14.01.2020 – 15:00 Uhr

Störung der Betriebsabläufe von Unternehmen als Hauptziel für Hacker - Services-Report von CrowdStrike

USA (ots) -

CrowdStrike, ein führender Anbieter von Cloud-basiertem Endgeräteschutz, veröffentlicht heute den CrowdStrike Services Cyber Front Lines-Report. Der Bericht gibt aufschlussreiche Einblicke in zahlreiche Incident-Response-Fälle aus dem vergangenen Jahr und teilt Erkenntnisse, die für 2020 und kommende Jahre von Bedeutung sind. Er identifiziert zudem neue Angriffsmethoden und Herausforderungen und bietet Empfehlungen für Unternehmen, die ihre Reaktionsfähigkeit bei Sicherheitsverletzungen verbessern möchten.

Mit Verweis auf das MITRE ATT&CK-Framework analysiert der Report zahlreiche Incident-Response-Fälle aus verschiedenen Ländern und Branchen. Er zeigt auf, dass im Laufe des Jahres 2019 36 Prozent der vom CrowdStrike Services Team untersuchten Vorfälle durch Ransomware, destruktive Malware oder Denial-of-Service-Angriffe verursacht worden sind. Das legt nahe, dass Unterbrechungen des Betriebsablaufes häufig das Hauptangriffsziel von Cyberkriminellen waren. Ein weiteres Ergebnis des Berichts zeigt eine starke Zunahme der Verweildauer von Angreifern in den Unternehmensnetzwerken. Sie ist auf durchschnittlich 95 Tage angestiegen - verglichen mit 85 Tagen im Jahr 2018. Dies bedeutet, dass Angreifer ihre Aktivitäten länger verstecken konnten und es den Unternehmen immer noch an der nötigen Technologie mangelt, die für die Erkennung und Abwehr von Angreifern notwendig ist.

Weitere zentrale Ergebnisse aus dem CrowdStrike Services Cyber Front Lines-Report:

- Manipulation von Dritten dienen als Multiplikator für Angriffe. Cyber-Akteure richten ihre Aktivitäten zunehmend auf Drittanbieter, um letzten Endes deren Kunden zu kompromittieren und ihre Angriffe somit zu skalieren.
- Angreifer zielen auf Infrastructure-as-a-Service (IaaS) ab. Kritische Aktivitäten rund um API-Schlüssel für Public-Cloud-Infrastrukturen werden immer gezielter, da die Angreifer immer mehr in der Lage sind, schnell und systematisch Informationsressourcen zu erlangen.
- Macs sind nun eindeutiges Ziel von Cyber-Akteuren. MacOS-Umgebungen werden verstärkt angegriffen, da Windows-Systeme meist von mehr Sicherheits-Tools überwacht werden.
- Patchen bleibt ein Problem. Grundlegende IT-Hygiene ist nach wie vor wichtig. Und obwohl Unternehmen beim Patching besser geworden sind, ist es nach wie vor eine komplexe Herausforderung.
- Die Art und Weise, wie Prävention konfiguriert wird, beeinflusst ihre Wirksamkeit. Viele Organisationen schöpfen die Möglichkeiten der bereits vorhandenen Tools nicht aus. Das Vorhandensein von Tools gibt ein falsches Gefühl von Sicherheit, wenn entscheidende Einstellungen nicht aktiviert werden.

"Der Services Cyber Front Lines-Report bietet Unternehmen wertvolle Anregungen, um die Sicherheitsmaßnahmen zur Schaffung einer cyberresistenten Umgebung proaktiv zu verbessern. Da Angreifer lange im Verborgenen arbeiten können und immer wieder neue Angriffsvektoren aufkommen, müssen Unternehmen agil und aktiv bleiben. Angreifer suchen den Weg des geringsten Widerstands - wenn ein Bereich besser geschützt wird, konzentrieren sie sich bereits auf das Eindringen in einen anderen", sagt Shawn Henry, Chief Security Officer und Präsident der CrowdStrike Services. "Unser Bericht macht klar, warum Lösegeldforderungen und Unterbrechungen des Geschäftsablaufes letztes Jahr die Schlagzeilen beherrscht haben. Für eine starke Cybersicherheit ist letztlich die Technologie entscheidend, die eine frühzeitige Erkennung, schnelle Reaktion und effektive Schadensbegrenzung bei Cyber-Angriffen gewährleistet."

Hier können Sie sich den CrowdStrike Services Cyber Front Lines-Report herunterladen: http://ots.de/PoJ7c4

Über CrowdStrike

CrowdStrike - ein führender Anbieter von Cybersecurity-Lösungen - definiert mit seiner State of the Art Endpoint Protection Platform Cybersicherheit im Cloud-Zeitalter neu. Die CrowdStrike Falcon Plattform bietet eine cloud-basierte, leichtgewichtige Single-Agenten-Architektur, die von künstlicher Intelligenz (KI) unterstützt wird. Mithilfe von Echtzeit-Schutz und hoher Transparenz über alle Unternehmensbereiche hinweg verhindert die Plattform Angriffe auf Endgeräte inner- oder außerhalb des Netzwerks. Die Falcon-Plattform korreliert mithilfe des CrowdStrike Threat Graph weltweit und in Echtzeit über zwei Billionen Events pro Woche. Damit gehört CrowdStrike Falcon zu einer der fortschrittlichsten Plattformen für Cybersicherheit. CrowdStrike

ermöglicht es Kunden, darunter führende Finanzinstitutionen, Energieunternehmen und Gesundheitsversorger, sich umfassender zu schützen, ihre Performance zu steigern und eine sofortige Wertschöpfung zu erreichen. CrowdStrike wurde 2011 gegründet, hat seinen Hauptsitz in Sunnyvale, Kalifornien, und ist seit 2019 am NASDAQ (CRWD) gelistet.

Kontakt:

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