der Standardisierung von Industrie 4.0 die entsprechenden Anforderungen an die Kommunikation im Sinn eines Security by Design zu berücksichtigen.

Die Sicherheit der Daten ist nicht nur während der Übertragung bedroht. In vielen Fällen ist die Kommunikation gefährdet, weil die *Endpunkte* angegriffen werden können. Bei fehlerhafter Umsetzung kann die Identität eines Kommunikationspartners gefälscht und die Kommunikation abgefangen oder manipuliert werden. Wenn Industrie-4.0-Komponenten über Unternehmensbereiche hinaus kommunizieren, öffnen sich gleichzeitig neue Angriffsflächen. Insofern müssen sie über entsprechende Sicherheitsmechanismen verfügen, die den erweiterten Bedrohungen Rechnung tragen.

Rechte und Rollen

Im unternehmensübergreifenden Einsatz sollten Zugriffe und Aktionen feingliedrig organisiert sein. Benutzer und Systeme aus einem externen Unternehmen müssen andere Zugriffsrechte haben als lokale Teilnehmer. Alle Zugangsberechtigungen müssen also über entsprechende Modelle abgebildet werden, die allerdings bisher in den meisten Industriekomponenten noch nicht vorhanden sind.

Als typisches Beispiel sei hier die Rollenbasierte Zugriffskontrolle (RBAC) genannt, die in der Standard-IT heute üblich ist. Für autonom agierende Systeme in der Industrie 4.0, die selbst Beauftragungen vornehmen können, ist die Betrachtung der technisch verfügbaren Rechte mit organisatorischen Vorkehrungen (z. B. Wertgrenzen) zu koppeln. Technisch müssen diese Anforderungen durch starke Authentifikation der Teilnehmer im Hinblick auf sichere Identitäten unternehmensübergreifend unterstützt werden.

Für die beschriebenen Anforderungen hat die sichere Identifikation und Integrität von Kommunikationsteilnehmern eine besondere Bedeutung. Um ein unternehmensübergreifendes Identitätsmanagement erreichen zu können, ist ein gemeinsames Vertrauensmodell notwendig. Dabei sind die Identitäten einzelner Kommunikationsteilnehmer aus Sicht ihrer Rollen zu betrachten. Dies können technische Rollen sein („Stanzmaschine links“) oder auch organisatorische Rollen („Einkäufer, i.V.“). Ebenso wichtig ist hierbei die Integrität der Kommunikationspartner. Ein elektronischer Schlüssel in einem Security-Modul alleine nützt nichts, wenn das System, das den Schlüssel verwendet, kompromittiert ist. Auch hier ist also der Integritätsschutz relevant, wenn sich beispielsweise die Frage stellt, ob die Identität der Software noch gegeben ist.

Fazit

Eine wirklich sichere Kommunikation, die auf allen Ebenen effizient funktionieren soll, verlangt mehr als verschlüsselte Verbindungen. Der Aufbau unternehmensübergreifender Wertschöpfungsnetzwerke erfordert also eine leistungsfähige, zuverlässige digitale Infrastruktur. Dabei muss die Sicherheitsbetrachtung auf Ebene der auszutauschenden Daten und Informationen stattfinden, sodass Application Level Gateways die Aufgaben von VPN und Firewall ergänzen können. Zusätzlich ergeben sich auch organisatorische Anforderungen an das Management der Teilnehmer. Integrität und Identität nehmen hier eine Schlüsselrolle ein. Die bestehenden Sicherheitsstandards müssen weiterentwickelt werden, um diese Anforderungen umzusetzen. Nur so kann eine gemeinsame Vertrauensbasis geschaffen werden, die den Austausch sensibler Unternehmensdaten ermöglicht.

