PETER FROMMENWILER

Fabrikation: Die Drucksensoren von Trafag werden in Einzelflussfertigung in der modernen Hightech-Anlage unter Reinraum-Bedingungen hergestellt.

«Wir sind Cyberkriminalität verstärkt ausgeliefert»

Aldo Rodenhäuser Der IT-Sicherheitsexperte über die zusätzlichen Risiken des Internets der Dinge, wie Cyber-Angriffe erkannt werden können und wie sich KMU am besten auf Attacken vorbereiten.

INTERVIEW: ROBERTO STEFANO

Im Internet der Dinge (Internet of Things, IoT) kommunizieren Mensch, Maschine und Produkt über das Internet. Worauf müssen sich die Unternehmen bezüglich Cyber-Kriminalität gefasst machen, wenn zukünftig die Geräte selbstständig auf das Internet zugreifen?

Aldo Rodenhäuser: Es kommt zu einer entscheidenden Veränderung: Bisher konnten die Firmen ihr Netzwerk mit einer virtuellen «Mauer» schützen. Diese bekommt nun sehr viele Löcher. Eine vergleichbare Entwicklung gab es mit dem Einzug der mobilen Geräte, die inzwischen aber recht gut kontrolliert werden. Mit IoT wird eine neue Stufe erreicht, die deutlich mehr Devices umfasst, welche zudem noch heterogener und dynamischer sind. Entsprechend schwieriger wird es, diese zu überwachen.

Ist man sich der Gefahren bewusst?

Da bin ich mir nicht so sicher. Unternehmen scheinen das Ausmass und die Schwere der Bedrohung, mit der sie sich auseinandersetzen müssen, oftmals zu unterschätzen. In vielen IoT-Visionen, und dies gilt auch bei führenden Unternehmen, findet IT-Sicherheit kaum einen Platz, obwohl neue Ansätze nötig sind. Bisher entwickelten die Ingenieure von eingebetteten Systemen hauptsächlich Offline-Produkte. Eine Pumpensteuerung beispielsweise war nicht mit dem Internet verbunden. Heute ist sie online. Und sobald etwas online ist, kann es auch von fern missbraucht werden.

Die Angriffsflächen für Kriminelle werden in Zukunft also immer grösser?

Zumindest sind wir der Cyberkriminalität heute verstärkt ausgeliefert, das gilt für Private genauso wie für Firmen. Heute kommuniziert ein Auto über das Internet, ein Thermostat und selbst der Herzschrittmacher. Einerseits können die IoT-Geräte selbst gehackt werden und anderseits auch derjenige, zu dem das IoT-Gerät nach Hause «telefoniert». Das Problem von IoT ist, dass wir uns häufig nicht bewusst sind, welche Geräte sich überhaupt über das Internet verbinden und was sie kommunizieren. Selbst ein Rasenmäherroboter, der über eine App gesteuert werden kann, könnte ein Sprungbrett sein, um in ein Netzwerk einzudringen. Es gibt aber auch keinen Grund, weshalb beispielsweise eine Heizungssteuerung im normalen Firmennetzwerk integriert sein soll. Mit einer Netzwerk-Segmentierung lassen sich einige Gefahren abwenden.

Welches sind derzeit die grössten Bedrohungen im Bereich Cyberkriminalität?

Am häufigsten werden Datenlecks herbeigeführt. Ein Ziel ist, geistiges Eigentum oder Geschäftsgeheimnisse abzuziehen. Ein weiteres Ziel sind Kundendaten, die üblicherweise an Dritte weiterverkauft werden. Schliesslich gibt es die digitale Erpressung, beispielsweise durch Ransomware, welche die Daten auf infizierten Rechnern verschlüsselt und erst nach Zahlung eines «Lösegeldes» wieder freigibt. Diese Bedrohungen gelten für alle Branchen. In der Industrie werden immer mehr Betriebsunterbrüche herbeigeführt. In einem deutschen Stahlwerk haben Hacker Ende 2014 beispielsweise den Hochofen übernommen und dadurch einen hohen Schaden verursacht. Hinzu kommt der Reputations- und Vertrauensverlust bei den Kunden. Als Langzeitschaden kann es sogar so weit kommen, dass diese abwandern.

Steckt hinter solchen Angriffen die Konkurrenz?

