PHARMATECHNIK-ONLINE
Das Fachportal für die pharmazeutische Industrie
https://www.pharmatechnik-online.com

Unternehmen erkennen Cyberattacken zu langsam

Kategorie: Organisation und Service

Datum: 31. Dezember 2018

CrowdStrike, Anbieter von Endpoint-Protection-Lösungen aus der Cloud, veröffentlichte mit dem CrowdStrike Cyber Intrusion Casebook 2018 einen Report, der Hacker-Aktivitäten und sicherheitsrelevante Vorfälle aus diesem Jahr an Beispielen verdeutlicht und Trends zusammenfasst. Der Report gibt Einblicke in die Angriffsmethoden und Techniken verschiedener Hacker-Gruppen und analysiert mögliche Reaktionen und Verfahren für Incident-Response-Teams. Darin enthalten sind auch Empfehlungen an Unternehmen, die ihre kritischen Daten zuverlässig schützen wollen und die Angriffserkennung, die Vorbereitung sowie die Reaktion auf Attacken verbessern möchten.

Die Trends sind aus mehr als 200 analysierten Cyberangriffen abgeleitet, die eine Vielzahl an Branchen getroffen haben. Für sieben Fälle analysiert das Casebook detailliert das Verhalten der Angreifer, ihre Motivation und Taktik sowie die Reaktionsmöglichkeiten. Einige der Fallbeschreibungen bieten eine umfassende, forensische Analyse von Artefakten, die bei mehreren Angriffen entdeckt wurden und erlauben so, Best Practices für Unternehmen abzuleiten.

Wichtige Ergebnisse der Studie

Unternehmen machen bei der Erkennung von Angriffen (Intrusion Detection) und der Abwehr von Cyberattacken keine großen Fortschritte. In diesem Jahr haben 75 Prozent der von CrowdStrike betreuten Unternehmen ein Eindringen in ihre Systeme aufdecken können – eine Steigerung von lediglich sieben Prozent gegenüber dem Vorjahr. Dies deutet darauf hin, dass Unternehmen ihre Fähigkeiten beim Aufdecken von Angriffen nur geringfügig verbessert haben. Die Verweildauer der Angreifer blieb mit durchschnittlich 85 Tagen (gegenüber 86) ebenfalls relativ konstant. Die Verweildauer entspricht der Anzahl der Tage zwischen der ersten nachträglich festgestellten Kompromittierung und ihrer tatsächlichen Erkennung.

Rund 20 Prozent der Angriffe geschahen mit Powershell oder Windows Management Instrumentation (WMI). Die Taktik „Living off the Land" (LotL) senkt den Aufwand für die Cyberkriminellen und wird deshalb immer öfter angewendet. Sie stellt somit eine große Herausforderung für Unternehmen dar.

Viele Cyberkriminelle bereiten schwere, langanhaltendende Angriffe mit Commodity-Malware vor. Wenn Hacker Zugang zu Systemen erlangt haben, verkaufen sie häufig die Daten und nutzen sie, um zunächst vorgefertigte Ransomware oder Trojaner für Kryptomining zu betreiben. Diese Muster sind häufig die Vorläufer größerer und langanhaltender Angriffe.

Angriffe durch Social Engineering und Phishing sind dramatisch angestiegen. Im letzten Jahr stieg die Zahl von Angriffen auf der Basis von Social Engineering, Phishing und Spear-Phishing dramatisch an. Dieses Segment der Cyberangriffe wuchs von 11 Prozent im letzten Jahr auf 33 Prozent im Jahr 2018, und macht somit ein Drittel aller von CrowdStrike untersuchten Angriffe aus. Angriffe auf Webserver sind das größte Segment der Einzelangriffsvektoren, gingen aber gegenüber den 37 Prozent des Vorjahres auf knapp 20 Prozent zurück.

Effizienter Schutz vor dynamischen Bedrohungen

„Cyberangriffe nehmen weiterhin zu und Cyberkriminelle sowie staatliche Angreifer steigern ihre Raffinesse. Es ist für Unternehmen essentiell, sich über aktuelle Angriffstrends und die Motivation der

Cyberkriminellen zu informieren, um Cybersicherheit proaktiv zu begegnen“, sagt Shawn Henry, Chief Security Officer und President von CrowdStrike Services. „Es ist nicht die Frage, ob sie ins Visier genommen werden: Das passiert jedem. Es handelt sich hier um ein klares Geschäftsrisiko. Vorstände und Geschäftsführer müssen ein Gefühl für die Dringlichkeit des Themas haben, um ihre Unternehmen zu schützen. Das CrowdStrike Services Casebook bietet ihnen wertvolle Einblicke in die proaktive Vorbereitung auf Cyberangriffe und effiziente Reaktionen.“

Das Casebook 2018 bietet Leitlinien für einen effizienten Schutz in der sich ständig verändernden Bedrohungslandschaft von heute. Dazu gehören auch die Integration von Endpoint Protection der nächsten Generation sowie proaktive Strategien zur Steigerung der Cyber-Resilienz. Machine Learning und Verhaltensanalyse helfen, Missbräuche und unbekannte Bedrohungen zu erkennen. Eine proaktive Suche nach Bedrohungen kann auch sehr vorsichtig agierende Angreifer aufdecken. Darüber hinaus verhindern effiziente Security-Lösungen, das kleinere Angriffe für die Unternehmen zu einer großen und kostspieligen Bedrohung werden.