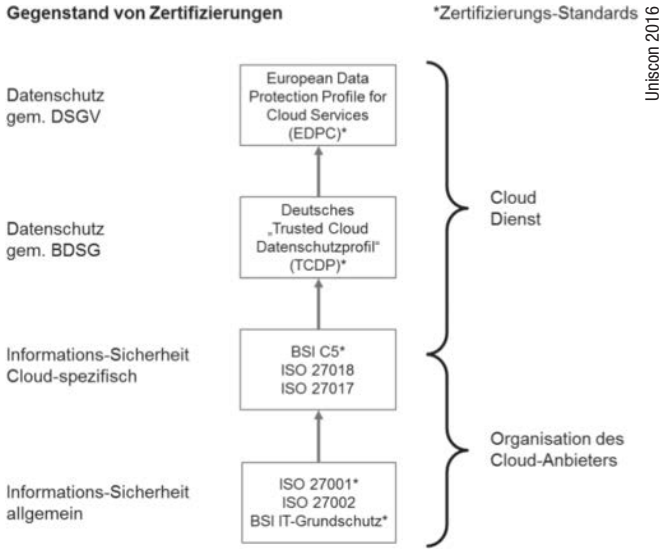
Dr. Lutz Jänicke,
Phoenix Contact GmbH & Co. KG.

Cloud-Anbieter auf dem Prüfstand

Unabhängige Zertifikate erleichtern die datenschutzkonforme Nutzung von Cloud-Diensten

Unternehmen kennen den Schutzbedarf der in ihrem Betrieb anfallenden Daten genau. Was sie oft nicht wissen: Welche Cloud-Dienste bieten das nötige Datenschutzniveau? Deshalb entwickelte eine Expertengruppe unter der Schirmherrschaft des BMWi das Trusted-Cloud-Datenschutzprofil (TCDP).

Die von Ernst & Young durchgeführte Studie „Datenklau 2015“ analysiert die Datensicherheit von 450 deutschen Unternehmen. Sie belegt: Diejenigen, die sich für Cloud-Dienste entscheiden, können aktuell noch immer schwer einschätzen, wie sicher ihre Daten in externen Rechenzentren sind. Besonders bei Public-Cloud-Diensten fehlte den Unternehmen bis jetzt eine Möglichkeit, das Datenschutz- und Sicherheitsniveau verschiedener Angebote zu vergleichen. Trotzdem müssen sie bei der Auftragsdatenverarbeitung Kontrollpflichten wahrnehmen, die bereits vor der eigentlichen Auftragserteilung greifen. Es gilt zu prüfen, ob die technischen und organisatorischen Maßnahmen des Cloud-Anbieters dem Schutzbedarf der Daten entsprechen. Die laufende Kontrolle aller Rechenzentren, die die Unternehmensdaten verarbeiten, verschlingt dabei Personal- und Zeitressourcen, und auch die verpflichtende Dokumentation dieser Kontrollmaßnahmen verursacht Kosten. Alles in allem also ein Aufwand, den gerade mittlere und kleinere Unternehmen kaum leisten können. Ganz zu schweigen davon, dass die Kontrollpflichten den Verantwortlichen erhebliches Know-how abverlangen. Sie müssen die sicherheitstechnischen Maßnahmen im Rechenzentrum zum Schutz der Daten tatsächlich auch einschätzen können.



Zertifizierungsschema mit dem Trusted-Cloud-Datenschutzprofil (TCDP)

Eine Zertifizierung von Cloud-Diensten hinsichtlich ihrer Datensicherheit, die unabhängige Prüfungsinstanzen durchführen, könnte hier für die notwendige Entlastung sorgen. Aus diesem Grund haben Datenschutzbehörden und Vertreter der Wirtschaft, der Anwaltschaft und der Rechtswissenschaft gemeinsam im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) im Rahmen des Trusted-Cloud-Programms einen Anforderungskatalog entwickelt. Dieser Katalog, das Trusted-Cloud-Datenschutzprofil (TCDP), bildet die Basis für eine umfassende Datenschutzzertifizierung.

