iX extra September 2017
Security

Eine Sonderveröffentlichung der Heise Medien GmbH & Co. KG

IT-Sicherheit im Fokus

Trends und Produkte zur it-sa

iX extra zum Nachschlagen:
www.ix.de/extra

Wenn der Angreifer dreimal klingelt

IoT-Missbrauch und Hacken von smarten Geräten

Immer mehr Dinge des Alltags verfügen über eine Netzwerk- oder WLAN-Schnittstelle und können mit Apps vom Smartphone aus überwacht und bedient werden. Die Sicherheit kommt dabei oft zu kurz.

Zu den prominentesten Beispielen für Dinge, die angreifbar sind, gehören ohne Zweifel Überwachungskameras. Negative Schlagzeilen machte im Januar 2016 eine solche Kamera, die bei Aldi zu haben war. Die Kameras wurden, wie viele andere IoT-Geräte auch, mit einem Webinterface und bekannten Login-Daten ausgeliefert, in diesem Fall mit dem Benutzernamen „admin“ und einem leeren Passwort.

Darüber hinaus allerdings richteten sie auch noch selbstständig eine Portweiterleitung per UPnP (Universal Plug and Play) auf den Internetzugangsroutern der Anwender ein. Somit waren im Januar 2016 mehr als 10 000 solcher Kameras im Internet erreichbar, viele davon mit einem bekannten Benutzernamen und ohne Passwort. Finden und zählen lassen sich solche vernetzten Dinge mit der Suchmaschine Shodan (Abb. 1), die dauerhaft das Internet nach „Dingen“ durchsucht und diese in ihrer Datenbank speichert. Jeder interessierte Internetnutzer kann dann über die Shodan-Website beispielsweise nach IoT-Geräten in seiner Umgebung suchen und von dort zum Beispiel direkt auf erreichbare IP-Kameras im Haus seiner Nachbarn zugreifen.

Problem Schwachstellen in Geräten

Das Problem reicht schon Jahre zurück und auf Sicherheitskonferenzen wurden schon IP-Kameras vorgeführt, die aufgrund von Schwachstellen in der Firmware kompromittiert werden können. Die bekannten Login-Namen und Default-Passwörter solcher Geräte waren auch der primäre Verbreitungsweg des Mirai-Botnetzes. Dieses verbreitete sich wie ein Wurm von IoT-Gerät zu IoT-Gerät weiter, um dann von diesen Geräten aus (D)DoS-Traffic mit bis dahin noch nie dagewesenem Volumen zu erzeugen. Eines der Opfer, der Sicherheitsblogger Brian Krebs, wurde beispielsweise mit mehr als 650 GBit/s getroffen und seine Website war nicht mehr erreichbar.

Der Missbrauch von IoT-Geräten ist aber nur eines von vielen Problemen. Oft führen Schwachstellen in vernetzten Geräten auch zu Gefährdungen für das gesamte Heimnetzwerk. Ein Beispiel hierfür ist die Video-Türklingel einer bekannten Firma. Sie wird einfach neben der Haustüre befestigt, und der Besitzer kann dann von seinem Smartphone aus sehen, wer vor der Türe steht. Dazu wird die Türklingel in das private WLAN des Besitzers integriert. Doch Zugangsdaten und Schlüssel für dieses private WLAN ließen sich einfach aus der Klingel auslesen – durch Öffnen des Gehäuses mit einem Schraubenzieher und Drücken des Reset-Knopfs der Klingel, fanden Forscher heraus. Die Klingel baut ein eigenes WLAN-Netz mit bekannten Zugangsdaten auf. Der Angreifer kann sich mit diesem WLAN verbinden und über die Weboberfläche der Klingel die WLAN-Schlüssel des Besitzers auslesen. Der Hersteller behob zwar die Schwachstelle umgehend, aber die Schlüssel für das private WLAN bleiben in der Klingel gespeichert. Ein Restrisiko bleibt also.

Auch im Bereich von Beleuchtungstechnik gab es zahlreiche spektakuläre Schwachstellen bei IoT-Geräten. Im Sommer 2016 zeigten mehrere Forscher, wie sich ein Wurm per Funk von Lampe zu Lampe bewegen kann und dabei die Firmware der Lampen austauscht. Auf der Sicherheitskonferenz Black Hat führten sie ein Video vor, in dem man eine ferngesteuerte Drohne beobachten kann, die sich einem Bürogebäude nähert und dort die Lampen infiziert, bis diese nur noch SOS blinken. Die Forscher verwendeten dafür unter anderem einen Seitenkanal-Angriff, um den geheimen Signaturschlüssel für Firmware-Updates aus der Firmware der Lampen auszulesen. Der Fall ist ein schönes Beispiel dafür, dass sich geheime Schlüssel kaum sicher in IoT-Geräten speichern lassen.

In der Unterhaltungselektronik sieht es nicht besser aus. Ein moderner Fernseher ist heute in der Regel automatisch ein Smart-TV, und damit steckt ein Computer – meist mit Linux beziehungsweise Android – im Gerät. Der smarte Fernseher ist mit dem Internet verbunden, kann über Smartphone-Apps gesteuert werden und verwendet zur Gestensteuerung Sensoren, die das Wohnzimmer überwachen. Schwachstellen in veralteten Netzwerkdiensten oder fehlende Sicherheitsupdates des Betriebssystems sind immer wieder die Einfallstore.

Spannend wird der Sicherheitsaspekt von IoT-Geräten besonders, wenn die Geräte gerade für die Sicherheit verkauft werden. Analysen haben in den letzten Jahren immer wieder Sicherheitslücken in elektronischen Türschlössern oder Alarmanlagen gefunden, die sich mit

Mit der Suchmaschine Shodan lassen sich vernetzte Gegenstände im Internet der Dinge finden – das nutzen Sicherheitsexperten, aber auch Cyberkriminelle (Abb. 1).

Smartphone-Anwendungen steuern lassen.

Betrachtet man die vielen Beispiele für unsichere IoT-Geräte mit etwas Abstand, dann sind Zusammenhänge und immer wieder ähnliche Probleme zu erkennen. Beim Design solcher Geräte spielt Informationssicherheit in der Regel keine oder eine sehr untergeordnete Rolle. Viel wichtiger scheinen den Herstellern der Funktionsumfang, ein attraktives Gehäuse und der Preis zu sein. Der Käufer eines Smart-TV wählt diesen ebenso wenig unter Sicherheitsaspekten, sondern eher anhand der verfügbaren Features, der Bildqualität und des Preises aus. Gleiches gilt für die meisten anderen IoT-Geräte. Daher ist das Verhalten der Hersteller zumindest teilweise nachvollziehbar.

