IT-SICHERHEIT

Neue Techniken gegen Cyberattacken

Von Uwe Sievers | 18. Oktober 2018 | Ausgabe 42

Im Wettlauf um technischen Vorsprung zwischen Angreifer und Verteidiger zeigten Anbieter letzte Woche auf Europas größter Messe für IT-Security, der IT-SA, wie sich der Schutz vor Eindringlingen verbessern lässt.

Foto: NuernbergMesse/Thomas Geiger

Zauberkräfte und Superpower: Das wünschen sich angesichts der vielschichtigen, stetig zunehmenden Cyberattacken viele IT-Anwender. Mit „Deception", einer neuen Täuschungstechnik, werden die Angreifer zumindest schon mal in Firmennetzen in die Irre geleitet.

Es boomt in der IT-Security: Laut Marktforschern von IDC werden 2018 an die 91 Mrd. $ für Sicherheitslösungen ausgegeben. 10 % mehr als noch im Jahr zuvor. Die IT-SA in Nürnberg gilt als Highlight der Branche. Hier überraschten insbesondere kleine und junge Unternehmen mit technologischen Neuerungen.

IT-Sicherheit in Zahlen

Der aktuelle Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI), der am letzten Donnerstag veröffentlicht wurde, ist zu einem 100 Seiten langen Dokument angewachsen.

Er bestätigt: Die Gefährdungslage hat im Vergleich zum Vorjahr zugenommen. BSI-Präsident Arne Schönbohm sprach bei der Vorstellung von einer „besorgniserregenden" Art neuer Cyberangriffe und Vorfälle. Er verwies auf Schadprogramme wie Wanna Cry und NotPetya, aber auch auf Hardwarelücken wie bei Spectre und Meltdown.

Die Bonner Behörde zählte allein 800 Mio. Schadprogramme und damit 200 Mio. mehr als letztes Jahr. Täglich kämen 390 000 neue Varianten hinzu, attestiert der jüngste Lagebericht. Ebenso nehme die Geschwindigkeit der Angriffe zu.

Laut jüngster Studie des Branchenverbands Bitcom waren in den vergangenen zwei Jahren sieben von zehn Industrieunternehmen Opfer von Wirtschaftsspionage, Sabotage oder Diebstahl. Der dadurch entstandene Schaden summierte sich im Untersuchungszeitraum auf 43 Mrd. €.

Für 2018 erwartet der Branchenverband, dass in Deutschland mit Hardware, Software und Services für IT-Sicherheit voraussichtlich 4,1 Mrd. € umgesetzt werden, also 9 % mehr als im Vorjahr. Der Löwenanteil, nämlich 2,2 Mrd. €, entfiel auf Dienstleistungen. rb

Der Markt habe sich verändert, hat Rik Turner beobachtet. Er hält als Chefanalyst für IT-Security beim Marktforscher Ovum seine Nase in den Wind. Turner erklärt: „Während Sicherheitssoftware in den 1990er- und 2000er-Jahren fast ausschließlich die Abwehr von Schadsoftware verfolgte, liegt der Schwerpunkt heute eher auf der Erkennung von Eindringlingen und deren Beseitigung sowie der Schadensminimierung." Die Ursache ist für Turner ganz klar: „Cybercrime ist ein eigener Markt geworden und Angriffswerkzeuge zur Massenware", weswegen „Attacken sich für wenig Geld realisieren lassen".

Angreifer in die Irre führen: Folgerichtig ist für Turner „Deception" eine neue Technik mit vielversprechendem Potenzial. Die namensgebende Irreführung oder Täuschung besteht darin, Angreifer in einen Irrgarten zu locken: Für potenzielle Eindringlinge werden in Firmennetzen attraktive Köder ausgelegt. Das können vielversprechende Zugangsdaten, wichtige Server mit Unternehmensdateien oder Ähnliches sein.

Turner beschreibt es als ein geschickt „arrangiertes System aus Honeypots". Mit im Internet aufgestellten Honigtöpfen werden Angreifer außerhalb des Firmennetzes angelockt, um sie vom wirklichen Ziel abzulenken. Deception soll für Eindringlinge innerhalb des Unternehmens ein Labyrinth bilden, in dem sie sich verfangen. So können ihre Vorgehensweise und Ziele analysiert werden, erklärt Turner. Zentrale Management-Tools erlaubten eine spontane Umkonfiguration und ein Refresh aller Komponenten, damit letztlich auch den Rausschmiss des Angreifers.

Die Technik sei allerdings eher für große IT-Netze geeignet, fügt Turner hinzu, und lasse ein solches Netz noch größer wirken. So würden durch Deception 5000 Computer als 25 000 erscheinen. Zu den Anbietern dieser Technologie gehört unter anderem das israelische Unternehmen Illusive Networks.

