28.12.2018 – 11:11 Uhr

Das waren die Trends bei Cyberattacken 2018

Kalifornien (ots) -

Die Anzahl destruktiver Cyber-Angriffe hat auch in 2018 weiter zugenommen. Kriminelle Hacker-Gruppen haben ihre Effektivität erhöht, agieren frei von geographischen Gegebenheiten und quer durch alle Industrien. Sie sind unermüdlich auf der Suche nach Lücken in der IT-Infrastruktur von Organisationen. Und wo Tore offen stehen, machen sie von der Chance Gebrauch. Ihre Ziele sind dabei geopolitischer oder finanzieller Natur.

Das Cybersecurity-Unternehmen CrowdStrike hat in seinem letzten Report, dem Cyber Intrusion Casebook, große Mengen an sicherheitsrelevanten Daten aus 2018 analysiert. Es fasst darin zusammen, welchen Herausforderungen Organisationen und Unternehmen gegenüber stehen und wie sie sich besser auf die nächste Angriffswelle vorbereiten können. Vier Trends sind bei den Angriffstaktiken und -Methoden erkennbar.

1. E-Crime-Akteure wenden immer kreativere Techniken an, um ihre Angriffe zu monetarisieren.

Die Innovationskraft von Angreifern und die Raffinesse der E-Crime-Akteure nimmt nicht ab. Das feindliche Ökosystem entwickelt sich weiter und Akteure, die früher diskret und isoliert gearbeitet haben, arbeiten nun koordiniert und bündeln ihre Kräfte. In 2018 bekamen das beispielsweise immer wieder Nutzer von Geschäfts-E-Mail-Adressen zu spüren. Der Report stieß auf Fälle, die weit über das einfache Lesen von E-Mails hinausgingen: Die Akteure konnten live zusehen, wie die E-Mails geschrieben und gesendet werden.

2. Angreifer schlagen schnell und tiefgreifend zu. Sie sind geduldig, wenn es darum geht, ihre Ziele zu erreichen.

Sie gelangen schnell in die Systeme, werden schnell aktiv, bringen aber, wenn es darauf ankommt, enorme Geduld auf. Staatliche Angreifer sind dabei besonders hartnäckig und einfallsreich bei der Suche nach hochwertigen Daten in der Zielorganisation.

Wie in den Vorjahren bot das unkritische Vertrauen in Legacy-Tools Angreifern die Möglichkeit, sich über einen längeren Zeitraum in den Systemen aufzuhalten. Oft dachten zum Beispiel Unternehmen, dass der Fall gelöst sei. Doch der Angreifer versteckte sich weiter oder war schnell zurück.

Oft migrierten Unternehmen ihre Daten in die Cloud, in der Erwartung, dass die Cloud-Services-Anbieter Sicherheitsmechanismen und -kontrollen haben. Ob die Anbieter die Kontrollen richtig konfiguriert und angewendet haben, konnten sie nicht wissen. Einfache Fehlkonfigurationen und Missverständnisse bei den Zugriffskontrollen ermöglichen Hackern, Zugang zu einem Unternehmen zu erhalten - ganz einfach über den Cloud-Anbieter.

3. Commodity-Malware ist oft ein Vorläufer eines stark disruptiven Angriffs.

Der mit Commodity-Malware (bösartiger Code, der sich auf eine Software auswirkt, die auf einer Vielzahl von Geräten eingesetzt wird) gewonnene Zugang wird zunehmend an andere Akteure verkauft. Die setzten dann Ransomware ein, stehlen geistiges Eigentum oder initiieren Kryptomining, Betrug und Erpressung. Es wurde zum Beispiel beobachtet, wie Angreifer eine Malware-Familie namens TrickBot benutzten, nur um den damit gewonnenen Zugriff an andere feindlich gesinnte Gruppen weiterzugeben, die daraufhin Erpressungsangriffe starteten. Diese Methode wurde sogar bei kleinen bis mittleren Unternehmen beobachtet. Die Anfälligkeit eines Unternehmens für Commodity-Malware kann letzten Endes ein Indikator für die Wirksamkeit der gesamten Sicherheitsstrategie sein.

4. Angreifer verstecken sich vor aller Augen und geben sich als legitime Nutzer aus.

Die schnellsten und schädlichsten Angriffe sind nach wie vor diejenigen, bei denen sich Angreifer als legitime Benutzer ausgeben. Sie treten häufig auf, wenn Benutzer-Anmeldeinformationen unkontrolliert, falsch konfiguriert oder umgangen werden. Sobald der Zugriff erfolgt ist, ist das Unternehmen vollständig exponiert. Falsch konfigurierter und undurchdachter Einsatz von Zugriffskontrollen vermittelt Unternehmen oft ein falsches Schutzgefühl.

Angesichts dieser Trends wird ebenfalls ersichtlich, dass Cybersecurity nicht nur ein Thema für die IT-Abteilung ist, sondern das ganze Unternehmen betrifft und strategisch mitbedacht werden muss. Als goldene Regel bietet sich das Zeitziel der "1-10-60-Regel". Im Durchschnitt sollten Unternehmen beziehungsweise Organisationen nicht mehr als eine Minute Zeit lassen, um eine Bedrohung zu erkennen, zehn Minuten, um sie zu untersuchen und 60 Minuten, um sie zu beheben. Unternehmen, die mit diesem Anspruch handeln, erhöhen ihre Chancen, dem Gegner voraus zu sein und einen Angriff zu verhindern.

Über CrowdStrike

CrowdStrike ist der führende Anbieter von Cloud-basiertem Schutz von Endgeräten. Die CrowdStrike Falcon® Plattform nutzt künstliche Intelligenz (KI), bietet sofortige Transparenz sowie Schutz im gesamten Unternehmen und verhindert Angriffe auf Endgeräte im oder außerhalb des Netzwerks. CrowdStrike Falcon ist in wenigen Minuten einsatzbereit und bietet vom ersten Tag an nutzbare Erkenntnisse und Echtzeitschutz. Es vereint nahtlos AV der neuesten Generation mit erstklassiger Endpoint Detection und Response (EDR), unterstützt durch eine 24/7 verwaltete Nachverfolgung. Die Cloud-Infrastruktur und die Single-Agent-

Architektur reduzieren Komplexität, verbessern die Verwaltung und erhöhen Skalierbarkeit und Geschwindigkeit. CrowdStrike Falcon schützt Kunden vor allen Arten von Cyber-Angriffen, indem es eine hochentwickelte, signaturlose Bedrohungsabwehr verwendet, die auf KI und Indicator of Attack (IOA) basiert, um bekannte und unbekannte Bedrohungen in Echtzeit zu stoppen. Mit dem CrowdStrike Threat Graph[TM] überprüft Falcon wöchentlich eine Billion Ereignisse pro Woche, um Angriffe sofort zu erkennen und zu verhindern.

Kontakt:

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