Funktion noch immer vor Sicherheit

Dies führt dazu, dass die Hardware der Geräte oft nur minimale CPU-Kapazitäten bereitstellt. Das senkt die Kosten, den Stromverbrauch und damit auch die Wärmeentwicklung. Bei Geräten mit Akkubetrieb halten die Akkus deutlich länger.

Das impliziert jedoch auch, dass kaum rechenintensive Funktionen auf den Geräten selbst ausgeführt werden können. Sie müssen auf einen Server oder ein zusätzliches Basis-Gerät ausgelagert werden. Wenn nun aber der Kunde zusätzlich zu einem IoT-Gerät noch einen passenden Server kaufen müsste, ist das nicht gerade verkaufsfördernd. Daher bieten die Hersteller solche Funktionen bevorzugt als Cloud-Services an, also als Dienst in einem Rechenzentrum, den die Geräte über das Internet erreichen.

Ein weiterer Grund für Nutzung von Cloud-Services ist, dass die Benutzer das Gerät ohne zusätzliche Konfiguration von IP-Adressen oder anderen Parametern sofort verwenden können. In einem individuellen Heimnetzwerk ist das nur mit fehleranfälliger Autokonfiguration möglich. Die Alternative ist auch hier ein Cloud-Dienst, dessen Adresse fest im IoT-Gerät und in der zugehörigen Smartphone-App hinterlegt ist. Beide öffnen eine ausgehende Verbindung zum Cloud-Service des Herstellers und können über diesen zentralen Punkt miteinander kommunizieren.

Bei IoT-Sicherheit geht es daher nicht nur um die Geräte selbst. Auch die Smartphone-Apps zur Steuerung, die zugehörigen Cloud-Services sowie die Kommunikations- und Vertrauensbeziehungen zwischen diesen drei Komponenten sind typische Angriffspunkte. In vielen Fällen war beispielsweise die Kommunikation zwischen dem Smartphone und dem IoT-Gerät oder der Cloud über einen Man-in-the-middle-Angriff manipulierbar oder es konnten versteckte Passwörter aus dem Code der Smartphone-App extrahiert werden.

Die Berichte über Sicherheitsdefizite eines IoT-Gerätes beginnen oft damit, dass ein Angreifer Daten, die auf dem Gerät gespeichert sind, auslesen kann oder dass er erweiterten Zugriff auf das Gerät mit den Rechten eines Administrators bekommt. Dadurch kann er zunächst die Funktionsweise und die Kommunikationsprotokolle in allen Details einsehen und weitere Schwachstellen ausfindig machen.

Ein weiterer typischer Angriffspunkt ist die Firmware der Geräte. Hacker und Sicherheitsforscher lesen die Firmware über Debug-Schnittstellen aus den Geräten aus und extrahieren geheime Schlüssel aus Firmware-Updates oder über Seitenkanal-Angriffe aus laufenden Geräten. Ein praktisches Werkzeug für die Analyse von Firmware-Update-Dateien ist beispielsweise die kostenlose Software Binwalk. Sie analysiert eine unbekannte Firmware-Datei, indem sie nach bekannten Mustern für bestimmte Dateien, Archive, Dateisysteme und Ähnliches sucht. Diese werden dann automatisch extrahiert beziehungsweise entpackt. Gerade bei Geräten, die mit Linux arbeiten, enthalten die Firmware-Updates ganze Dateisysteme. Daraus kann man dann leicht eine Passwortdatei extrahieren und die dort gespeicherten Passwörter per Brute Force angreifen.

Sicherheits-GAU: Überwachungskameras werden mit dem Benutzernamen „admin“ und ohne Passwort geliefert (Abb. 2).

Trotz der einfachen Angriffstechniken vertrauen immer noch viele Hersteller auf versteckte Schlüssel in den Geräten als Grundlage für ihre Sicherheitsfunktionen. Das mag einerseits an fehlendem Fachwissen liegen, andererseits sind IoT-Geräte oft mit minimaler Hardware ausgestattet, sodass Public-Key-Verfahren sich nicht sinnvoll implementieren lassen. Knappe CPU-Ressourcen auf IoT-Geräten sind einer der Gründe, warum oft zulasten der Sicherheit auf Public-Key-Verschlüsselung verzichtet wird und stattdessen symmetrische Schlüssel in den Geräten versteckt werden.

Security by Design

Der Weg zu sicheren IoT-Geräten muss in der Designphase beginnen. Schon hier werden die Weichen gestellt, denn Anforderungen der Sicherheit an die Hardware können sich durchaus auf den Stromverbrauch und damit die Dimensionierung von Akkus und die Größe des Gehäuses auswirken.

Ein erster Schritt sollte deshalb eine Bedrohungs- und Risikoanalyse für das geplante Gerät sein. Dabei werden alle Bedrohungsszenarien aufgelistet und mit Eintrittswahrscheinlichkeit und möglichem Schaden bewertet. Auf dieser Grundlage können die Verantwortlichen dann entscheiden, welche Risiken akzeptabel sind und welche mit geeigneten Maßnahmen zu minimieren oder zu vermeiden sind.

Ebenso muss Sicherheit ein Bestandteil des kompletten Entwicklungsprozesses sein. Dazu gehören beispielsweise Richtlinien für die sichere Entwicklung und Schulungen. Aber selbst wenn Entwickler geschult und sensibilisiert sind, machen Menschen Fehler. Deshalb ist auch eine regelmäßige Sicherheitsüberprüfung des Codes notwendig. Da sich Schwachstellen dennoch nicht ausschließen lassen, müssen Hersteller ein Konzept zum Umgang mit Schwachstellen haben, wenn Geräte bereits bei den Kunden sind: Dies beginnt mit dem Melden von Schwachstellen. Selbstverständlich muss ein Prozedere vorgesehen sein, die Firmware von IoT-Geräten bei Bedarf auch nach dem Verkauf zu aktualisieren, um kritische Fehler zu beheben.

