**IT-Bedrohungen der Zukunft – Informieren Sie sich bevor es zu spät ist!**

Luca Rechsteiner, Junior Berater

*Vom Laptop über Smartphone bis zum Tablet, im Zeitalter der mobilen Endgeräte ist jedermann jederzeit mit dem Internet verbunden. Dies bringt schon jetzt erhebliche Sicherheitsrisiken mit sich. Unternehmensdaten werden verschlüsselt, Promifotos veröffentlicht und Finanzinstitute werden ausgeraubt ohne dass jemand das Gebäude betreten hat. Zukünftig werden solche Cyberangriffe noch raffinierter und noch schneller vonstattengehen.*

Das Jahr 2015 war geprägt von Meldungen über Cyberkriminalität. Über einige Hacker-Grossangriffe und Sicherheitslücken wurde in den Medien ausführlich berichtet. Vor allem wie eine Gruppe Cyberkrimineller es schaffte fast eine Milliarde US-Dollar zu stehlen, ohne je einen Fuss in die Bank zu setzen. All diese Meldungen erhöhen den Druck auf die Sicherheitsbeauftragen, CEOs oder CIOs. Für grosse Verunsicherung bei den IT-Verantwortlichen sorgte 2015 zudem das erhöhte Aufkommen von Verschlüsselungs-Trojanern, auch Ransomware genannt. Diese Schadsoftware schleust sich in das Unternehmensnetzwerk ein und verschlüsselt beliebig viele Daten auf dem Server. Der Entschlüsselungscode wird von den Angreifern nur gegen Bezahlung (meistens in Form einer nicht zurückverfolgbaren Währung) ausgehändigt. Die anschliessende Geldtransaktion wird im „dunklen Netz“ abgewickelt. All diese Angriffe laufen über das Internet. Deshalb bietet das sogenannte Internet der Dinge (Internet of Things – IoT) den Cyberkriminellen viele Möglichkeiten ihrer Tätigkeit nachzugehen.

In Deutschland verschafften sich Cyberkriminelle unerlaubt Zugriff auf das Netzwerk eines Stahlwerkes. Die Angreifer steuerten über das Internet den Hochofen an und überhitzten diesen. Daraus resultierte ein erheblicher Sachschaden. Wie an diesem Beispiel eindrücklich gezeigt, ist die Industrie 4.0 ein immer wichtiger werdendes Ziel von Cyberkriminellen. Mit Industrie 4.0 wird die Informatisierung der Fertigungstechnik und Logistik bezeichnet. Ein Beispiel dafür ist die nahtlose Kommunikation vom Sensor bis ins Internet. Dies birgt viele Gefahren. Oft wollen Unternehmen die neusten Technologien adaptieren und schliessen ihre Maschinen ohne grosse Vorabklärung ans Netz an. Das ist sehr problematisch, da die älteren Maschinen nicht für diese Verwendung gebaut wurden. Auch für Industrie 4.0 konzipierte Produktionsanlagen können möglicherweise Opfer dieser Attacken werden. Dies kann zu Fehlproduktionen oder im schlimmsten Fall zu Schäden an Leib und Leben führen.

Ein weiteres Ziel von Hackern sind und werden vermehrt Systeme die in Verbindung mit Geld stehen. Das können Kassen, Bankomaten oder Bezahlterminals sein. Oft sind herkömmliche Computer mit einem Code-Lesegerät ausgestattet und werden als legitime Kassensysteme verwendet. Das stellt ebenfalls ein erhebliches Sicherheitsrisiko dar, da diese Computer nicht für diese Tätigkeit konzipiert wurden. Nebst der Gefahr bei Kassen, Bankomaten und Bezahlterminals werden in Zukunft auch die Zahlungssysteme von Apple und Android auf die Probe gestellt. Das Bezahlen mit dem Smartphone über ApplePay oder AndroidPay wurde in den USA bereits eingeführt. Diese neue Art Einkäufe zu bezahlen wird bei vielen Cyberkriminellen das Interesse wecken. Die bargeldlose Bezahlung wird auch in Europa Einzug halten. Aus diesem Grund gilt es jetzt abzuwägen, inwieweit sich die Konsumenten schützen lassen.

