Gefahr aus dem Netz

Ob beruflich oder privat: Die Digitalisierung hat mittlerweile nahezu alle Bereiche unseres Lebens erreicht. Verwaltung und Unternehmen unterschiedlichster Branchen arbeiten bereits heute IT-gestützt und hochgradig vernetzt, für die grundlegenden Veränderungen im Produktionsbereich wird gerne das Schlagwort Industrie 4.0 verwendet. Smart Home, Mobile Work, eHealth und Entwicklungen wie selbstfahrende Autos sind weitere Beispiele für die fortschreitende Digitalisierung. Und die eröffnet zweifelsohne große Chancen, birgt aber auch erhebliche Herausforderungen zum Beispiel in der Prävention, Detektion und Abwehr digitaler Angriffe, die zunehmend professionalisiert durchgeführt werden.

Der jüngste vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Lage der IT-Sicherheit in Deutschland vorgestellte Bericht lässt in Sachen Cyberkriminalität keinerlei Entwarnung zu. Danach ist die Gefährdungslage weiterhin angespannt, und das auf hohem Niveau. Bekannte Einfallstore für Cyber-Angriffe bleiben unverändert kritisch bestehen. Vor allem die gestiegene Zahl an IT-Sicherheitsvorfällen mit Erpressungssoftware (Ransomware) zeigt, dass Cyber-Kriminelle hier eine lukrative Möglichkeit gefunden haben, in großem Umfang Geld zu erpressen. Zudem spielt auch der „Faktor Mensch" eine zunehmende Rolle: Phishing-Angriffe, bei denen gezielt einzelne Mitarbeiter oder Unternehmen adressiert wurden, sind häufiger als in den letzten Jahren zu beobachten.

„Unser Lagebericht macht deutlich, welche teils immensen Auswirkungen Cyber-Angriffe wie WannaCry, Petya/NotPetya oder der Ausfall hunderttausender Router für Unternehmen und Bürger in Deutschland haben können und dass es notwendig ist, Informationssicherheit als unabdingbare Voraussetzung einer erfolgreichen Digitalisierung zu verstehen", betont BSI-Präsident Arne Schönbohm. Zur Information: Das BSI ist die zentrale und neutrale Stelle für alle Fragen zur IT-Sicherheit – es schützt zum einen die Netze des Bundes, richtet sich aber zugleich auch an gewerbliche und private Anbieter sowie Nutzer von Informationstechnik. Die 840 Mitarbeiter starke Behörde mit Sitz in Bonn ist in ihrer Art europaweit führend und hat in der Vergangenheit schon unzählige Male die Zerschlagung sogenannter Botnetz-Infrastrukturen ermöglicht.

Als nationale Cyber-Sicherheitsbehörde hat das BSI außerdem Lösungsansätze entwickelt und Maßnahmen getroffen, mit denen die Cyber-Sicherheit in Deutschland verbessert wird. Wichtige Grundlage dafür sind zum einen das in der letzten Legislaturperiode verabschiedete IT-Sicherheitsgesetz und die Cyber-Sicherheitsstrategie der Bundesregierung. Zum anderen ist dies die gewachsene Kompetenz des BSI auf dem Gebiet der Informationstechnik. „Durch intensive Vernetzung nach innen können wir den täglich neu entstehenden Risiken die gesamte Wertschöpfungskette der Cyber-Sicherheit entgegensetzen und so die Widerstandsfähigkeit Deutschlands gegen Cyber-Gefahren weiter erhöhen", erklärt Arne Schönbohm.

Verstärkte Schutzmaßnahmen

Tatsache ist: Angesichts der flächendeckenden Angriffe durch bereits genannte Erpressersoftware wie WannaCry oder regelmäßige Berichte über Hackerangriffe macht sich die große Mehrheit der Bundesbürger Sorgen um einen Anstieg der Internetkriminalität und wünscht sich mehr Einsatz von der Politik. Aktuell sind 85 Prozent der Meinung, dass die Bedrohung durch Internetkriminalität immer größer wird. 79 Prozent sagen, dass die Politik mehr Geld in spezielle Polizeieinheiten investieren sollte, die gezielt gegen Internetkriminalität vorgehen. Das ist das Ergebnis einer repräsentativen Befragung von 1.017 Internetnutzern ab 14 Jahren im Auftrag des Digitalverbands Bitkom.