Erst wenn den Herstellern klar wird, dass Unsicherheit auf Dauer noch viel mehr Geld kostet, wird sich das Gesamtbild des IoT-Marktes in Bezug auf Security ändern. Erfreulicherweise gehen hier einige deutsche Anbieter mit gutem Beispiel voran und so gibt es Grund zur Hoffnung, dass die Tendenz am Markt doch zu sichereren IoT-Geräten geht. (ur)

Stefan Strobel ist Buchautor sowie Gründer und Geschäftsführer des IT-Sicherheitshauses cirosec.

Wer bin ich?

Identität im Internet of Things

Grundsätzlich müssen vernetzte Dinge kein unkalkulierbares Sicherheitsrisiko darstellen. Dann muss die Sicherheit der Kommunikation, Identifikation und Autorisierung von Anfang an mitgedacht werden. Das Internet der Dinge oder IoT (Internet of Things) schließt immer mehr vernetzte „Dinge“ ein – von einfachen Endgeräten für Verbraucher wie Fitness-Armbändern über komplexe Systeme wie das vernetzte Fahrzeug bis hin zu vernetzten Systemen in der Produktion.

Bezüglich der Sicherheit im IoT ist eine der entscheidenden Fragen, ob Dinge eine Identität haben. Vom Standpunkt des Identitäts- und Berechtigungsmanagements, das die Grundfragen „Wer (oder was) darf worauf zugreifen?“ regelt, ist die Antwort klar: Alles, was auf andere Systeme zugreifen kann, hat eine Identität.

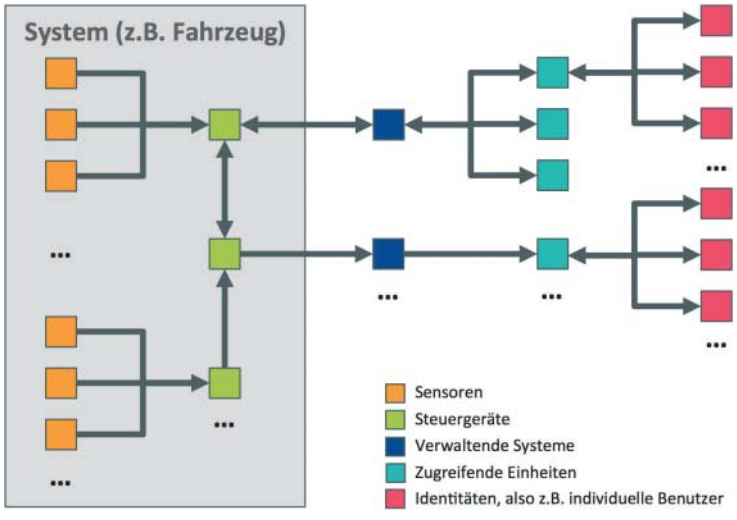
Das sind natürlich die Benutzer, aber auch Anwendungen, die direkt mit anderen Anwendungen kommunizieren und dafür heute beispielsweise oft technische Benutzerkonten verwenden. Es sind Geräte, die von Dingen Informationen anfordern, wie Apps auf einem Smartphone in Verbindung mit Fitness-Armbändern. Es können aber auch autonom agierende Dinge in einem größeren System wie einem vernetzten Fahrzeug sein, die mit anderen Dingen kommunizieren. Daher muss der Begriff der Identität auf Dienste, Geräte und Dinge ausgeweitet werden.

Nicht jedes Ding hat eine Identität

Allerdings ist es nicht ganz so einfach. Denn beispielsweise Sensoren, die ausschließlich über definierte Steuergeräte verwaltet werden und nicht direkt angesprochen werden können, benötigen zumindest aus Sicht eines übergeordneten Identitätsmanagements für das Internet der Dinge keine eigenständige Identität, wohl aber aus Sicht ihres Steuergeräts. Letztlich hängt es sowohl von der technischen „Intelligenz“ der Dinge als auch von ihrer Anbindung ab, inwieweit ein Identitätsmanagement für IoT diese berücksichtigen muss.

Es gibt aber noch weitere fundamentale Unterschiede zwischen den Dingen und dem klassischen Blick auf Nutzer, die sich in irgendeiner Form – meist auch heute noch mit Benutzername und Kennwort – authentifizieren. Für viele Geräte ist nur ein lesender Zugriff möglich. Sensoren stellen zwar oft Daten bereit, können aber nicht gezielt gesteuert werden. Aber auch getrennte Wege sind denkbar, teilweise sogar über eine physische Trennung, um aktiv Dinge zu steuern und für das Auslesen der Daten. Die Steuerung ist typischerweise für die Sicherheit wesentlich kritischer als das Auslesen von Daten.

Die englische Sprache unterscheidet zwischen „Safety“ und „Security“, also Produktions-/Produktsicherheit und IT-Sicherheit. Diese beiden Bereiche hängen bei vernetzten Dingen sehr eng zusammen. Doch ist es essenziell wichtig, sie getrennt und sorgfältig zu behandeln.



Quelle: KuppingerCole

Selbst in einer stark abstrahierten Darstellung ist Identitätsmanagement für vernetzte Dinge oft sehr komplex, wie beispielsweise bei Fahrzeugen.

Dinge authentifizieren sich anders

Die Authentifizierung erfolgt bei Dingen anders als bei der Interaktion mit Menschen. Im einfachsten Fall sind beispielsweise Geräte-IDs vorhanden, denen vertraut wird. Diese sind jedoch potenziell einfach zu fälschen, sodass dies kein besonders sicheres Verfahren ist. Dennoch ist es zum Beispiel für die Kopplung von Geräten und Dingen oder von Geräten mit Systemen durchaus üblich, wobei in der Kopplungsphase oft noch einfache PINs zusätzlich genutzt werden, so etwa bei der Bluetooth-Verbindung zwischen einem Smartphone und dem Multimedia-System eines Autos.

Bei höheren Sicherheitsanforderungen kommen dagegen für die Kommunikation häufig eine zertifikatsbasierte Authentifizierung oder digitale Signaturen zum Einsatz. Damit lassen sich beispielsweise Steuergeräte so konfigurieren, dass sie nur Änderungsanforderungen von definierten Systemen akzeptieren.

Zugriffssteuerung im IoT

Ein solches Verfahren wirkt im ersten Moment eher umständlich, weil es scheinbar wenig flexibel ist. Tatsächlich hängt die Flexibilität aber nicht vom Authentifizierungsverfahren ab, sondern davon, wie differenziert das Autorisierungskonzept des Dings ist – ob nun Sensor, Steuergerät oder ein anderes Ding – und in welchem Maß dieses sich steuern lässt. Grundsätzlich lässt sich auch in einem solchen Ansatz ein differenziertes Modell aufbauen.

