20.11.2019 – 12:40 Uhr

Zu langsam, um Hackern das Handwerk zu legen - Unternehmen weltweit benötigen über sechs Tage, um Hacker aus ihren Systemen zu verbannen

Kalifornien (ots) -

CrowdStrike (Nasdaq: CRWD), ein führender Anbieter von Cloud-basiertem Endgeräteschutz, gab heute die Veröffentlichung des CrowdStrike Global Security Attitude Survey 2019 bekannt, die vom unabhängigen Forschungsunternehmen Vanson Bourne erstellt wurde. Im Rahmen der Studie wurden 1.900 hochrangige IT-Entscheidungsträger und IT-Sicherheitsexperten in den USA, Kanada, Großbritannien, Mexiko, dem Nahen Osten, Australien, Deutschland, Japan, Frankreich, Indien und Singapur aus allen wichtigen Industriesektoren befragt. Der Bericht befasst sich mit den Einstellungen und Überzeugungen der Cybersicherheitsverantwortlichen und ermittelt, wie sie sich gegen gut ausgestattete nationalstaatliche Angreifer behaupten.

Die Umfrage ergab, dass Unternehmen weltweit im Durchschnitt über sechs ganze Tage (insgesamt 162 Stunden) benötigen, um Cyberangriffe zu entdecken, auszuwerten und zu beheben. Durchschnittlich brauchen sie 31 Stunden, um einen Cyberangriff einzudämmen, nachdem sie ihn erkannt und untersucht haben. Infolgedessen gibt die Mehrheit der Befragten (80%) an, dass sie in den letzten zwölf Monaten nicht in der Lage waren, Eindringlingen in ihrem Netzwerk den Zugriff auf ihre Zieldaten zu verwehren. Die Ursache hierfür sehen 44 Prozent in einer langsamen Erkennung.

Unternehmen aus den wichtigsten Branchen weltweit sind folglich nicht ausreichend darauf vorbereitet, innerhalb der Breakout-Zeit auf Angriffe der größten Cybergegner zu reagieren. (Breakout-Zeit = die kritische Zeitspanne, die ein Eindringling benötigt, um in weitere Systeme eines Netzwerks vorzudringen, nachdem er den ersten Endpunkt kompromittiert hat). Zukunftsorientierte Unternehmen sollten versuchen, so gut wie möglich die 1-10-60-Regel zu beherzigen: Bedrohungen in einer Minute erkennen, in zehn Minuten untersuchen und in 60 Minuten beheben.

Einige der wichtigsten Ergebnisse des Berichts sind:
- Derzeit kommen 95 Prozent der Befragten nicht annähernd an diese Best Practice-Empfehlung heran.
- Nur 11 Prozent der befragten Unternehmen können einen Eindringling in weniger als einer Minute erkennen, nur neun Prozent können einen Vorfall in zehn Minuten untersuchen, nur 33 Prozent können einen Vorfall in 60 Minuten eindämmen, und nur fünf Prozent können alle drei Maßnahmen in der empfohlenen Zeit durchführen.
- Obwohl 86 Prozent die einminütige Erkennung als "Game-Changer" der Cybersicherheit für ihr Unternehmen ansehen, ist die Erkennung von Eindringlingen für nur 19 Prozent der Befragten der primäre Schwerpunkt in der IT-Sicherheit.

Der Global Threat Report 2019 von CrowdStrike (http://ots.de/pBTEpr) bietet Unternehmen wertvolle Einblicke in die verschiedenen Breakout-Zeiten von Cyberkriminellen. Der Bericht zeigt, dass russische Angreifer die schnellsten aller Cyber-Akteure sind und in weniger als 19 Minuten von ihrem ursprünglichen Startpunkt aus agieren können. Die langsamsten Gegner (eCrime-Akteure) benötigen knapp zehn Stunden. Somit zeigt die Global Security Attitude Umfrage, dass die Unternehmen nicht in der Lage sind, die aktuell operierenden großen Cybergruppierungen zeitnah zu erkennen, zu verstehen oder zu unterbinden, um Bedrohungen für die eigenen Organisationsnetzwerke zu verhindern.