Danach ist in jüngerer Zeit jeder zweite deutsche Internetnutzer (49 Prozent) Opfer von Cybercrime geworden. Mit Abstand häufigstes Delikt ist dabei die Infizierung des Computers mit Schadprogrammen wie Viren. 43 Prozent der Internetnutzer wurden Opfer eines solchen Angriffs. Rund jeder Fünfte gibt an, dass Zugangsdaten zu Online-Diensten wie Sozialen Netzwerken oder Online-Shops gestohlen (19 Prozent) oder persönliche Daten illegal genutzt (18 Prozent) wurden. Rund jeder Sechste (16 Prozent) ist beim Online-Shopping oder Online-Banking betrogen worden. Acht Prozent berichten von massiven Beleidigungen, fünf Prozent von sexueller Belästigung im Netz.

Immerhin ergreift die große Mehrheit der Computernutzer heute schon Maßnahmen, um sich vor Cyberkriminellen zu schützen. 88 Prozent geben an, dass sich auf ihrem privaten Gerät mindestens ein Sicherheitsprogramm befindet oder sie einen Sicherheitsdienst nutzen. Virenschutzprogramme setzen 81 Prozent ein, eine Firewall 61 Prozent. Jeder Vierte, der privat einen Computer oder ein Smartphone nutzt (27 Prozent), gibt zudem an, dass er die eingebaute Kamera an den Geräten abklebt, da es Hackern immer wieder gelingt, über diesen Weg heimlich Aufnahmen zu machen. Doch trotz all dieser Schutzmaßnahmen haben rund zwei Drittel der Internetnutzer (62 Prozent) das Gefühl, dass sie es gar nicht merken würden, wenn Fremde ihren Computer oder ihr Smartphone ausspionieren würden. Und nur jeder Dritte (34 Prozent) sieht sich selbst in der Lage, seine Geräte ausreichend vor Angriffen durch Cyberkriminelle zu schützen. Zugleich würde sich aber ebenfalls nur jeder Dritte (36 Prozent) gerne weiterbilden, um sich im Internet selbst besser schützen zu können.

Gefährdung durch das Internet der Dinge

Im Rahmen der zunehmenden Digitalisierung hält das Internet der Dinge (Internet of Things, IoT) mehr und mehr Einzug in Haus, Wohnung und den persönlichen Bereich der jeweiligen Anwender. Immer mehr vernetzte Geräte ermöglichen immer neue Anwendungen zur Komfortsteigerung, beispielsweise im Bereich der Haushaltsgerätesteuerung, der Hausüberwachung oder im Gesundheitsmanagement. Gleichzeitig werden ehemals bestehende Hürden für den Endverbraucher abgebaut, indem verstärkt funkbasierte Lösungen oder Powerline-Technologien eine zuvor notwendige Verkabelung ablösen. Dies führt zu einer immer höheren Vernetzungsdichte.

Die IT-Sicherheit spielt bei IoT-Geräten bisher jedoch keine oder nur eine untergeordnete Rolle. Für die Kaufentscheidung sind in der Regel die Gerätefunktionalität und der damit verbundene Komfortgewinn sowie der Kaufpreis ausschlaggebend. Dies führt dazu, dass ein neuer Bereich der Ge-

fährdung entsteht, eine größere Angriffsfläche, die von Cyber-Kriminellen für ihre Zwecke genutzt werden kann.