Cyberkriminelle setzen oft auf Quantität statt Qualität. Deshalb liegt ihr Fokus meistens bei der grossen Masse, wo es die meisten Möglichkeiten gibt etwas zu erbeuten. Mobile Endgeräte sind deshalb ganz oben auf der Liste. Experten schätzen, dass bis 2018 etwa 22 Milliarden vernetzte Geräte in Betrieb sein werden. Hinzu kommen ca. 200‘000 neue Anwendungen die bis zu diesem Zeitpunkt entwickelt werden. Bei einer so grossen Anzahl an Geräten wird es für Nutzer, wie auch für IT-Sicherheitsdienstleister schwierig werden, den

Überblick zu behalten. Deshalb ist das Internet der Dinge bei Cyberkriminellen sehr beliebt.

Diese drei Angriffsziele haben zwei Dinge gemeinsam. Zum einen sind diese Geräte, Maschinen und Kassensysteme ständig mit dem Netz verbunden. Zum anderen sind diese Gerätschaften grösstenteils zu jung beziehungsweise zu wenig ausgereift, um umfassende Sicherheitskonzepte zu gewährleisten. Diese beiden Faktoren spielen den Cyberkriminellen natürlich in die Hand. Es gibt jeden Tag neue Ziele für Hacker. Zudem darf nicht ausser Acht gelassen werden, dass sich die Internetkriminellen selbst auch weiterentwickeln. Sie werden immer raffinierter und kreativer, was die Sicherheitsdienstleister und -beauftragten vor grössere Herausforderungen stellt und stellen wird.

Was kann also gegen die Bedrohungslage unternommen werden? Eine hundertprozentige Sicherheit wird nie gewährleistet werden können. Jedoch kann jedes Unternehmen wie auch jeder Privatanwender Schutzmassnahmen ergreifen. Bevor diese Massnahmen aber ergriffen werden, sollte eine umfassende Schutzbedarfsanalyse durchgeführt werden. Mittels dieser wird evaluiert, was es zu schützen gilt. Dies können Server, Applikationen, Geräte, Maschinen wie auch Festplatten oder Clouds sein. Daraus werden Handlungsempfehlungen und Sofortmassnahmen, in Anlehnung an die ISO Normen 31000:2009 und 27001:2013, abgeleitet. Beispiele solcher Handlungsempfehlungen können der Aufbau und die Pflege eines Sicherheitsbewusstseins, kryptographische Standards, Sicherung/Schutz der Infrastruktur und Vorschläge zur Optimierung verschiedener Programme sein. Um ein höheres Level des Sicherheitsbewusstseins zu erreichen, können Informationsanlässe, Schulungen, Weiterbildung und Erfahrungszirkel eingesetzt werden. Kryptographische Standards werden erreicht in dem Passwortrichtlinien eingeführt werden, die folgendermassen lauten können: Passwörter müssen Gross- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Ein Beispiel, wie kritische Infrastrukturen geschützt werden können, sind unternehmensinterne Netzwerktrennungen in Sicherheitszonen. Diese werden wie das äussere Unternehmensnetzwerk zum Perimeterschutz mit einer Firewall abgesichert. Somit müssen Angreifer zuerst die Firewall im Perimeter hacken und anschliessend die Firewalls der internen Netzwerkzonen. Das bedeutet mehr Aufwand für die Cyberkriminellen und je mehr Aufwand benötigt wird desto weniger attraktiv ist das Ziel. Die Programmoptimierungen können verschiedene Dinge beinhalten. Es besteht die Möglichkeit die neusten Antivirus-Programme zu implementieren, die einen regelmässigen Datenaustausch mit der Cloud machen, um jederzeit auf die aktuellsten Bedrohungen reagieren zu können. Eine weitere Möglichkeit stellen Programmeinstellungen von Java, Flashplayer und dem Internetbrowser dar, die automatischen Updates aktiviert haben. All diese Massnahmen und viele weitere tragen dazu bei, dass mit jeder zusätzlichen Schutzschicht das Risiko des Eindringens verringert wird. Ganz im Sinne des „Zwiebelschalenprinzips“.