Datenflüsse kontrollieren und unterbinden: Eine weitere Neuentwicklung nennt sich „Mikrosegmentierung". Deren Funktionsweise beschreibt Stefan Strobel, Geschäftsführer und Gründer des Sicherheitsspezialisten Cirosec, so: „Softwareagenten auf den einzelnen Geräten analysieren, welche Maschinen miteinander reden und welche Daten sie dabei austauschen."

Im zweiten Schritt würden die Ergebnisse in eine Kommunikationsmatrix überführt. Dadurch würden Datenaustausch und Abhängigkeiten zwischen den Maschinen sichtbar und Soll- mit Istzustand vergleichbar. Regelmäßig stelle sich heraus, dass mehr ausgetauscht wird als gedacht, insbesondere, wenn Cloud-Anwendungen zum Einsatz kommen. „Deshalb werden Kommunikationsmöglichkeiten anschließend bei jedem Gerät auf das für die vorgesehene Aufgabe notwendige Minimum reduziert, zum Beispiel soll eine Datenbankanwendung nur mit dem Datenbankserver in Verbindung treten", erklärt Strobel.

Aus den Ergebnissen würden automatisch Firewall-Regeln erstellt, die auf den betreffenden Computern installiert werden. Denn so ziemlich jedes System käme heute mit einer eingebauten Firewall, oftmals würden diese aber nicht genutzt. Zu den Anbietern dieser Technologie gehört u. a. das 2013 gegründete Unternehmen Illumio, zu dessen Kunden bereits Oracle, Salesforce oder die Bank PNB Paribas gehören.

Virtuelles Netz ersetzt Standleitungen: Ein rasantes Wachstum beobachten Experten bei einer neuen Technik für Weitverkehrsnetze: „SD-WAN“. Die Technik hat nur auf den ersten Blick wenig mit IT-Sicherheit zu tun. Ähnlich, wie in Rechenzentren durch Software-Definierte-Netzwerke (SDN) die Hardware von der Software entkoppelt wird, geschieht dies nun auch im WAN-Bereich.

„Betreiber erhoffen sich davon neben flexiblerer Konnektivität bei niedrigeren Kosten mehr Verfügbarkeit, geringere Latenz – also besseres Antwortverhalten – und eine vereinfachte Administration durch die geringere Komplexität“, erklärt Mark Sobol, Leiter des Fachbereichs Security beim Systemhaus SVA. Jedoch ist die Sicherheit aus seiner Sicht noch einer der Schwachpunkte dieser Netzwerktechnologie.

Neue Anbieter wie Netfoundry haben genau das erkannt und stellen Security ins Zentrum ihrer Lösungen. Denn durch erhöhte Kontrolle und Steuerbarkeit ergeben sich neue Möglichkeiten zur Absicherung. Dabei bündelt SD-WAN vorhandene Technologien wie LTE oder MPLS (Multiprotocol Label Switching, die verbindungsorientierte Übertragung von Datenpaketen).

Softwaregesteuert kann von einer Verbindungsvariante auf eine andere umgeschaltet werden, etwa bei der Anbindung von Filialen oder der Cloud. Dementsprechend ist diese Technologie besonders für große verteilte Firmennetze interessant. „Wer weltweit mehr als 20 Standorte hat, sollte sich damit beschäftigen“, rät Mark Sobol.

Mehr Sicherheit durch mehr Verständnis: „Das Problem sitzt vor dem Computer“, heißt es spöttisch in der Security-Branche. Schulungen liegen im Trend, jedoch hat sich die Vorgehensweise verändert. Ausgefeilte Awareness-Schulungen sollen bei den Mitarbeitern Bewusstsein für Gefahren schaffen und werden in zahlreichen Varianten angeboten. Die Angebote unterscheiden sich stark, gemeinsam haben sie, dass die Schulungen, für die junge Start-ups eigene Tools entwickelt haben, online durchgeführt werden.

Mitarbeiter werden dabei zunächst aufs Glatteis geführt: Sie bekommen fingierte Phishing-Mails, um zu prüfen, ob sie auf darin enthaltene Links klicken. Das gerade von der auf Schulungen spezialisierten Firma KnowBe4 aufgekaufte Start-up Exploqii bietet seine Cloud-basierte Lernplattform mit eigenen Lerninhalten in 30 Sprachen an. Anbieter IT-Seal misst zunächst das Awareness-Niveau der Mitarbeiter und verfolgt nach den Schulungsmaßnahmen die Veränderungen. Das kleine Unternehmen SoSafe wartet dagegen mit speziellen Branchenlösungen auf.