Häufig erfolgt die Kommunikation über zwischengeschaltete Systeme, die beispielsweise Da-

ten von sehr vielen Dingen wie Fitness-Armbändern, bestimmten Komponenten von Fahrzeugen wie Unfalldatenrekorder et cetera sammeln und dann als Schnittstelle zu anderen Systemen und Nutzern dienen. Damit wird die Kommunikation stark zentralisiert, was die Verwaltung von Identitäten und ihren Berechtigungen deutlich vereinfacht und auf eine andere Ebene verlagert, bei der es sich wieder um gewohnte IT-Systeme handelt.

Statt also etwa unterschiedlichsten relevanten Organisationen und ihren Nutzern Zugriff auf vernetzte Fahrzeuge zu erlauben, erfolgt die Kommunikation zentralisiert. Das reduziert die Komplexität der Kommunikation und damit auch des Managements von Zugriffen, denn es kommunizieren nur einzelne Systeme mit bestimmten Komponenten in den verschiedenen Dingen. Der Versuch, auf der Ebene der Dinge zu steuern, welche lesenden und schreibenden Zugriffe in welchen Situationen erlaubt sein sollen, wäre eine kaum zu bewältigen Herausforderung für das Identitäts- und Zugriffsmanagement – man denke beispielsweise bei Fahrzeugdaten an die Zugriffe von Polizeibehörden unterschiedlicher Länder, an Fahrer und Insassen über ihre Smartphones, an den Hersteller, die Vertrags- und andere Werkstätten, Versicherungen sowie weitere unzählige Parteien.

Entsprechend sicher müssen die zentralen Systeme sein. Sie benötigen eine ausgefeilte Steuerung der Autorisierung, um regeln zu können, wer was durchführen darf, und um sicherzustellen, dass es nicht zu unautorisierten Änderungen kommt. Die Zentralisierung reduziert auf der einen Seite die Komplexität der Zugriffssteuerung, stellt andererseits aber auch ein Risiko dar, weil es hier zu Fehlern kommen kann, die sich auf viele Dinge auswirken.

Ohne umfassende Standards und Konzepte für die Softwareentwicklung auf der Ebene der Dinge, die eine zentrale Verwaltung von Identitäten und den Richtlinien für die Zugriffssteuerung mit einer dezentralen Durchsetzung verbinden, sind Unternehmen aber im Moment noch auf solche Ansätze angewiesen, die über zentrale Komponenten oder eben nur mit einfachen Identifikations- und Autorisierungsansätzen zwischen Geräten und Dingen arbeiten.

Sicherheitsrisiko IoT?

Mit durchdachten Konzepten für die Absicherung der Kommunikation zwischen zentralen Systemen und den Dingen lässt sich ein hohes Maß an Sicherheit erreichen, wenn die Identifikation der zentralen Systeme sichergestellt und die Kommunikation gut geschützt ist. Hier hängt dann alles davon ab, wie ausgefeilt das Sicherheitsmodell der zentralen Systeme ist.

Wichtig ist vor allem, schon vor der Vernetzung von Dingen zu überlegen, wie diese eine Identität erhalten können und wie sie insbesondere auch diejenigen Systeme, Geräte und anderen Dinge identifizieren sollen, mit denen sie kommunizieren. Des Weiteren sollte auch das Patch-Management von Beginn an berücksichtigt werden.

Dabei ist es oft der bessere Ansatz, zwischen die Dinge und die Menschen noch Systeme zu stellen und die Kommunikation zu kanalisieren. Denn damit lässt sich die Komplexität des Managements von Identitäten und Zugriffsberechtigungen auf den vernetzten Dingen wesentlich reduzieren.

Martin Kuppinger ist Gründer des Analystenunternehmens KuppingerCole und als Principal Analyst verantwortlich für den Bereich KuppingerCole Research.

Wir sind alle erpressbar

Ransomware: Vergangenheit, Gegenwart und Zukunft

Die Bedrohung durch Ransomware ist größer denn je und die Zahl der Angriffe steigt seit Jahren kontinuierlich. Ein Wundermittel dagegen gibt es nicht, doch Wissen über die Malware und einige Schutzmaßnahmen können helfen.

Den Begriff Ransomware oder digitale Erpressersoftware kennen alle, und jeder Computernutzer, jeder Sicherheitsbeauftragte und jede IT-Abteilung fürchtet die Bedrohung. Prominente Fälle von Angriffen, die finanzielle Schäden nach sich zogen, betrafen das Neusser Lukas-Krankenhaus oder die Stadt Dettelbach (dieser und weitere Links sind über „Alle Links“ im blauen Kästchen zu finden). Wie brisant die Bedrohung durch Ransomware ist, zeigen Zahlen einer SonicWall-Studie: Erkannten die Sicherheitsforscher 2015 noch 3,8 Millionen Angriffe, so stieg diese Zahl 2016 auf 638 Millionen – 167 Mal mehr Angriffe als ein Jahr zuvor.

Das Prinzip dieser Malware, Daten oder Rechner als Geisel zu nehmen, ist bereits 28 Jahre alt. Der wahrscheinlich erste Verschlüsselungstrojaner machte 1989 als „AIDS-Trojaner“ Schlagzeilen, denn er wurde damals mithilfe von 20 000 infizierten Disketten auf einer AIDS-Konferenz der Weltgesundheitsorganisation verteilt. Im Anschluss an die Infektion eines PCs wurden nach dem 90. Systemstart Dateien verschlüsselt. Das damalige Lösegeld lag bei 189 US-Dollar – zu versenden per PO Box.

Am Anfang war der Sperrbildschirm

Erste größere mediale Aufmerksamkeit erhielt in Deutschland der sogenannte BKA- oder Bundestrojaner. Er schüchterte Nutzer mit der Information ein, auf ihrem Rechner sei illegales Material gefunden worden und ein Bußgeld sei fällig, andernfalls werde der Rechner mit einem sogenannten Sperrbildschirm blockiert.

Der Boom der Ransomware startete vor rund fünf Jahren mit CryptoLocker. Mit ein Grund für dessen Erfolg waren die Nutzung der 2008 entwickelten Kryptowährung Bitcoin und die Möglichkeiten der Dateiverschlüsselung. Die digitale Währung gewährte den Tätern eine gewisse Anonymität im Zahlungsverkehr, was die Fahndung deutlich erschwerte und damit das Risiko, entdeckt zu werden, verringerte.

