Wenn IT-Kriminalität zunehmend industriell betrieben wird, müssen CIOs vor allem eins:

Sicherheit neu denken!

Wirtschaftsleben und Consumer-Welt werden zu einer vernetzten Informations- und Wissensgesellschaft. Dabei kommt nicht nur immer neueren, sinnvollen und erfolgsverspechenden Technologien eine besondere Bedeutung zu. Sondern auch unserem nötigen – und möglichen - Vertrauen auf Sicherheit.

Je wertvoller Daten werden, die als Bits und Bytes zur Verfügung stehen, desto größer ihre Abhängigkeit von sicheren IT-Dienstleistungen aus dem Netz. Aus zwei Gründen: Die möglichen Angriffsflächen werden immer breiter und vielfältiger. Und die Ausführung von Attacken – auch auf die Verfügbarkeit der IT-Systeme - stetig verteilter, raffinierter und professioneller. Zugleich erfährt IT-Kriminalität eine zunehmende Industrialisierung und mögliche Schäden eine kaum zu überschätzende Nachhaltigkeit. Die Anforderung an Individuen und Organisationen, Unternehmen und Behörden ihre Daten und damit ihre Werte zu schützen, ist höher als je zuvor.

Sicherheitsproblem: Software-Qualität

Die Software stellt in allen Branchen einen anhaltend größeren Wertschöpfungsanteil dar. Wir nutzen sie in PCs, Notebooks, SmartPhones, aber auch immer mehr in Autos, Industrieanlagen oder Kühlschränken.

Eine gute Software erreicht ein hohes Maß an Qualität, wenn alle Funktionen korrekt und zuverlässig arbeiten. Eine schlechte Software hingegen hat viele Schwachstellen und ist damit einfach anzugreifen. Die Ursachen für leicht angreifbare Software sind z.B. steigende Komplexität, kein Sicherheitsbewusstsein sowie fehlende Expertise der Entwickler. Oder einfach nur der Zeitdruck für die Fertigstellung. Die Hersteller arbeiten daran, die Anzahl der Schwachstellen in ihrer Software zu minimieren. Aber die Angreifer machen zurzeit einen besseren "Job". Aus heutiger Sicht ist festzustellen, dass sich dieser Zustand nicht kurzfristig ändern wird, d.h. die Fehlerdichte von Software wird zwar kleiner, Fehlerfreiheit ist aber nicht erreichbar. Die kleiner werdende Anzahl der Software-Schwachstellen wird gleichwohl wegen der professionelleren Nutzung durch kriminelle Organisationen immer bedrohlicher.

Angriffsvektor: Malware

Angreifer verfolgen im ersten Schritt gern das Ziel, "Schadsoftware" wie Viren, Würmer, Trojanische Pferde durch Software-Schwachstellen auf IT-Endgeräte zu schleusen. Diese Malware wird z.B. über E-Mail-Anhänge oder Webseiten mit Schadcode, auf

denen die Nutzer surfen, unbemerkt auf deren Endgräten installiert. Wir gehen davon aus, dass aktuell auf jedem 25-ten IT-Endgerät ungewollte Malware vorhanden ist, die über ein Botnetz gesteuert wird. So können Angreifer nicht nur die Devices von Unternehmen für die Spam-Verteilung einsetzen und so für DDoS-Angriffe (Distributed Denial of Service) auf andere Adressaten nutzen. Mit gleich zwei Effekten: Die IT-Systeme anderer Netzwerke oder Organisationen werden unter Umständen komplett lahmgelegt und die Spur zur möglichen Rückverfolgung der Täter verschleiert.
Viel gefährlicher kann werden, wenn IT-Kriminelle Informationen von unseren Endgeräten auslesen (Keylogger) und Software oder Daten unbrauchbar machen. Zurzeit liegt die Rate der Attacken, die von Anti-Malware-Produkten erkannt werden, nur bei 75 bis 90 Prozent!