Unter Schweizer KMU zumindest gehe ich nicht davon aus, dass sich die Konkurrenten mittels Cyberattacken auszuschalten versuchen. Hinter solchen Angriffen vermute ich eher grössere Organisationen oder Staaten.

Security-Experte

Name: Aldo Rodenhäuser
Funktion: Senior IT Consultant, AdNovum Informatik AG
Alter: 42
Wohnort: Baar
Familie: Verheiratet
Ausbildung: Dipl. El.-Ing. FH, CAS ETH INFK/Informationssicherheit, KMU Management HSG

Das Unternehmen Der Zürcher Software- und Security-Spezialist AdNovum fokussiert sich laut eigenen Angaben auf «High-End Software Engineering». Die 1988 gegründete Firma beschäftigt weltweit gut 500 Mitarbeitende.

Der Werkplatz Schweiz besteht vor allem aus kleinen und mittelgrossen Unternehmen. Wie sehr sind diese gefährdet?

KMU sind attraktive Ziele, genauso wie Startup-Firmen. Oftmals verfügen sie über interessante Assets, sind aber vielfach nicht sehr gut geschützt. Dadurch werden sie zu einer relativ einfachen Beute. Vielfach wird aber auch das angegriffene KMU als Sprungbrett benutzt, um in die meist grössere Firma, welche beliefert wird, einzudringen.

Wie erkennen die Unternehmen, dass sie angegriffen werden? Selbst der Technologieriese Sony hatte lange dazu benötigt.

Das sagt eigentlich schon alles. Es ist extrem schwierig. Je ausgeklügelter der Angriff, desto schwieriger ist es, ihn zu entdecken. Das A und O ist die Erkennung von Anomalien. Die Mitarbeiter und auch die Systeme müssen die Normalität kennen. Sobald es hiervon zu Abweichungen kommt, müssen Abklärungen getroffen werden. Überwacht werden zum Beispiel die Log-Einträge auf dem Server, der Mailverkehr oder das Datenvolumen. Neben technischen Lösungen braucht es das Bewusstsein der Mitarbeitenden. Sie müssen sich im Klaren sein, dass es zu Cyberangriffen kommen kann.

Wie informiert sind die Mitarbeitenden?

Das Bewusstsein ist wohl noch zu wenig hoch, besonders in KMU.

Welche minimalen IT-Sicherheitsanforderungen sollten KMU erfüllen?

Eine allgemeingültige Aussage hierzu gibt es nicht. Hilfsmittel wie zum Beispiel das «Merkblatt IT-Sicherheit für KMU» der Melde- und Analysestelle Informationssicherung (Melani) können helfen. Grundsätzlich muss jedes Unternehmen seine wichtigsten Assets kennen und basierend darauf eine Risikoanalyse vornehmen. Das Resultat zeigt dann, welche minimalen Anforderungen erfüllt sein müssen.

Was wollen die Angreifer eigentlich?

Es kommt darauf an, um welchen Angreifer es sich handelt. Script-Kiddies, sprich Gelegenheitshacker, sind eher am Challenge und Ruhm interessiert. Die Firmen sollten eigentlich von den Script-Kiddies unbehelligt bleiben, ansonsten sind die Sicherheitsvoraussetzungen sicherlich zu wenig hoch. Handelt es sich um organisierte Angriffe, so geht es typischerweise um Geld. Die Kriminellen sind an Daten interessiert, die sich zu Geld machen lassen. Noch komplexer und gefährlicher sind die staatlich gesponserten Attacken, bei denen es eher um Spionage geht. Diese sind sehr schwer zu erkennen, da sich Angreifer lange Zeit nehmen können und beispielsweise über Social Engineering langsam herausfinden, wer wann und wie Zugriff auf gewisse Daten hat. So fällt eine Attacke kaum auf, da sie von der Normalität nicht stark abweicht.

Wie sollen die Firmen reagieren, wenn sie angegriffen werden?