Zum Erfolg trug auch die teilweise erfolgreiche Wiederherstellung der verschlüsselten Dateien nach Zahlung des Lösegelds bei. Und das publizierten die Täter mit gezielten (Falsch-)Meldungen in den sozialen Netzwerken wie Twitter. Auch die unglückliche Wiedergabe einer FBI-Meldung (siehe „Alle Links“) in deutschen Medien erzeugte den (falschen) Eindruck der oft erfolgreichen

Entschlüsselung, verbunden mit einer Zahlungsempfehlung des FBI. Da häufig nur ein relativ niedriges Lösegeld gefordert wurde (in der Regel unter 500 Euro), führte dies dazu, dass insbesondere kleine und mittelständische Unternehmen bereit waren, das Lösegeld zu zahlen, um die verlorenen Daten zurückzuerhalten. Aber auch für den privaten Benutzer war das Lösegeld im Austausch gegen die Urlaubsfotosammlung eine akzeptable Option. Dadurch erhielt die Tätergruppe weitere Mittel, um nachfolgende Angriffe zu finanzieren.

Insbesondere durch den steigenden Bitcoin-Kurs entwickelte sich Ransomware zu einem sehr lukrativen Geschäftsmodell. Die Folge war ein dramatischer Anstieg der Bedrohungen mit einer Vielzahl verschiedener Verschlüsselungstrojaner, die nahezu alle Betriebssysteme und Plattformen attackieren konnten.

Die ersten Wellen großen Ausmaßes gab es 2015. Viele Benutzer wurden Opfer von TeslaCrypt oder Fusob, der für 93 % der Ransomware-Angriffe auf Smartphones verantwortlich war. Erstmals zeigten sich die Schwächen des signaturbasierten Virenschutzes deutlich. Die Angreifer waren durch gezielte Verbreitung und regelmäßige „Patches“ der Ransomware den Antivirenherstellern immer um ein paar Stunden bis Tage voraus. Prominentes Beispiel ist GoldenEye, der von namhaften Antivirenherstellern erst mit mehreren Tagen Verzögerung erkannt wurde („Alle Links“).

Angriffsvektoren für die digitale Erpressung

Technisch gesehen nutzen die Ransomware-Varianten die komplette Klaviatur aktueller Angriffsvektoren. Oft handelt es sich um Social-Engineering-Angriffe mit E-Mails, die zum Öffnen von Dateien verleiten sollen. Auch die längst totgesagten Makroviren wurden reaktiviert, um Schadcode auszuführen. Teilweise wird der Schadcode von Loader-Modulen erst im Bedarfsfall nachgeladen, um eine Entdeckung zu erschweren.

Aber auch beim normalen Surfen werden durch Drive-by-Downloads und Exploiting Schadprogramme verteilt und gestartet. Hierzu nutzen die Kriminellen teilweise Werbebanner oder im Vorfeld gehackte Content-Management-Systeme.

Entschlüsselung der „gekaperten“ Daten wird meistens garantiert – ob sie auch erfolgt, ist eine andere Sache.

Quelle: Trend Micro

Mehr Opfer – mehr Gewinn

Mit dieser Vielfalt der Angriffsvektoren erreichen die Täter eine hohe Anzahl an Infektionen und somit eine Maximierung des Gewinns durch Lösegeld. Sobald sie in einem System eingedrungen sind, starten einige Varianten eine selbstständige Suche im LAN nach weiteren Opfern.

Auch sind neue Geschäftsmodelle entstanden wie „Ransomware als Service“ („Alle Links“), um die Verteilung Dritten zu überlassen und an einer Provision zu verdienen. Zudem werden im Darknet komplette Ransomware-Kits angeboten.

Die unterschiedlichen Schädlinge lernen voneinander und übernehmen Features wie das kostenlose Entschlüsseln einer einzelnen Datei zu Demonstrationszwecken. Auf technischer Ebene setzte sich die Verschlüsselung mit AES 256 durch, da andere in der Regel schnell durch die Antivirenindustrie erfolgreich aufgebrochen werden konnten.

Sicherlich wird die digitale Erpressersoftware künftig mehr andere bekannte Malware-Funktionen einbinden. Neue Infektionswege werden erschlossen werden. Denkbar ist beispielsweise die Nutzung von Fernwartungszugängen, Update-Mechanismen und vieles mehr.

Die Kampagnen werden kleiner und gezielter. Zielgerichtete Angriffe auf große Finanzorganisationen etwa sind für die Angreifer doppelt lukrativ, denn einerseits ist die Bereitschaft (und die Möglichkeit), Lösegeld zu zahlen, im Finanzsektor hoch, andererseits wird der Kurs der Kryptowährungen stetig nach oben getrieben. Gelingt es Ransomware, sich gezielt in kritische Infrastrukturen einzuschleusen, sind massive infrastrukturelle Schäden zu erwarten.

Die Ziele sind mannigfaltig und teilweise leichte Beute. Beispielsweise ist es bei Spezialanwendungen in der Medizin und in der Verteidigung aus Zulassungsgründen nur mit einem deutlich höheren zeitlichen und technischen Aufwand möglich, die notwendigen Sicherheitsupdates einzuspielen, Systeme zu aktualisieren oder Systemupgrades durchzuführen. Dies kann zu längeren Zeiten der Verwundbarkeit der Systeme führen. Somit sind Schwachstellen leichter auszunutzen. Gleichzeitig ergeben sich hier ganz neue Erpressungs- und Bedrohungsszenarien.

Ransomware wird wahrscheinlich auch als Waffe eingesetzt werden. Die Wirkung auf die Infrastruktur des öffentlichen Lebens bei gezielten Angriffen ist enorm. Man denke nur an die Androhung einer Manipulation von Stellwerken im Bahnverkehr. Die zerstörerische Wirkung, die Terroristen und gegebenenfalls auch fremde Regierungen im Rahmen eines Cyberkriegs entfalten könnten, ist ebenfalls nicht zu unterschätzen.

Wohin geht die Reise?