Die Angriffe auf IoT-Geräte erfolgen in der Regel direkt übers Internet oder über vorhandene Funkschnittstellen „over-the-air". Hierbei sind verschiedene Gefährdungslagen mit unterschiedlichen Bedrohungen zu unterscheiden:

- Das IoT-Gerät wird angegriffen, um dem Nutzer direkten Schaden zuzufügen. So können zum Beispiel Smart-Home-Komponenten zur Zutrittssteuerung angegriffen und manipuliert werden, um einen Einbruch vorzubereiten. Über eine kompromittierte Webcam können vertrauliche Informationen über die Bewohner und deren Verhalten in Erfahrung gebracht werden.
- Das IoT-Gerät wird kompromittiert und zum Angriff auf andere Infrastrukturkomponenten oder Services missbraucht. Häufig werden ungesicherte oder nicht ausreichend gesicherte IoT-Geräte kompromittiert und zu Botnetzen zusammengeführt, um gezielte DDoS-Attacken gegen Webseiten oder Webservices von Dritten durchzuführen. Hierbei bleibt der Angriff für den Nutzer häufig unentdeckt, da er selbst von dessen Auswirkungen nicht direkt betroffen ist.
- Das IoT-Gerät wird durch ein Schadprogramm außer Betrieb gesetzt und ist für den Endnutzer zumindest vorübergehend nicht mehr nutzbar. Hiervon waren in jüngster Vergangenheit speziell kleine und mittelständische Unternehmen (KMUs) betroffen, deren Infrastruktur teils tagelang über das Internet nicht mehr erreichbar war.

Was ist Cybercrime?

Cybercrime umfasst nach bundesweit gültiger Definition alle Straftaten, die sich gegen
- das Internet
- weitere Datennetze
- informationstechnische Systeme oder
- deren Daten richten.

Darüber hinaus umfasst Cybercrime auch solche Straftaten, die mittels dieser Informationstechnik begangen werden.

Gefährdung durch mobile Kommunikation

Für viele Menschen sind Smartphones und Tablets unverzichtbar geworden. Sie bereichern die Kommunikation und Unterhaltung, sie ermöglichen Navigation und Interaktion über soziale Netzwerke. Mit wenigen Handgriffen installierte Anwendungsprogramme – Apps – machen dies möglich. Die immer intensivere App-Nutzung sorgt aber auch dafür, dass auf den Geräten immer mehr zum Teil sehr sensitive Daten verarbeitet werden. Adressbücher, Standort- und Zugangsdaten, E-Mails und andere Kommunikationsdaten machen Mobilgeräte zu einem immer lohnenderen Angriffsziel für Kriminelle. Ihre Sicherheit wird dabei durch zahlreiche Aspekte beeinflusst. So räumen Anwender dem Datenschutz und der Sicherheit bei der App-Auswahl oft keine oder bestenfalls eine untergeordnete Rolle ein. Die Kombination von Nützlichkeit und Bequemlichkeit sowie die Kosten sind ausschlaggebend für die Auswahl einer App. Dabei stellt der mögliche Abfluss persönlicher beziehungsweise kritischer Daten einen mit potenziell erheblichen Gefährdungen verbundenen Kontrollverlust dar.

Die Installation von Software-Aktualisierungen, um Sicherheitslücken zu beseitigen, ist Voraussetzung für den sicheren Betrieb mobiler Endgeräte. Aufgrund der Vielfalt der Gerätetypen, sowohl auf Hardware- als auch auf Softwareebene, ist eine kurzfristige und flächendeckende Versorgung mit Aktualisierungen durch Hersteller und Anbieter allerdings kein einfaches Unterfangen. Trotz Initiativen der Industrie, dies zu beschleunigen, waren nach Angaben des BSI im aktuellen Berichtszeitraum viele Mobilgeräte insbesondere mit dem Betriebssystem Android auf einem sicherheitskritischen Softwarestand.