Die Bedenken der Unternehmen bezüglich der Art der Angriffe waren im Bericht auch unterschiedlicher Natur. Zu den wichtigsten Erkenntnissen gehören:
- 2019 gaben 34 Prozent der Befragten an, bereits mehrfach Opfer eines Angriffs auf die Software-Lieferkette geworden zu sein (im letzten Jahr oder davor). Diese Zahl hat sich im Vergleich zu 2018 (16 Prozent) somit mehr als verdoppelt. Konträr dazu ist jedoch die Angst vor Angriffen auf die eigene Lieferkette von 33 Prozent (in 2018) auf 28 Prozent gesunken.
- In gleicher Weise hat sich auch die Zahl der Unternehmen, die Lösegelder zahlen, um die bei einem Angriff auf die Software-Lieferkette verschlüsselte Daten wiederherzustellen, von 14 Prozent auf 40 Prozent fast verdreifacht. Die Analyse zeigt, dass über 50 Prozent der Lebensmittel- und Getränkeindustrie, des Gastgewerbes sowie der Unterhaltungs- und Medienindustrie in den letzten zwölf Monaten Lösegelder gezahlt haben.
- Durchschnittlich 83 Prozent der Befragten glauben, dass nationalstaatlich initiierte Angriffe eine klare Gefahr für Unternehmen in ihrem Land darstellen, wobei Indien (97%),

Singapur (92%) und die USA (84%) sich am stärksten durch nationalstaatliche Angriffe bedroht sehen.

"Egal woran es liegt - am Wille, zu handeln oder an der Fähigkeit, angemessen zu handeln - es gelingt den Unternehmen nicht, die Reaktionsgeschwindigkeit zu erreichen, die erforderlich ist, um anspruchsvolle nationalstaatliche Gegner, die auf alle Arten von Organisationen abzielen, zu erkennen", sagt Thomas Etheridge, Vice President von CrowdStrike Services. "Es besteht nach wie vor ein großes Vertrauen in die bestehende Legacy-Infrastruktur. Diese wird allerdings den heutigen Sicherheitsanforderungen, die einen ganzheitlichen Ansatz erfordern, um Bedrohungen zu stoppen, nicht gerecht. Zukunftsorientierte Unternehmen sollten deshalb einen plattform-basierten Ansatz verfolgen, der den Teams umfassende Transparenz und Schutz bietet, um ein breites Spektrum an Sicherheits- und Betriebsanforderungen zu erfüllen."

CrowdStrike Falcon wurde als einzige transformative Cloud-native Single-Agenten-Lösung entwickelt und setzt einen neuen Standard in der Endpunkt-Sicherheit. Heute integriert die Falcon-Plattform 11 Cloud-Module, die sich über mehrere Funktionen erstrecken, darunter Endpoint-Sicherheit, Sicherheitsvorgänge und Bedrohungsinformationen, um den Kunden den umfassenden Schutz zu bieten, der notwendig ist, um die komplexen Angriffe der heutigen Zeit zu verhindern. Der einzigartige Ansatz von CrowdStrike beginnt mit einem intelligenten leichtgewichtigen Agenten, der eine reibungslose Bereitstellung der Plattform ermöglicht. Der Agent ermöglicht es Kunden, die Technologie schnell für jeden Workload mit mehreren Endpunkten einzusetzen und Daten in die Cloud zu übertragen, ohne die lokalen Erkennungs- und Präventionsfunktionen zu beeinträchtigen.

Für weitere Informationen laden Sie bitte das Whitepaper "2019 CrowdStrike Global Security Attitude Survey" herunter (http://ots.de/iYBp8B). Hier (http://ots.de/E3hePA) finden Sie auch einen Blogbeitrag von Thomas Etheridge von CrowdStrike.

Kontakt:

Pressekontakt:

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