Datensicherheit nach TCDP

Es ist die Aufgabe eines Zertifikats zu beglaubigen, dass Cloud-Dienstleister die gesetzlichen Vorgaben und Normen einhalten. Deshalb wurde in zwei Jahren Arbeit ein Anforderungskatalog entwickelt, der die gebotenen Maßnahmen für den Datenschutz und die IT-Sicherheit bei Cloud-Diensten festhält. Das TCDP basiert auf anerkannten Standards, deckt alle datenschutzrechtlichen Vorgaben für die Auftragsdatenverarbeitung in der Cloud ab und stellt dabei selbst einen prüffähigen Standard dar.

Das Zertifikat nach dem TCDP bezieht sich explizit auf den Datenschutz und die Datensicherheit einer Public Cloud. Damit Unternehmen und andere Cloud-Nutzer eine Wahl zwischen verschiedenen Diensten treffen und den Grad der jeweiligen Datensicherheit beurteilen können, müssen sie vergleichen können. Hierfür ist die Einteilung in Schutzklassen (I-III) vorgesehen. Diese gehen auf den unterschiedlichen Schutzbedarf der Daten ein, die im Auftrag verarbeitet werden sollen.

Die Schutzklassen erleichtern den Cloud-Nutzern grundsätzlich die Wahl eines für ihre Daten geeigneten Dienstes, weil sie auf einen Blick sehen können, ob der notwendige Schutzbedarf erfüllt ist. Beauftragt ein Unternehmen einen Dienst, der in der korrekten Schutzklasse zertifiziert ist, gelten damit vor dem Gesetz die regelmäßigen Kontrollpflichten als erfüllt. Das Zertifikat bezieht sich heute auf das Bundesdatenschutzgesetz, ist aber so gestaltet, dass es zeitgerecht an die Vorgaben der EU-Datenschutz-Grundverordnung angepasst werden kann.

2016 erhielten bereits vier Public-Cloud-Dienste ein Zertifikat nach TCDP. Dienstanbieter, die noch nicht zertifiziert sind, können auf der

Trusted-Cloud-Plattform einen Plausibilitätscheck hinsichtlich Vertrauenswürdigkeit, Transparenz, Sicherheit, Qualität und Compliance durchführen lassen. Entsprechen die Maßnahmen eines Anbieters den vielfältigen Anforderungen, wird der Dienst auf der Seite trusted-cloud.de gelistet.

Gütesiegel im Vergleich

Mit der Veröffentlichung des Anforderungskatalogs zum Cloud Computing C5 schafft das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine weitere Grundlage für die Cloud-Sicherheit. Der Katalog fasst aus Sicht des BSI Anforderungen zusammen, die Cloud-Anbieter unabhängig vom Anwendungskontext erfüllen sollten, um ein Mindestmaß an Sicherheit gegenüber ihren Kunden zu gewährleisten. Auch bei C5 handelt es sich um einen Prüfstandard. Er beinhaltet daher nur prüfbare Anforderungen und schreibt nicht vor, durch welche Maßnahmen diese zu erfüllen sind. Eine Besonderheit ist allerdings, dass Methoden und Standards der Wirtschaftsprüfer angewendet werden und ein Audit auch von diesen erfolgt. Im Unterschied zum TCDP fokussiert das BSI primär auf die Informationssicherheit beim Cloud Computing, wohingegen das TCDP als Compliance-Standard die rechtlichen Aspekte von Datenschutz und Informationssicherheit als wesentlichen Bestandteil umfassend behandelt.

Das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) legt sein Augenmerk ebenfalls auf den Datenschutz. Das ULD startete 2007 das EU-Gütesiegel EuroPriSe, das die Europäische Union im Rahmen des eTEN-Programs fördert. Seit 2014 bietet die EuroPriSe GmbH in Bonn Zertifizierungen an. Das Gütesiegel zertifiziert datenschutzkonforme IT-Produkte und IT-basierte Dienste auf der Grundlage des europäischen Datenschutzrechts, einerlei über welche Art der Cloud die Dienstleistung erfolgt.