Quantensprung von Angriffssoftware: „Stuxnet“
CyberWar wird eine immer realere Bedrohung in Form von gezielten Angriffen auf kritische Infrastrukturen. Neben den DDoS-Angriffen auf Server der Regierung von Estland, ist *Stuxnet* unlängst als eine weitere potentielle Bedrohung von Staaten bekannt geworden. Unter dem Namen wird ein Botnet mit einer qualitativ sehr hochwertigen Malware verstanden, die speziell für Produkte zur Überwachung und Steuerung technischer Prozesse (SCADA/Supervisory Control and Data Acquisition) entwickelt wurde. Es wird spekuliert, dass diese Malware mit dem Ziel geschrieben wurde, die Leittechnik einer Anlage zur Uran-Anreicherung im Iran zu sabotieren. Damit hat *Stuxnet* eine neue Qualität an Malware eingeleitet, die sehr viel intelligenter ist, viel gezielter vorgeht und vor allem einen sehr viel größeren Schaden anrichten kann. *Stuxnet* markiert den Startpunkt der Entwicklung von qualitativen Cyberwaffen, die Industrien und Infrastrukturen ganzer Länder lahm legen können.

Trends in der IT-Sicherheit
Die zunehmende Vielfalt unserer IT-Endgeräte braucht deutlich verlässlichere und wirkungsvollere Sicherheitskonzepte. Wir müssen weg von den reaktiven hin zu aktiven Sicherheitssystemen, die eine Ausführung von Malware verhindern können. Solche aktiven Sicherheitssysteme arbeiten mit einem Sicherheitskern und Virtualisierung, können Software messbar machen und mit einer starken Isolation, Daten und Anwendungen – und damit den Werten auf unseren Endgeräten - nachhaltige Sicherheit bieten.
Außerdem geht der Trend fort von der Perimeter-Sicherheit, mit der Unternehmen bislang versuchten, mehr oder weniger erfolgreich ihre IT-Außengrenzen abzuschotten. Stattdessen wird eine domänenorientierten Objektsicherheit Raum greifen, bei der die Objekte mit Rechten versehen werden, die definieren, wer sie in welcher IT-Umgebung wie nutzen darf.

Für beide Trends muss die Softwarearchitektur der IT-Endgeräte allerdings grundlegend anders aufgebaut sein als bisher. Außerdem müssen Sicherheits-Infrastrukturkomponenten aufgebaut werden, damit diese Technologien organisationsübergreifend genutzt werden können. Auf der Forschungsebene stehen innovative Sicherheitssysteme, wie z.B. die Open-Source-Technologie Turaya, schon länger zur Verfügung. Die ersten IT-Sicherheitsunternehmen bieten bereits ausgereifte Produkte. Jetzt wird es Zeit, dass diese von der Industrie eingeführt werden, damit eine höhere Sicherheit und Verlässlichkeit der IT-Endgeräte erzielt werden kann.

Cloud-Computing sichert Compliance

Grundsätzlich ist Cloud Computing eine sehr einfache preisgünstige Alternative für den dynamischen IT-Leistungsbezug. Vor allem aber sind einige Compliance- und Sicherheitsaspekte i.d.R. effektiver in Cloud-Umgebungen umzusetzen, als die IT-Ressourcen in vielen Unternehmen selbst das je leisten könnten.
Sehr wichtig ist, dass sich die Unternehmen dafür den richtigen vertrauenswürdigen Anbieter aussuchen. Denn natürlich gibt es eine Abhängigkeit vom Dienstleister, die Auswahl ist entsprechend wichtig. Zum Beispiel muss jedem Unternehmen klar sein, dass amerikanische Cloud-Dienstleister laut Patriot-Act dazu verpflichtet sind, Daten an ihre Regierung weiterzugeben, auch wenn diese das ohne richterlichen Beschluss anfragt, auch wenn die Rechenzentren in Europa stehen. Insofern kommt dem Standort sowie den Besitzverhältnisse von Rechenzenten besonderen Bedeutung zu, in dem Provider ihre Clouds buchstäblich beheimaten.

Autor:
Prof. Dr. Norbert Pohlmann ist Geschäftsführender Direktor des Instituts für Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen.
https://norbert-pohlmann.com/