CrowdStrike Global Threat Report 2020:

Gezielte Angriffe auf die Telekommunikations-Branche und „Big Game Hunting“ standen 2019 im Fokus der Cyber-Angreifer

Der aktuelle Report enthüllt Daten und Trends über gezieltes Eindringen sowie Angriffstechniken von nationalstaatlichen Angreifern und Cyberkriminellen

Sunnyvale, Kalifornien – 3. März 2020 – CrowdStrike® Inc. (Nasdaq: CRWD), ein führender Anbieter von Cloud-basiertem Endgeräteschutz, veröffentlicht heute den CrowdStrike Global Threat Report 2020. Der Report gibt einen umfassenden Einblick in die aktuelle Bedrohungslandschaft und zeigt auf, welche Cyber-Angriffe das Jahr 2019 geprägt haben. Neben finanziell motivierter Cyberkriminalität, die nahezu kontinuierlich im vergangenen Jahr stattgefunden hat, beobachtete CrowdStrike eine Zunahme von Ransomware-Attacken, verschiedene Weiterentwicklungen bei den angewandten Taktiken sowie steigende Lösegeldforderungen von eCrime-Akteuren. Diese Angreifergruppen haben darüber hinaus verstärkt damit begonnen, Daten zu exfiltrieren, um mit der Veröffentlichung von peinlichen oder proprietären Informationen zu drohen.

Das Jahr 2019 war nicht nur von eCrime-Kriminalität geprägt, sondern auch von nationalstaatlichen Angriffen, die auf eine Vielzahl von Branchen abzielten. Ein weiterer zentraler Trend im diesjährigen Bericht betrifft die Telekommunikationsindustrie, die zunehmend ins Visier von Angreifern wie beispielsweise China oder der DVRK gerät. CrowdStrike vermutet, dass verschiedene Nationen und ganz besonders China ein Interesse an diesem Sektor haben, um geistiges Eigentum und Wettbewerbsanalysen zu stehlen.

Die Bekämpfung von Bedrohungen durch fortschrittliche nationalstaatliche und eCrime-Angreifer erfordert einen ausgereiften Prozess, der solche Angriffe verhindern, erkennen sowie schnell und flexibel auf sie reagieren kann. CrowdStrike empfiehlt Unternehmen, die „1-10-60-Regel" zu befolgen, um Cyberattacken wirksam zu vereiteln. Die 1-10-60-Richtlinien lauten wie folgt: Erkennen eines Eindringens in weniger als einer Minute; Analysieren innerhalb von 10 Minuten; Eindämmen und Beseitigen des Angreifers innerhalb von 60 Minuten. Organisationen, die diese Vorgaben erfüllen, sind nicht nur eher in der Lage, einen

potentiellen Angreifer rechtzeitig unschädlich zu machen, bevor dieser sich vom Angriffspunkt aus tiefer ins System vorarbeiten kann, sondern können auch die Auswirkungen eines Angriffs auf die Organisation minimieren.

„2019 gab es zahlreiche neue Techniken von nationalstaatlichen Akteuren und einen zunehmend komplexeren eCrime-Untergrund voller dreister Taktiken und einer massiven Zunahme gezielter Lösegeldforderungen. Daher müssen moderne Sicherheitsteams zur Aufdeckung, Untersuchung und Behebung von Sicherheitsvorfällen auf Technologien mit schnellen, präventiven Gegenmaßnahmen wie Threat Intelligence setzen und die 1-10-60-Regel befolgen“, so Adam Meyers, Vice President of Intelligence bei CrowdStrike.

Weitere interessante Erkenntnisse aus dem Global Threat Report 2020:

- **Die Bedrohungslandschaft wandelt sich – malwarefreie Angriffe nehmen zu und übersteigen das Volumen von Malewareangriffen:** 2019 verwendeten 51 Prozent der Angriffe malwarefreie Techniken, im Vorjahr waren es noch 40 Prozent. Dies unterstreicht die Dringlichkeit, dass über traditionelle Antiviren-Lösungen (AV) hinaus gedacht werden muss.