Für die organisierte Kriminalität ist die Kombination mit anderen Angriffszielen denkbar. So bietet es sich an, Dateien vor der Verschlüsselung auf die Inhalte zu untersuchen und diese gegebenenfalls abzugreifen (Personaldaten, Kreditkartendaten, Login-Daten et cetera). Ähnliches erfolgte bereits mit dem Abgreifen von Bitcoin-Kontoständen bei Ransomware-Nutzern.

Die benötigten Schwachstellen zum Einschleusen von Ransomware wird es auch künftig geben. Besonders gefährlich sind die Schwachstellen in den Händen der Nachrichtendienste. Neben dem direkten Ausnutzen

durch die jeweiligen Staaten bieten sie bei Bekanntwerden ein gigantisches Angriffspotenzial. Das führten die geleakten NSA-Tools und das darauf aufsetzende NotPetya plastisch vor Augen.

Wie man Infektionen vorbeugt

Die Antivirenindustrie arbeitet stetig an neuen Erkennungsmethoden und einem globalen Abgleich ihrer Erkenntnisse (zur Erkennung siehe Tabelle „Auswahl von Anbietern und Lösungen aus dem Bereich Breach Detection"). Neben signaturbasierten und heuristischen Methoden kommen mittlerweile insbesondere auch Verhaltensanalysen zum Einsatz. Technische Lösungen wie Sandboxing zur Durchführung und Auswertung von Laufzeittests erhöhen die Erkennungsrate bei unbekannter Schadsoftware. Allerdings entwickeln die Malware-Autoren häufig Techniken, um solche Testumgebungen zu erkennen und ihrer Schadsoftware für diesen Fall ein anderes Verhalten mitzugeben.

Generell können Black-/Whitelisting-Ansätze für das Ausführen von Programmen helfen, das Risiko zu reduzieren. Im Idealfall werden alle ausführbaren Dateien in einer Whitelist verwaltet und vor jedem Programmstart wird geprüft, ob ein Eintrag für die entsprechende Datei vorhanden ist. Schadprogramme werden somit nicht ausgeführt.

Neben rein technischen Erkennungsmaßnahmen muss aber auch die letzte Verteidigungslinie – der Nutzer – gestärkt werden. Dies funktioniert nur über eine regelmäßig Sensibilisierung und Schulung der Mitarbeiter. Diese Aus- und Weiterbildungsmaßnahmen sollten Schutzmaßnahmen für den privaten Gebrauch mit den firmeneigenen Weisungen verbinden. Bei Umsetzung eines solchen Konzepts zeigen die Erfahrungswerte ein deutlich erhöhtes Risikobewusstsein der Mitarbeiter. Sie werden seltener aus Neugierde eine E-Mail anklicken oder den vor dem Werkstor gefundenen USB-Stick ohne Kontrolle anschließen. Letztendlich entscheidet oft der Anwender darüber, ob eine Ransomware ihr Unwesen treiben kann oder nicht.

Sicherheit braucht einen Plan

Unerlässlich für Unternehmen, auch im Mittelstand, ist die Einrichtung eines aktiven IT-Sicherheitsmanagements nach BSI oder ISO 2700x. So ist die Entwicklung vom bloßen Beschaffen von Firewalls, Antivirensoftware und Datensicherungen hin zu einem ganzheitlichen, strukturierten und bedarfsgerechten Sicherheitsniveau für alle Geschäftsprozesse und Informationen in den IT-Systemen möglich.

Zu Beginn bedarf es einer ganzheitlichen Strukturanalyse (der Informationen und Systeme) des Unternehmens sowie einer Schutzbedarfsanalyse. Dabei zeigt sich, wo die unterschiedlichen Daten gesichert und welche Übertragungswege benutzt werden. Danach kann eine Sicherheitsstrategie aufgesetzt werden. Denn das beste und teuerste Sicherungsprogramm nützt nichts, wenn die Sicherung im gleichen Raum liegt und zum Beispiel bei Feuer ebenfalls vernichtet wird. Oder wenn Forschungsdaten zwar ausgelagert sind, aber auf dem unverschlüsselten Übertragungsweg jeder die Daten mitlesen kann. Auch aktiv angeschlossene Datenspeicher zur Sicherung kommen in der Praxis (leider) häufig vor, sodass eine „gute" Ransomware nicht nur die Arbeitsdaten, sondern gleichzeitig auch die Datensicherung verschlüsseln kann. Diese konzeptionellen Fehler lassen sich im Rahmen eines Informationssicherheitsmanagementsystems (ISMS) erkennen und beseitigen.

Das ISMS bietet auf Managementebene verankert ein an die Unternehmensprozesse angepasstes Risikomanagement mit umfangreichen Maßnahmenkatalogen zu den einzelnen Gefährdungen und erhält die erreichte Informationssicherheit aufrecht. Unerlässlich ist hierfür aber die Anerkennung des strategischen Ziels „Informationssicherheit" durch die Unternehmensführung und deren Übernahme der Verantwortung, da sonst die Maßnahmen aus Kosten-, Personal- oder Bequemlichkeitsgründen regelmäßig nicht in dem erforderlichen Maße umgesetzt werden.

Alles auf Anfang

Kommt es doch zu einer erfolgreichen Infektion, hilft nur das Einspielen des Backups. Dies bedingt ein schlüssiges Backup-Konzept mit entsprechend langer Vorhaltedauer und Medienbrüchen. Die Zahlung von Lösegeld sollte man gar nicht erst in Erwägung ziehen, da das Geld reinvestiert und zur Entwicklung neuer Varianten genutzt wird.

Für Betroffene bietet das Portal https://www.nomoreransom.org/ eine Sammlung von Entschlüsselungstools für die unterschiedlichsten Ransomware-Varianten. Das Portal basiert auf einer Kooperation der niederländischen Ermittlungsbehörden mit Antivirenherstellern. Sobald im Rahmen von Ermittlungsverfahren Schlüssel zur Entschlüsselung bekannt werden, werden diese über No-More-Ransom der Öffentlichkeit zugänglich gemacht.

Stephan Amelang ist IT-Sicherheitsbeauftragter des Luftfahrtamtes der Bundeswehr.
Thomas Stasch ist IT-Sicherheitsbeauftragter im Zweckverband civitec, geschäftsführender Gesellschafter der ProKoSi GbR.