DAS DATENSCHUTZ-ZERTIFIKAT NACH DEM TCDP AUF EINEN BLICK

- Audit durch einen unabhängigen Zertifizierungsdienst, zum Beispiel den TÜV Nord (TÜViT).
- Berücksichtigung anerkannter Standards (wie ISO 27018 und die BSI Grundschutzkataloge).
- Anbieter, die mit dem Zertifikat nach dem TCDP ausgezeichnet sind, erfüllen die gesetzlichen Anforderungen.
- Die Einteilung der Zertifikate in drei Schutzklassen gibt dem Anwender die Möglichkeit, den für seine Daten geeigneten Cloud-Dienst auszuwählen. Die Auswahl richtet sich nach dem individuellen Schutzbedarf des Unternehmens.
- Hat ein Unternehmen einen Dienst mit der korrekten Schutzklasse beauftragt, gelten vor dem Gesetz die regelmäßigen Kontrollpflichten als erfüllt (= Rechtsfolge).

Das TCDP hingegen deckt nicht alle Cloud-Dienstleistungen ab, sondern bezieht sich ausschließlich auf den Bereich Public Cloud. Durch die Prüfung der Cloud-Dienste nach Modulen erzielt eine Zertifizierung nach dem TCDP Flexibilität. Unternehmen können die zertifizierten Module sozusagen herauslösen und passend zusammenstecken. Dieses Baukastensystem dürfte sich bei den schnell wandelnden Public-Cloud-Angeboten bewähren: Unternehmen können sich so schneller dem Markt anpassen.

Dr. Hubert Jäger,
Geschäftsführer der Uniscon 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.), Ralph Novak, Martin Fuhrmann (Redaktion), Rudolph Schuster (Lektorat)

Autoren dieser Ausgabe:
Florian Bierhoff, Thomas Fritzsche, Alexander Geschonneck, Dr. Hubert Jäger, Dr.-Ing. Lutz Jänicke, Lukasz Kubik, Ramon Mörl, Dr. Holger Mühlbauer, Siegfried Müller, Andreas Philipp, Oliver Schonschek, Dr. Jörn-Marc Schmidt

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

NO ROCKET SCIENCE

Jetzt für 12,90 € bestellen!

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

heise shop
shop.heise.de

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

CONNECTED LIVING ConnFerence

//15.-16.2.2017, BERLIN //

Bis zum 4. Januar 2017 15 % Frühbucherrabatt sichern!

CONNECTED LIVING ConnFerence 2017

Der Mensch im Fokus der Digitalen Transformation

Die Digitale Vernetzung hält Einzug in unser Leben. Auf der **3. Connected Living ConnFerence** erfahren die Teilnehmer, wie sie die Potentiale der Digitalen Transformation für Ihr Unternehmen erkennen und nutzen können.

Themenschwerpunkte

- Geschäftsmodelle und Marktstrategien im Connected Life
- Future of Connected Devices
- Chancen für Telekommunikationsanbieter
- Smart Living- & Smart Working-Spaces
- Datenschutz & Security
- Mit Big Data zu Business Intelligence
- Innnovative Ansätze in Connected Health & Connected Energy
- Künstliche Intelligenz & Autonome Systeme im Connected Life

Top-Speaker beleuchten, wie sich der digitale Wandel auf Unternehmen auswirkt und liefern mögliche Strategien, um für die Zukunft gerüstet zu sein.

Teilnahmegebühr (inkl. MwSt.):

Frühbucherticket: 799,00 Euro
Standardticket: 940,00 Euro

Eine Veranstaltung von:

CONNECTED LIVING

heise Events
Conferences, Seminars, Workshops

www.heise-events.de/connected-living