

01.10.2019 – 15:05 Uhr

CrowdStrike OverWatch Report 2019 zeigt aktuelle Trends in der Cyberkriminalität



USA (ots) -

Das OverWatch Team von CrowdStrike, einem führenden Anbieter von cloud-basiertem Endgeräteschutz, hat heute seinen Falcon OverWatch Halbjahresbericht für 2019 herausgegeben. Er fasst die Erkenntnisse des OverWatch Threat Hunting Teams im ersten Halbjahr 2019 zusammen und zeigt aktuelle Trends bei Cyberattacken. Des Weiteren liefert er anhand von Beispielen Einblicke in die gängigen Werkzeuge, Techniken und Verfahren staatlich organisierter sowie kriminell motivierter Hackergruppen und gibt Empfehlungen für einen wirksamen Schutz.

Datenbasis: Pro Woche zwei Billionen Vorfälle auf Endgeräten

Das OverWatch Team besteht aus interdisziplinären Spezialisten und überwacht mehr als 120 staatsnahe und kriminelle Hackergruppen, die es auf die Netzwerke von CrowdStrikes Kunden abgesehen haben. Auf den Endgeräten der Nutzer werden dabei mit Hilfe der cloud-basierten und KI-gestützten Falcon-Plattform mehr als zwei Billionen sicherheitsrelevanter Vorfälle pro Woche erfasst, untersucht und gestoppt. Anhand dieser riesigen Datenmengen lassen sich mit intelligenten Algorithmen Bedrohungsmuster und Angriffstrends erkennen und wirksam verteidigen. Im OverWatch Report 2019 werden die wichtigsten Trends und Erkenntnisse aus diesen massiven Datensets vorgestellt und wirksame Abwehrmaßnahmen aufgezeigt.

Hier einige der wichtigsten Beobachtungen des OverWatch-Berichts:

- Massive Steigerung gezielter, finanziell motivierter Angriffe (E-Crime): Im ersten Halbjahr 2019 machten diese Aktivitäten - anders als bisher - die Mehrheit der beobachteten Attacken aus. Dies bedeutet nicht, dass nationalstaatlich motivierte Angriffe gesunken sind, sondern vielmehr, dass kriminell motivierte Hacker(gruppen) sich gezielt lohnende Ziele suchen, statt weit gestreute aber leicht verpuffende Angriffe zu fahren.
- Der Einzelhandel rückt verstärkt ins Visier von Cyberkriminalität: E-Crime-Kampagnen, ganz besonders mit erpresserischer Ransomware, sind überall auf dem Vormarsch. Bewegte sich der Einzelhandel in den vergangenen Jahren noch unter dem Radar cyberkrimineller Akteure, hat er sich in 2019 zu einem lukrativen Angriffsobjekt entwickelt. Insgesamt am häufigsten wurden sowohl in 2018 als auch in 2019 Unternehmen der Branchen Technologie, Telekommunikation und Finanzdienstleistung angegriffen.
- China bleibt einer der aktivsten Angreifer: Ähnlich wie in den letzten Jahren waren staatlich organisierte Angreifer aus China die aktivsten. Es war zu beobachten, dass dabei fast alle Branchen ins Visier genommen wurden - darunter Chemie, Gaming, Gesundheit, Industrie, Technologie und Telekommunikation.

"Sowohl kriminell als auch nationalstaatlich motivierte Angreifer sind in Netzwerken ihrer Angriffsziele durch heimliche Attacken oft gut positioniert. Im ersten Halbjahr 2019 hat OverWatch immer wieder beobachtet, wie Angreifer gültige Benutzerkonten dazu genutzt haben, um in kompromittierte Endgeräte einzudringen", so Jennifer Ayers, Vice President of OverWatch and Security

Response bei CrowdStrike. "Angreifer werden auch künftig dreist agieren und zu ausgeklügelten Mitteln greifen. Angesichts sich ständig verändernder IT-Architekturen und der Nutzung mobiler Endgeräte, die oft nicht durch ein Unternehmens-VPN geschützt werden können, ist es für Unternehmen essentiell, modernste Möglichkeiten zur Gefahrenabwehr zu nutzen."

Endgeräte als Einfallstore für Cyberkriminalität

Die gesammelten Daten zeigen, dass ungeschützte mobile Endgeräte oft die Einfallstore für Angreifer sind und herkömmliche Schutzmechanismen nicht mehr ausreichen. Es gilt, sich gegen raffinierte Bedrohungen zu schützen, die über klassische Malware wie dateilose Angriffe, Zero Day Exploit-Attacks (ZETA) oder andere ausgeklügelte Techniken hinausgehen. EDR-Lösungen (Endpoint Detection & Response), die cloud-basiert mit intelligenten Algorithmen auf den Endgeräteschutz konzentriert sind, kombiniert mit interdisziplinären Threat Hunting Teams aus erfahrenen Spezialisten helfen dabei, auch raffinierteste Bedrohungen schnell zu entdecken, zu analysieren und unschädlich zu machen. CrowdStrike bietet seinen Kunden mit Falcon eine Plattform für Endgeräteschutz, die auch von Gartner als "Leader" ausgezeichnet wurde.

Bildmaterial sowie der Original-Report sind unter diesem Link zu finden:
www.dropbox.com/sh/2gxbq85wbsl92h9/AADDXd5rxj5rflavTgO_2y4ya?dl=0

Über CrowdStrike

CrowdStrike ist der führende Anbieter von Cloud-basiertem Schutz für Endgeräte. Die CrowdStrike Falcon Plattform verhindert mithilfe von künstlicher Intelligenz Angriffe auf Endgeräte im oder außerhalb des Netzwerks und bietet sofortigen Schutz und Transparenz im gesamten Unternehmen. Sie ist in wenigen Minuten einsatzbereit. Durch ihre Cloud-Infrastruktur und die Single-Agent-Architektur reduziert die Plattform Komplexität, erleichtert die Verwaltung und erhöht die Skalierbarkeit. CrowdStrike betreut Kunden aus fast allen Industrien und Branchen, darunter führende Finanzinstitutionen, Energieunternehmen und Gesundheitsversorger. Insgesamt werden Lösungen des Unternehmens in 176 Ländern eingesetzt. CrowdStrike wurde 2011 gegründet, hat seinen Hauptsitz in Sunnyvale, Kalifornien, und ist am NASDAQ gelistet. Weitere Informationen finden Sie unter www.crowdstrike.de

Kontakt:

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

Medieninhalte



CrowdStrike Overwatch Report 2019. as OverWatch Team von CrowdStrike, einem führenden Anbieter von cloud-basiertem Endgeräteschutz, hat heute seinen Falcon Overwatch Halbjahresbericht für 2019 herausgegeben. Weiterer Text über ots und www.presseportal.de/nr/132391 / Die Verwendung dieses Bildes ist für redaktionelle Zwecke honorarfrei. Veröffentlichung bitte unter Quellenangabe: "obs/CrowdStrike"

Diese Meldung kann unter <https://www.presseportal.ch/de/pm/100066723/100833255> abgerufen werden.