Auswahl von Anbietern und Lösungen aus dem Bereich Breach Detection

Anbieter	Produkt	Webseite
AhnLab	MDS	global.ahnlab.com/site/product/productSubDetail.do?prodSeq=15231
Check Point	Next Generation Threat Prevention Appliance	https://www.checkpoint.com/products-solutions/threat-prevention/
Cisco	Advanced Malware Protection	https://www.cisco.com/c/de_de/products/security/amp-appliances/index.html
FireEye	EX-3400 v7.1.6, NX-4400 v7.5.3	www.fireeye.de
Fortinet	FortiSandbox	https://de.fortinet.com/products/sandbox/fortisandbox.html
IBM	XGS	https://www.ibm.com/us-en/marketplace/network-security
Lastline	Breach Detection Platform	https://www.lastline.com/tag/lastline-breach-detection-platform/
McAfee	Advanced Threat Defense	https://www.mcafee.com/de/products/advanced-threat-defense.aspx
Palo Alto Networks	Next Generation Security Platform	https://www.paloaltonetworks.de/products
SecureWorks	Enterprise Security Counter Threat	https://www.secureworks.co.uk/counter-threat-platform
SonicWall	Capture Advanced Threat Protection	https://www.sonicwall.com/en-us/products/firewalls/security-services/capture-advanced-threat-protection
Sophos	InterceptX	https://www.sophos.com/en-us/products/intercept-x.aspx
Symantec	Advanced Threat Protection	https://www.symantec.com/products/advanced-threat-protection
Trend Micro	Deep Discovery Inspector	www.trendmicro.de/deep-discovery/index.html

Die Uhr tickt

Die Europäische Datenschutz-Grundverordnung – was Unternehmen ändern müssen

Ab Mai 2018 gelten europaweit neue Regeln für den Datenschutz. Das bringt Veränderungen mit sich, die alle Unternehmen betreffen.

Am 25.05.2018 tritt die Europäische Datenschutz-Grundverordnung oder kurz GDPR (General Data Protection Regulation) in Kraft. Die GDPR ist eine Verordnung („Regulation“) und keine Direktive wie die bisherige europäische „Directive 95/46/EC“ zum Schutz von Personen bezüglich der Verarbeitung der persönlichen Daten und der freien Weitergabe solcher Informationen. Eine Direktive umfasst nur Vorgaben für die Umsetzung in nationales Recht. Erst bei Umsetzung ist sie wirksam. Eine Verordnung hingegen steht über nationalem Recht und wird unmittelbar wirksam.

Die GDPR gilt für alle Organisationen, die Daten von Personen verarbeiten, die in der EU ansässig sind. Für die Compliance zur neuen Verordnung hat es keine Bedeutung, ob es sich um ein Unternehmen handelt, das rechtliche Einheiten in der EU hat oder nicht, sondern es gilt vielmehr das Kriterium, ob die Firma Daten von EU-Bürgern verarbeitet.

Zukünftig drastische Strafen

Die Durchsetzung der GDPR übernehmen die nationalen Datenschutzbehörden und gegebenenfalls regionale Stellen. Bei Verstößen kommt es im Regelfall erst zu einer Verwarnung. Mögliche Strafen sind signifikant und betragen bis zu 20 Millionen Euro oder 4 % des gruppenweiten jährlichen Umsatzes, je nachdem, welcher Betrag höher ist. Diejenigen, deren personenbezogene Daten verarbeitet werden, sind berechtigt, Beschwerde bei den zuständigen Stellen einzulegen. Die GDPR enthält eine Vielzahl von Veränderungen im Vergleich zur bisherigen Direktive, viele davon mit erheblichen Auswirkungen. Dazu gehört insbesondere die explizite Zustimmung der Personen zur Nutzung ihrer Daten. Personenbezogene Daten sind dabei nicht nur solche, die explizit mit dem Namen einer Person verknüpft sind, sondern generell solche, die eine Identifikation von Personen ermöglichen könnten. Das ist eine sehr weite Definition.

Grundsätzlich ist eine Zustimmung zur Verarbeitung dieser Daten erforderlich, es sei denn, es bestehen Verträge, in denen dieses Einverständnis bereits geregelt ist. Diese muss aus freiem Willen, informiert und unzweideutig durch eine klare Willensbekundung erfolgen. So wird etwa die Zustimmung zur Nutzung von Cookies, wie sie heute bei praktisch allen Websites üblich ist, nicht mehr ausreichen, da hier beispielsweise der Aspekt „informiert“ fehlt und darüber hinaus eine Sammlung und Nutzung von Daten typischerweise schon erfolgt, bevor die Zustimmung gegeben wird.

Des Weiteren muss die Zustimmung zweckgebunden sein (Consent per Purpose) – sie muss auch eingeholt werden, wenn sich der Nutzungszweck von Daten erweitert. Außerdem kann sie für einzelne Nutzungszwecke rückgängig gemacht werden.

Diese Regelungen stellen einige der heute üblichen Geschäftsmodelle, die auf der sehr breiten und umfassenden Nutzung personenbezogener Daten basieren, auf den Prüfstand. Die Herausforderung wird in Zukunft sein, die Zustimmung zu erhalten und sie zu behalten.

Neben der Gestaltung der Kunden- und Konsumenteninteraktion, die grundlegend überdacht werden muss, entstehen auch technische Herausforderungen. Denn wenn eine Firma genau festhalten muss, welchem Nutzungszweck eine Person wann zugestimmt hat respektive wann die Zustimmung widerrufen wurde, muss die Organisation spätestens jetzt damit beginnen, die Prozesse und darunterliegenden Datenmodelle und Anwendungen zu überdenken. Zudem muss das möglichst für alle Kommunikationskanäle des Unternehmens einheitlich gelten, was zu signifikanten Architekturänderungen führen kann.

Hinzu kommen umfangreiche Rechte bezüglich der Einsichtnahme in die gespeicherten Daten, ihre Änderung, die zeitweilige Untersagung der Verarbeitung und die Änderung dieser Daten. Sie gehen über das „Recht auf Vergessen“ deutlich hinaus. Personen können beispielsweise Einsicht in alle über sie gespeicherten personenbezogenen Daten verlangen, die entsprechend der Definition sehr umfassend sein können. Sie können auch ihre Löschung verlangen, soweit die Daten nicht aufgrund anderer gesetzlicher Bestimmungen gespeichert werden müssen.

Recht auf Einsicht und Löschung

Es ist nicht einfach, diese Rechte technisch umzusetzen. Die erste Herausforderung der GDPR für Unternehmen ist zu analysieren, wo welche personenbezogenen Daten gespeichert und verarbeitet werden. Nur wenn das überhaupt bekannt ist, kann man die regulatorischen Vorgaben erfüllen.