Weitere Probleme: Ein Teil der auf mobilen Geräten anfallenden persönlichen und sensitiven Informationen wird nicht oder nur unzureichend verschlüsselt und oft in einer Cloud gespeichert. Der Nutzer vertraut somit seine Daten dem Cloud-Anbieter an. Falls der Zugriff nicht ausreichend geschützt ist, können sowohl die Nutzerdaten als auch die Zugangsdaten für die Cloud selbst in falsche Hände geraten. Dazu kommt, dass Mobilgeräte sich oft mit öffentlichen Hotspots verbunden. Hier werden die Daten in der Regel unverschlüsselt übertragen und können somit von unbefugten Dritten mitgelesen werden. Eindeutige Nutzerkennungen wie die International Mobile Subscriber Identification (IMSI) sind hiervon potenziell betroffen. Nicht vergessen werden darf außerdem, dass Betreiber von Mobilfunknetzwerken sowie App-Anbieter in der Lage sind, Mobilgeräte zu orten und damit auch den Standort des Besitzers festzustellen. Schwachstellen in der Infrastruktur des Mobilfunkbetreibers können dazu führen, dass eine Ortung von Mobilfunkgeräten auch durch Dritte möglich ist. Angreifer können so ein umfassendes Bewegungsprofil des Opfers anlegen. Auch die Nutzung von SMS als Authentifizierungsfaktor sowie zur Autorisierung von Transaktionen (mTAN-Verfahren) birgt Risiken. Angreifer können durch die Ausnutzung von Schwachstellen in der Netzwerkinfrastruktur den SMS-Verkehr umleiten und so die verschickten Codes missbrauchen. So gab es laut BSI im Berichtszeitraum etwa Schwachstellen im für den Austausch zwischen Mobilfunknetzen wichtigen SS7-Protokoll und damit die Möglichkeit, SMS-Nachrichten beim Online-Banking abzufangen. Ein entsprechender Missbrauch ist auch durch Schadsoftware auf dem Endgerät möglich.

Die Auswirkungen dieser zahlreichen Schwachstellen auf den Schutz der Privatsphäre und der sensitiven Daten sind ebenso beachtlich wie mannigfaltig. Einerseits können durch den Abfluss persönlicher Daten, sei es durch Apps auf dem Endgerät, beim Netzwerkbetreiber oder Cloud-Anbieter, detaillierte Rückschlüsse über das Verhalten, die Interessen, die Aufenthaltsorte und die Gesinnung des Nutzers abgeleitet werden. Diese Informationen könnten anschließend ohne Zustimmung des Betroffenen beispielsweise zu Werbezwecken verwertet beziehungsweise auf unbestimmte Zeit gespeichert, zu kriminellen Zwecken oder zur Diskreditierung einer Person ausgenutzt werden.

Nützliche Links zum IT-Grundschutz und zur Sicherheit im Netz:

www.bsi.bund.de
www.sicher-im-netz.de
www.bka.de
https://lka.polizei-bw.de/zentrale-ansprechstelle-cybercrime
www.bitkom.org
www.bmwi.de

Andererseits sind die Mobilgeräte selbst das Ziel aktiver Angriffe. Sollten Sicherheitsupdates nicht vorhanden oder eingespielt worden sein, kann ein Angreifer, wie bei stationären Rechnern auch, die Kontrolle über das Mobilgerät übernehmen. Neben dem üblichen Missbrauch der Ressourcen (zum Beispiel Einbindung in ein Botnetz) ist das finanzielle Risiko von Schadsoftware im mobilen Kontext sehr hoch, da kostenpflichtige Telefonate, SMS-Nachrichten oder andere Premium-Dienste ohne Zutun des Betroffenen ausgeführt werden können.

Gefährdungslage in der Wirtschaft

Wirtschaftsunternehmen in Deutschland sind aufgrund ihres technologischen Know-hows und durch ihre Auslandsaktivitäten interessante Ziele für Cyber-Spionage. In den letzten Jahren haben viele Unternehmen reagiert und eigene Computer-Notfall-Teams (CERTs) sowie branchenübergreifende Organisationen zum Informationsaustausch gegründet. Unternehmen sind grundsätzlich den gleichen Gefahren ausgesetzt wie jeder andere Nutzer von IT und Internet. Zusätzlich sehen sie sich aber Angriffen ausgesetzt, die im privaten Umfeld nicht vorkommen. Hierzu gehört zum Beispiel der CEO-Betrug, bei dem Angestellte von Unternehmen dazu verleitet werden sollen, große Geldbeträge auf Konten zu überweisen, die der Kontrolle der Angreifer unterliegen. Bei Ransomware-Angriffen ist zu beobachten, dass von Unternehmen mehr Lösegeld gefordert wird als von privaten Anwendern.

