Internet Security Threat Report 2017

Executive Summary

Die Bedrohungslage spitzt sich zu.

Die Professionalisierung der Cyber-Attacken nahm 2016 abermals zu. Zu den unrühmlichen Höhepunkten zählten virtuelle Bankeinbrüche, bei denen Millionen von Dollar gestohlen wurden, die Manipulation der US-Wahl sowie die bis dato größten DDoS-Attacken über gekaperte IoT-Endpoints. Auch die dadurch verursachten Schäden waren höher denn je.

Symantec

Destabilisierende Attacken auf die US-Wahl
Geheimdienste agieren meist im Verborgenen. 2016 erhielt die Öffentlichkeit einen Einblick in die Arbeit der Cyberspione: Nach einem Angriff auf die US-Demokraten versuchten die Hacker, durch die Veröffentlichung vertraulicher Dokumente den US-Wahlkampf zu beeinflussen. Die US-Geheimdienste geben an, dass die Angriffe aus Russland stammten und bewerten sie als Erfolg. Wir müssen also damit rechnen, dass diese Taktik auch in Zukunft zum Einsatz kommen wird.

Cyberangriffe zur Sabotage sind eher selten. Doch 2016 wurden gleich zwei dieser Attacken dokumentiert. In der Ukraine verursachten Angreifer im Januar und Dezember mithilfe festplattenlöschender Malware Stromausfälle, in Saudi-Arabien wurde eine Reihe von Einrichtungen mit dem Trojaner Shamoon attackiert.

Verdeckte Attacken zur Wirtschaftsspionage oder zum Diebstahl von geistigem Eigentum gingen dafür zurück. Dies ist womöglich auf ein 2015 gezeichnetes Abkommen zwischen den USA und China zurückzuführen, das beide Länder verpflichtet, auf Wirtschaftsspionage im Internet zu verzichten.

Der große Coup: Angriffe auf das Finanzwesen
2016 machten zwei Hacker-Crews mit verheerenden Attacken gegen das Finanzwesen von sich reden: Die Gruppe Banswift infiltrierte über eine Sicherheitslücke das Netzwerk der Zentralbank von Bangladesch und stahl 81 Millionen US-Dollar sowie die SWIFT-Codes der Bank, die dann für Überweisungen missbraucht wurden.

Die Gruppe Odinaff nutzte eine spezielle Malware, um Banken zu infiltrieren und unbemerkt SWIFT-Überweisungen durchzuführen. Aber auch mit weniger raffinierten Mitteln werden immer wieder hohe Summen erbeutet. In den letzten drei Jahren wurden allein mit gefälschten Business-E-Mails und Spear-Phishing über 3 Millarden US-Dollar gestohlen.

Angriffe mit Bordmitteln
Viele Angreifer setzen bei Attacken vermehrt auf klassische Remote-Management-Tools, Betriebssystemfeatures und Cloud-Services. Das beste Beispiel für solche Angriffe mit Bordmitteln geschah im US-Wahlkampf: Über eine einfache Spear-Phishing-Mail verschafften sich Hacker Zugang zum Gmail Account von John Podesta, dem Leiter der Hillary-Clinton-Kampagne, ohne dass dafür Malware nötig gewesen wäre.

Der Griff zum Bordmittel ist leicht erklärt: Initiativen für eine sichere Software-Entwicklung und hohe Prämien für gemeldete Schwachstellen haben dafür gesorgt, dass Zero-Day-Exploits heute weitaus seltener sind als früher. Daher missbrauchen Angreifer lieber Scripting-Tools wie PowerShell oder Macros in Windows und Microsoft Office, um Systeme zu übernehmen oder mit Malware zu infizieren.

Das Risikopotenzial dieser Attacken ist dabei enorm: Wenn die Malware geschickt über legitime Systeme eingeschleust wird, ist die Infektion kaum zu erkennen.

E-Mail ist wieder der gefährlichste Angriffsvektor
Für die meisten Angreifer waren als Angriffsvektor infizierte E-Mails 2016 die erste Wahl. Im Schnitt entfiel ein Angriff auf 131 versendete E-Mails – die höchste Quote der vergangenen fünf Jahre. Auch bei der Verbreitung von Ransomware kamen vielfach infizierte E-Mails zum Einsatz, oft als Rechnungen oder Auftragsbestätigungen getarnt. Mietbare Spambot-Netze wie Necurs ermöglichten es Angreifern, bei großangelegten Kampagnen täglich Hunderttausende von E-Mails zu verschicken.

An die Stelle von Zero-Day-Attacken und mehrstufiger Malware treten Spear-Phishing und der Missbrauch vorhandener Management-Tools.

Erpressung durch Ransomware
Ransomware war für Anwender und Unternehmen 2016 die wohl größte Bedrohung. In einigen Unternehmen brachen die Mail-Systeme unter der Last infizierter E-Mails zusammen. Auch die Forderungen der Angreifer steigen rasant: Aktuell liegen sie im Schnitt bei 1.077 US-Dollar, 294 US-Dollar über dem Vorjahr. Die Kombination aus mit Malware infizierten E-Mails, unknackbarer Verschlüsselung und nicht zurückverfolgbaren Zahlungsströmen war so erfolgreich, dass zahllose Trittbrettfahrer auf den Ransomware-Zug aufgesprungen sind: Die Zahl neu entdeckter Ransomware-Familien hat sich 2016 auf 101 mehr als verdreifacht, die Zahl der Infektionen stieg um 36 Prozent.

IoT und Cloud zunehmend im Fokus
Auch wenn von Ransomware und Phishing die größte Gefahr ausgeht, zeichnet sich die nächste Threat-Generation bereits ab: Angriffe auf IoT-fähige Geräte haben sich 2016 verdoppelt, in Spitzenzeiten werden diese alle zwei Minuten attackiert. Wohin dies mündet, zeigt das 2016 entdeckte, aus Routern und Sicherheitskameras bestehende Botnetz Mirai, das für Angriffe auf Infrastrukturdienste wie Dyn DNS genutzt wurde. Dies legt den Schluss nahe, dass Cloud-Angriffe 2017 weiter zunehmen werden. Unternehmen sollten sicherstellen, dass sie gegen diese Bedrohungen geschützt sind. Unternehmen haben heute im Schnitt 928 Cloud-Apps im Einsatz. Die meisten CIO gehen von maximal 30 oder 40 Apps aus – und unterschätzen die Abhängigkeit und Gefahr, die mit diesen Anwendungen einhergeht.

Symantec (Deutschland) GmbH, Wappenhalle,
Konrad-Zuse-Platz 2-5, 81829 München, T.: +49 (0)89 94302-0

Den vollständigen Bericht finden Sie unter http://symc.ly/2qwYc6m sowie unter www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Symantec