Es gibt gute Richtlinien im Internet. Wichtig ist, dass man einen Prozess für die Bewältigung von Sicherheitsvorfällen bereithält, wenn es zu einer Attacke kommt. Dazu gehört beispielsweise, dass man ein System nicht gleich rebootet, damit die Beweise erhalten bleiben. Erst sollte man analysieren, welche Systeme, Stellen und Personen betroffen sind, und diese auch benachrichtigen. Anschliessend muss

«KMU sind attraktive Ziele. Oftmals verfügen sie über interessante Assets, sind aber nicht sehr gut geschützt.»

man den Angriff eindämmen, indem man beispielsweise das System vom Netz nimmt. Dies kann grosse Auswirkungen auf die Verfügbarkeit haben und hohe Kosten verursachen. Daher sollte die Firma vorbereitet sein, um solche Entscheide nicht in der Hektik treffen zu müssen. Beweissammlung, Bereinigung und Wiederherstellung des normalen Betriebs sind dann typischerweise die nächsten Schritte. Am Ende gilt es, die Lehren aus dem Angriff zu ziehen und sicherzustellen, dass dies nicht mehr geschieht.

Mit welchen Hilfsmitteln können sich Unternehmen schützen?

Häufig stehen technische Massnahmen im Fokus. Faktisch sind organisatorische Massnahmen und Prozesse genauso wichtig. Die Mitarbeiter müssen aufmerksam sein. Wenn ihnen etwas auffällt, sollen sie sich melden. Auch die Zuständigkeiten müssen definiert sein. Was die Prozesse betrifft, so ist das Incident Handling ein wichtiger Teil. Zuerst braucht es aber ein Risikomanagement sowie bei grösseren Firmen ein Information Security Management System. Ein Business Continuity Management respektive das darin enthaltene Disaster Recovery sorgt dafür, dass der Betrieb nach einer Attacke wieder schnell zur Normalität zurückkehren kann. Die Prozesse sollten alle vorhanden und auch getestet sein.

Und bei den technischen Hilfsmitteln?

Auf der technischen Seite geht es darum, das Prinzip «Verteidigung in der Tiefe» zu implementieren. Dies beginnt bei klassischen Elementen wie Virenscanner, Firewalls, Netzwerk-Segmentierung, hin zu verhaltensbasierten Systemen, welche Unregelmässigkeiten im Netzwerk selbst erkennen und Alarm schlagen. Das Schlagwort hierzu ist «Network Behavior Anomaly Detection». Zentral ist sicherlich auch ein Identiy and Access Management, welches Identitäten, sprich heute vor allem Personen und ihre Berechtigungen, verwaltet und Zugriffe entsprechend aufzeichnet. Dieses muss nun auch auf die IoT-Geräte ausgedehnt werden. Alle IoT-Devices müssen verwaltet werden.

Wie sinnvoll ist es, sich auf eine Cloud zu verlassen?

Ist der Cloud-Anbieter seriös, dann ist sie eine sehr gute Sache. Der Anbieter übernimmt dann zahlreiche Aufgaben wie beispielsweise die Überwachung oder das Aktualisieren der Server. Es löst aber nicht alle Probleme: Für die Sicherheit an den Endgeräten und den Umgang der Mitarbeitenden mit den Daten bleibt das Unternehmen weiterhin selber zuständig. Und auch über die sichere Verbindung in die Cloud muss sich das Unternehmen Gedanken machen.

Zum Schluss: Wie schützen Sie sich selber vor Cyberattacken?

Bei mir ist sicherlich die Sensibilisierung sehr hoch. Ich überlege mir genau, ob ich auf eine E-Mail klicke, geschweige denn noch ein Attachment öffne. Zudem verwende ich in E-Mails kein HTML, damit keine Programme ausgeführt werden. Als Spezialist überprüfe ich meine IT sporadisch auf gewisse Anomalien, insbesondere auch, wohin sich die Geräte verbinden. Zudem verwende ich verschiedene physische und virtuelle Geräte für unterschiedliche Anwendungen.

Und welche Empfehlung haben Sie für normale User?

Ein funktionierender Virenscanner, sämtliche Software auf dem aktuellen Stand halten und eine hohe Sensibilität sind entscheidend. Wenn man etwas herunterlädt und Berechtigungen erteilt, sollte man sich im Klaren sein, was eine solche Anwendung bewirken könnte. Denn auch wenn Sie selber nicht das Ziel eines Angriffs sein sollten, so können Hacker Sie als Sprungbrett missbrauchen, um an die Daten Ihres Chefs oder der Firma zu gelangen. Dies gilt auch für IoT-Devices.