Die Erfahrung zeigt, dass zunehmend auch Kriminelle Techniken anwenden, die bisher nur aus Spionage-Angriffen bekannt waren. So griff beispielsweise die Lazarus-Gruppe weltweit Banken an, um gefälschte Überweisungen über das SWIFT-Netzwerk zu veranlassen. Die Carbanak-Gruppe wiederum kompromittierte Finanzinstitute und Geldautomaten, um ebenfalls Überweisungen zu fälschen. Dabei setzen beide Gruppen Techniken ein, die über die bei normaler Crimeware beobachteten Methoden hinausgingen. Dazu zählt das Social Engineering auf ausgewählte Mitarbeiter und das Lateral Movement, also das Ausbreiten im internen Netz, indem erbeutete Zugangsdaten verwendet und Nutzer-rechte ausgeweitet werden.

Cyber-Spionage bleibt weiterhin eine Herausforderung, gegen die sich Unternehmen wappnen müssen. Da die Angriffe sehr oft in den weniger abgesicherten Netzwerken

von Auslandsstandorten oder zugekauften Tochterunternehmen ihren Ursprung nehmen, sollte der Fokus darauf liegen, unternehmensweit ein einheitliches IT-Sicherheitsniveau zu erlangen. Da in vielen Unternehmen die IT-Netze zu wenig voneinander getrennt sind, gelingt es den Angreifern sonst zu leicht, sich weltweit im Unternehmensnetz auszubreiten. Wenn Standard-Sicherheitsmaßnahmen unternehmensweit etabliert wurden, sollten in der Folge Prozesse für das Netzwerk-Monitoring erarbeitet und eingeführt werden. Wenn diese Infrastrukturen und geschultes Personal existieren, kann zusätzlich über den gezielten Einkauf von Threat Intelligence Services nachgedacht werden. Diese Services liefern aktuelle Informationen zur Bedrohungslage der IT-Sicherheit durch Cyberangriffe und andere Gefahren.

Dessen ungeachtet können Unternehmen gegen Cyberangriffe zumindest ein paar Vorkehrungen treffen. Seitens der Firmenleitung macht es nach Angaben des Bundeskriminalamtes auf jeden Fall Sinn, schon vor Eintritt eines Schadensfalls im Unternehmen Verfahrensweisen oder Anleitungen zum Umgang mit Vorfällen beziehungsweise Straftaten aus dem Bereich der Cybercrime vorbereitet zu haben. Insbesondere sollten die Compliance- und Datenschutzbeauftragten in die Planungen eingebunden werden. Die Verfahrensweisen oder Anleitungen sind regelmäßig zu überprüfen und allen Mitarbeitern zugänglich zu machen, die Verantwortung für die Systemsicherheit haben. Darüber hinaus sollten die Verfahren konkrete Anweisungen insbesondere zu folgenden Punkten enthalten: Wer hat im Unternehmen welche Verantwortung für die interne Reaktion auf einen Schadensfall? Wer ist die Ansprechstelle für interne und externe Kontakte? Wer sollte innerhalb und außerhalb der Firma unmittelbar verständigt werden? Und an welchem Punkt sollten die Strafverfolgungsbehörden informiert werden? Hilfreich ist es auch, firmenintern bereits im Vorfeld festzulegen, welche Protokolle beziehungsweise Logdaten gegebenenfalls routinemäßig vom System wie lange erfasst und gespeichert werden und somit im Bedarfsfall als Beweismittel zur Verfügung stehen.