Anders als bislang sollen Datenschutzverstöße nicht folgenlos bleiben.

Deutsche Unternehmen erfüllen in der Regel bereits die Anforderung, dass ein Datenschutzbeauftragter vorhanden sein muss. Grundsätzlich kann der DPO (Data Protection Officer) auch ein externer Mitarbeiter sein, der für diese Aufgabe beauftragt wird.

Neu sind dagegen die „Data Protection Impact Assessments" (DPIA), die für bestimmte Informationen wie Gesundheitsdaten oder die bei der Überwachung öffentlicher Plätze erhobenen Daten in Zukunft durchgeführt werden müssen. Diese Datenschutzprüfungen sind in einer definierten Weise umzusetzen und es ist der Nachweis zu erbringen, dass die besonders heiklen Daten angemessen geschützt sind. Das kann in Deutschland beispielsweise im Gesundheitswesen sowohl zu einer technischen als auch zu einer wirtschaftlichen Herausforderung werden, weil dort der Stand der IT oft nicht so ist, dass die Umsetzung der GDPR ohne Weiteres funktioniert.

Pflicht zur Offenlegung von Pannen

Schwierig für alle Unternehmen dürften dagegen die neuen Benachrichtigungspflichten sein. Bei Verlust personenbezogener Daten und in vergleichbaren Situationen muss eine Benachrichtigung innerhalb von 72 Stunden nach der Entdeckung des Vorfalls erfolgen.

Da die Öffentlichkeit inzwischen viel mehr als bisher für solche Verletzungen des Datenschutzes sensibilisiert ist, könnte eine solche Benachrichtigung erhebliche Folgen für die Reputation von Unternehmen haben. Deshalb sollten Unternehmen sich auf eine solche Situation vorbereiten und eine Strategie entwickeln, wie sie im Ernstfall damit umgehen. Das geht bis hin zur Einbindung der Unternehmenskommunikation und der Geschäftsleitung. Der Umgang mit Benachrichtigungen kann nicht erst besprochen werden, wenn es zu einem Vorfall gekommen ist.

Der derzeit wohl noch unklarste Bereich der GDPR sind die Vorgaben für „Privacy by Default" und „Security by Design". Dabei handelt es sich um viel diskutierte, aber wenig definierte Prinzipien. Das Konzept „Privacy by Default" umfasst grundsätzlich die Einstellungen, die einen Schutz personenbezogener Daten garantieren. So ist es nicht zulässig, Optionsfelder für eine Zustimmung vorab mit einem Kreuz oder Haken zu versehen, sodass der Nutzer diese Einstellungen explizit abwählen muss.

Bei „Security by Design" geht es um grundsätzliche Architekturprinzipien, die gewährleisten, dass Anwendungen sicher sind. Das ist insgesamt ein sehr unscharf definierter Bereich, weil die Messlatte fast beliebig hoch liegen kann. Anwendungsarchitekturen, bei denen beispielsweise die Verwaltung von Benutzern und ihre Authentifizierung über definierte Dienste und nicht hart codiert erfolgen, gehören aber grundsätzlich ebenso dazu wie ein umfassendes Auditing von Zugriffen auf personenbezogene Daten oder die Sicherheitsüberprüfung von Code.

Chancen durch die GDPR

Die genannten Punkte sind nur ein Ausschnitt der Veränderungen, die die GDPR mit sich bringt. Im ersten Moment hören sich diese Veränderungen negativ an. Es gibt aber durchaus auch positive Seiten. Da wäre etwa das „gleiche Recht für alle" zu nennen, denn die Regelungen gelten ja für alle Unternehmen, die Geschäfte mit in der EU ansässigen Personen machen. Es sind eben nicht nur europäische Unternehmen, die sich nach der GDPR richten müssen.

Auch die veränderten Anforderungen an die Zustimmung zur Nutzung personenbezogener Daten lassen sich als Chance begreifen. Zum einen gelten sie nur so weit, als nicht ohnehin vertragliche Vereinbarungen bestehen, wobei letztere die GDPR nicht beliebig aushebeln können.

Zum anderen können sie im Idealfall die Kundenbindung stärken, wenn der Nutzen für beide Seiten gegeben ist. Das setzt voraus, dass die gesammelten und verarbeiteten Daten wirklich zweckbezogen sind.

Potenziell kann die GDPR auch den Weg zu Freemium-Modellen ebnen, bei denen Varianten mit reduziertem Funktionsumfang, solche mit umfassendem Funktionsumfang und einer „Bezahlung in personenbezogenen Daten" neben solchen mit umfassendem Funktionsumfang und kostenpflichtigen Diensten stehen. Es spricht aber einiges dafür, dass mehr solche Varianten entstehen, die es Anbietern sogar ermöglichen könnten, endlich zu Abonnement-Modellen statt einer ausschließlichen Finanzierung über Werbung zu gelangen. In solchen Modellen kann der Kunde dann entscheiden, welchen Weg er wählen möchte – personenbezogene Daten zur Nutzung zur Verfügung stellen oder eben für den Dienst zu zahlen, der sich ja in irgendeiner Weise finanzieren muss.

Fazit

Jedem Unternehmen muss bewusst sein, dass die GDPR für alle Unternehmen gilt. Außerdem muss spätestens beim Blick auf den genannten Ausschnitt an Veränderungen klar sein, dass die GDPR in jedem Fall erhebliche Veränderungen mit sich bringt, auf die man sich vorbereiten muss.

Realistisch betrachtet dürfte es für manches Unternehmen jetzt schon zu spät sein, um im nächsten Mai alle Anforderungen der GDPR vollumfänglich erfüllen zu können. Schon die Analyse, in welchen zentralen und dezentralen Systemen personenbezogene Informationen gehalten werden, wird in vielen Unternehmen zur Herausforderung werden. Auch die Anpassung der Registrierung auf Websites und des Umgangs mit der Einwilligung kann äußerst komplex sein.

Die Regelung bedeutet eine Herausforderung, an der man nicht vorbeikommt. Sie bietet aber auch Chancen, die man als Unternehmen nicht ignorieren sollte.

Martin Kuppinger ist Gründer des Analystenunternehmen KuppingerCole und als Principal Analyst verantwortlich für den Bereich KuppingerCole Research.