27.12.2019 – 09:00 Uhr

Bedrohungen durch Hacker: Das erwartet Unternehmen in 2020

USA (ots) -

Kaum etwas ändert sich so dynamisch wie Cyber-Gruppierungen: Sie entstehen, pausieren, schließen sich neu zusammen, lösen sich auf und nutzen ständig neue Tools und Taktiken. Michael Sentonas, VP of Technology Strategy bei CrowdStrike, hat deshalb die fünf wahrscheinlichsten Entwicklungen zusammengefasst, die Unternehmen im nächsten Jahr begegnen könnten. Er fokussiert sich hierbei auf die Angriffsmethoden, die am ehesten genutzt werden und gibt Anhaltspunkte, wie sich Unternehmen gegen diese Art von Angriffen schützen können.

Gezielte Ransomware-Angriffe auf Unternehmen nehmen zu

Ransomware verfolgte bisher eher das Ziel, Privatleute um ihr Geld zu bringen. Seit einiger Zeit hat dieser Angriffsvektor jedoch neue Monetarisierungsmöglichkeiten entdeckt und Hacker erpressen vermehrt hohe Lösegeldsummen von Unternehmen. Angreifer haben erkannt, dass Unternehmen und Regierungen wertvolle Informationen, mehr Geld für Lösegeldzahlungen und oft eine unzureichende Cyber-Hygiene haben. Bereits 2019 legten Hacker in den USA über 70 staatliche und lokale Regierungen mit Ransomware lahm. Die Ryuk-Ransomware traf Hunderte Schulen. Mehrere US-Organisationen berichteten außerdem von Lösegeldzahlungen in einer Größenordnung von Hunderttausenden bis fast einer halben Million US-Dollar. Hacker weltweit beobachten diese Entwicklung und erkennen, wie lukrativ Ransomware-Angriffe auf Unternehmen sind. Sie nehmen deshalb immer weiter von der Spray-and-Pray-Methode Abstand, organisieren sich und ihre Operationen globaler und erzielen damit immer größere Geldsummen.

Vermehrte Angriffe auf SMB-Protokoll

Dass alte Schwachstellen großen Schaden verursachen, ist bekannt und wird sich in 2020 nicht ändern. Angreifer bemühen sich, die Entwicklung von Exploits zu verstärken, die Schwachstellen im Microsoft Server Message Block (SMB)-Protokoll ausnutzen. Und aller Voraussicht nach werden sie großen Erfolg damit haben. Ransomware wie Ryuk ermöglicht es, dass sich ein Angriff auf nur ein einzelnes infiziertes Gerät schnell im gesamten Unternehmen verbreitet. Dies deutet darauf hin, dass Exploits, die bei den Ransomware-Angriffen von 2017 verwendet wurden, weiterhin die Millionen von noch nicht gepatchten Endpunkten ins Visier nehmen werden.

Der Iran wird aktiver

Iranische Cyber-Kriminelle haben in den letzten Jahren einige der zerstörerischsten Angriffe verübt. Die Erkenntnisse aus 2019 deuten darauf hin, dass sich aus dem Iran organisierte Cyber-Gruppierungen im kommenden Jahr verstärkt auf destruktive Cyberangriffe konzentrieren und schon jetzt die Grundlagen dafür legen. Bloße Cyberspionage und das Sammeln von Informationen treten in den Hintergrund. Iranische Cyber-Kriminelle nutzen fortschrittliche Fähigkeiten und Techniken, zu denen auch die Entwicklung destruktiver Malware gehört. Regierungen auf der ganzen Welt könnten somit in das Visier destruktiver und folgenschwerer Aktionen geraten, die von aus dem Iran koordinierte Hacker-Gruppen verübt werden.

Balkanisierung des Internets zum Schutz nationaler Interessen und Infrastrukturen

Die Balkanisierung des Internets wird aufgrund technologischer, politischer, wirtschaftlicher und nationaler Agenden weiter fortgesetzt. Sie bezieht sich auf die Segmentierung eines globalen offenen Internets in mehrere kleinere Bereiche, die meist an geopolitischen Grenzen ausgerichtet sind. Im Jahr 2020 werden Regierungen - wie China, Russland oder der Iran - weitere Anstrengungen unternehmen, um das Internet in ihrem Sinne für sich zu nutzen. Eine stärkere Nutzung der Technologiebereiche zum Schutz nationaler Interessen und Infrastrukturen wird zu beobachten sein. In dem Zusammenhang ist auch die vierjährige Teilnahmesperre russischer Athleten bei internationalen Wettbewerben wie den Olympischen Spielen in Tokio 2020 interessant. Von Russland organisierte Angreifer werden darauf höchstwahrscheinlich mit gezielten Cyber-Operationen reagieren.

Grenzen zwischen staatlichen Angriffen und eCrime-Aktionen verschwimmen

Seit mehreren Jahren verschwimmen die Grenzen zwischen nationalstaatlichen und eCrime-Akteuren. Dieser Trend verschärft sich zusehends. Das liegt nicht nur daran, dass die eCrime-Akteure immer anspruchsvoller werden, sondern auch daran, dass staatlich geförderte, gut ausgebildete Gegner dazu übergehen, ganz bewusst weniger fortgeschrittene Techniken und Taktiken zu verwenden, um eine Zuordnung ihrer Aktivitäten zu erschweren.

Unabhängig davon, ob es sich um nationalstaatliche Angreifer, eCrime-Akteure oder Hacktivisten handelt: Die beste Verteidigung für Unternehmen ist es, fortschrittliche Cybersecurity-Lösungen der nächsten Generation einzusetzen, die auf Endpunkterkennung und -reaktion (EDR), Managed Threat Hunting, Next Generation AV (inkl. Verhaltensanalyse und maschinellem Lernen) sowie automatisierte Threat Intelligence setzen. Eine solche Lösung bietet beispielsweise die CrowdStrike Falcon-Plattform. Tools, die diese Funktionalitäten abdecken, sind der Schlüssel zu mehr Transparenz und Kontext, um kritische und ergebnisorientierte Kennzahlen zu erfüllen und den Wettlauf selbst gegen die anspruchsvollsten Gegner zu gewinnen.

Kontakt:

PIABO PR GmbH
Caroline Jechow | Senior Account Manager
E-Mail: crowdstrike@piabo.net
Telefon: +49 30 2576 205 261