- **China konzentriert sich** weiterhin bei vielen Operationen **auf Lieferketten-Angriffe** und zeigt damit, dass der Staat weiterhin auf diese Taktik setzt, um auf diese Weise mehrere Opfer gleichzeitig zu identifizieren und zu infizieren. Zudem ist es sehr wahrscheinlich, dass **gezielte Angriffe auf die Schlüsselindustrien der USA** weitergehen werden, die bedeutsam für Chinas strategische Interessen sind. Dazu zählen Clean Energy, Gesundheitswesen, Biotechnologie, Pharma und die Luftfahrt.

- **Die am häufigsten von Enterprise-Ransomware („Big Game Hunting“) betroffenen Branchen** waren lokale Regierungen und Gemeinden, akademische Einrichtungen, die Technologiebranche, Gesundheitswesen, Produktion, Finanzdienstleistungen und Medienunternehmen.

- Zusätzlich zur Unterstützung der Währungsgenerierung könnte der **Fokus der DVRK auf Kryptobörsen auf Spionagebemühungen hindeuten**, um Informationen über Nutzer oder Kryptowährungen zu sammeln. Zudem vermutet CrowdStrike Intelligence,

dass **die DVRK ihre eigene Kryptowährung entwickelt, um weiter internationale Sanktionen zu umgehen.**

„Der diesjährige Report zeigt auf, dass ein massiver Anstieg von eCrime leicht zu einer Störung von Geschäftstätigkeiten führen kann, da Kriminelle auf Taktiken setzen, die darauf abzielen, betroffene Organisationen für längere Zeit geschäftsuntüchtig zu machen. Es ist unumgänglich, dass moderne Organisationen eine ausgeklügelte Sicherheitsstrategie verfolgen, die zuverlässige Erkennung und Reaktion ebenso umfasst wie kontrolliertes Threat Hunting rund um die Uhr, um Vorfälle zu lokalisieren und Risiken zu mindern“, so Jennifer Ayers, Vice President of OverWatch bei CrowdStrike. „Die umfassende Technologie von CrowdStrike, gepaart mit unseren Einblicken in die Beweggründe von Angreifern und proaktivem Hunting setzt alle kritischen Komponenten ein, die nötig sind, um unsere Kunden vor fortschrittlichen Bedrohungen zu schützen.“

Der Global Threat Report analysiert umfassende Bedrohungsdaten von CrowdStrike Falcon® Intelligence, CrowdStrike Falcon OverWatch™, dem branchenführenden Team für die verwaltete Bedrohungssuche, von CrowdStrike Threat Graph, einer massiv skalierbaren, Cloud-basierten Graph-Datenbanktechnologie, die pro Woche fast 2,5 Billionen Ereignisse in 176 Ländern verarbeitet, und CrowdStrike Services. Der Report bietet tiefe Einblicke in moderne Angreifer und ihre Taktiken, Techniken und Verfahren (TTPs).

Im Blogpost von George Kurtz, Mitgründer und Geschäftsführer von CrowdStrike, erfahren Sie mehr über die Ergebnisse des Reports.

Laden Sie den *CrowdStrike Global Threat Report 2020* herunter.

lÜber CrowdStrikel

CrowdStrike® Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Endgeräteschutzplattform die Sicherheit im Cloud-Zeitalter neu. Die Plattform CrowdStrike Falcon® verfügt über eine einzigartige, Cloud-basierte, schlanke Agentenarchitektur, die von künstlicher Intelligenz (KI) unterstützt wird und unternehmensweit für Schutz und Transparenz in Echtzeit sorgt. So werden Angriffe auf Endgeräte sowohl innerhalb als auch außerhalb des Netzwerks verhindert. Mit Hilfe des firmeneigenen CrowdStrike Threat Graph® korreliert CrowdStrike Falcon weltweit und in Echtzeit über 2,5 Billionen endpunktbezogene Ereignisse pro Woche. Damit ist die CrowdStrike Falcon Plattform eine der weltweit fortschrittlichsten Datenplattformen für Cyber-Sicherheit. CrowdStrike ermöglicht es Anwendern, 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.

Mehr Informationen finden Sie unter: https://www.crowdstrike.de/

Folgen Sie uns: Blog | Twitter

Für weitere Informationen kontaktieren Sie bitte:

HARVARD ENGAGE! COMMUNICATIONS GMBH
Oliver Salzberger / Ava Dühring
Tel: +49 89 53 29 57 23
E-Mail: Crowdstrike@harvard.de