Im Verdachtsfall sollte man sich nicht scheuen, die Polizei einzuschalten. Grundsätzlich kann und wird jede Polizeidienststelle eine Strafanzeige entgegennehmen. Es empfiehlt sich jedoch, sich direkt an die inzwischen in mehreren Bundesländern eingerichteten Fachdienststellen für Cybercrime-Delikte zu wenden. Darüber hinaus stehen auch in vielen Landeskriminalämtern oder im Bundeskriminalamt zentrale Ansprechstellen zur Verfügung. ■

„Ziehen Sie Experten hinzu"

Fragen an Max Schaber, CEO der zu den führenden deutschen IT-Full-Service-Providern zählenden Datagroup SE mit Stammsitz in Pliezhausen

top: Herr Schaber, Cyberkriminalität ist für jedes Unternehmen eine immense Gefahr. Wie kann man sich davor schützen?
Schaber: IT-Security entsteht nicht von selbst – sondern nur, indem das Thema angegangen und mittels handlungsfähiger und definierter Strukturen organisiert wird. Darüber hinaus müssen natürlich die wesentlichen technischen Fähigkeiten vorhanden sein, um IT-Sicherheit zu überwachen und aus Sicherheitsmeldungen Aktionen ableiten zu können. Viele Unternehmen machen meines Erachtens den Fehler, zu sehr im eigenen Saft zu kochen und scheuen sich, externe Experten und Ratgeber als zusätzliche Meinungen zu hören.

top: Gibt es angesichts immer neuer Hackerangriffe und Malware überhaupt den 100-prozentigen Schutz?
Schaber: Den gibt es auch ohne Hacker und Malware nicht – schon alleine, weil Menschen als Betreiber von IT-Systemen Fehler machen können. Deswegen ist es auch so wichtig, diese Risiken zu erkennen, zu beschreiben und mittels geeigneter Maßnahmen zu managen – also im Griff zu halten. Deshalb meine klare Empfehlung: Ziehen Sie Experten hinzu.

top: Könnte vor diesem Hintergrund die Auslagerung der IT an einen externen Dienstleister Sinn machen?
Schaber: Das ist in der Tat sogar ein sehr gutes Argument für IT-Outsourcing. Schon heute wissen wir aus Untersuchungen zum Beispiel der BITKOM, dass interne IT-Abteilungen tendenziell mehr Sicherheitsvorfälle abarbeiten müssen als eine vergleichbare Kundenumgebung im Outsourcing-Fall. Das ist auch naheliegend und nachvollziehbar. IT-Systeme, die durch einen externen Dienstleister betreut werden, müssen für diesen exakt beschrieben und nachvollziehbar sein. Das schafft explizite Strukturen, die eine gute Voraussetzung bilden, um IT-Sicherheit besser zu organisieren.

top: Lohnt sich die Auslagerung der IT in die Cloud auch schon für kleinere Unternehmen?
Schaber: Diese Frage ist schwer eindeutig zu beantworten – es kommt sehr stark auf die Art und den Umfang der geplanten Auslagerung an. Bestimmte Teilaufgaben wie zum Beispiel ein CRM- beziehungsweise Kundenbeziehungsmanagementsystem bieten sich gerade dafür an. Bei anderen Themen wie etwa einem komplexen Fertigungs-/Steuerungssystems ist eine Auslagerung erst ab einer bestimmten Größe sinnvoll. Aber keine Frage: Dieses Thema ist sehr in Bewegung. Der Anbietermarkt entwickelt sich im Moment sehr dynamisch und es existieren für fast alle Aufgaben sinnvolle Lösungsansätze.

top: Woran erkennt man einen geeigneten IT-Partner?
Schaber: Eine der wichtigsten Voraussetzungen scheint mir die Zertifizierung auf Basis allgemein anerkannter Normen wie beispielsweise der ISO 20000. Damit weist der Anbieter eine Grundprofessionalität nach. Darüber hinaus sind auch weitere Kriterien wie technische Fähigkeiten, ausreichende personelle und technische Ressourcen sowie eine definierte Sicherheitsstrategie wichtig. Aber am Ende des Tages und auch in der finalen Entscheidung für einen Partner darf die Vertrauensfrage nicht unterschätzt werden. Die Chemie muss einfach stimmen.