Neue Studie von Check Point: Weltweit 32 Prozent mehr Cyber-Angriffe pro Woche

Die Angriffe auf staatliche und militärische Organisationen stiegen zudem um 143 Prozent. Im Durchschnitt ist eins von vierzig Unternehmen von Ransomware betroffen.

San Carlos, Kalifornien – 2. August 2022 – Das Jahr 2022 begann mit einer massiven Ausnutzung einer der schwerwiegendsten Schwachstellen in der Geschichte des Internet: Apache Log4J. Danach setzte es sich mit einem virtuellen Kampf im Rahmen des Russland-Ukraine-Krieges fort. Nun berichtet Check Point Research (CPR), die Spezialisten-Abteilung von Check Point Software Technologies, dass im zweiten Quartal 2022 ein neuer Höchststand an Cyber-Attacken erreicht wurde. Die weltweiten Angriffe sind demnach um 32 Prozent gestiegen (die Vergleiche beziehen sich stets auf das zweite Quartal im Jahr 2021). Die durchschnittlichen wöchentlichen Angriffe pro Unternehmen weltweit erreichten einen Spitzenwert von 1'200. Die am häufigsten angegriffene Branche im zweiten Quartal 2022 war der Bildungs- und Forschungssektor. Ausserdem war eine von 40 Organisationen weltweit von Ransomware betroffen, was einem Anstieg von 59 Prozent entspricht.

Bildung und Forschung ist der am häufigsten angegriffene Sektor

Nach Branchen betrachtet, scheinen Cyber-Kriminelle die meisten Angriffe auf den Bildungs- und Forschungssektor zu richten, mit durchschnittlich mehr als 2'300 Angriffen pro Organisation pro Woche. Dies entspricht einem Anstieg von 53 Prozent. Darauf folgt der Regierungs- und Militärsektor mit durchschnittlich 1'600 Angriffen pro Woche, was einem Anstieg von 44 Prozent entspricht. Danach kommen die IT- und Internet-Dienstleister mit durchschnittlich 1'340 Angriffen und einem Zuwachs von 29 Prozent.

Industrie/Sektor	**Wöchentlich betroffene Organisationen**	**Veränderung zum Vorjahr**
Am meisten betroffen		
Bildung/Forschung	1'620	+ 52 %
Regierungen/Militär	1'342	+ 44 %
IT-/Internet-Dienstleister	1'340	+ 29 %
Am geringsten betroffen		
Software-Hersteller	721	+ 15 %
Unternehmensberatungen	693	+ 12 %
Hardware-Hersteller	426	+ 54 %

Abbildung 1: Globale durchschnittliche wöchentliche Angriffe pro Branche im Vergleich zu Q2 2021

Ransomware steht weiterhin im Zentrum der Aufmerksamkeit
Im Mai 2022 jährte sich der berüchtigte WannaCry-Angriff zum fünften Mal und es scheint, dass Ransomware die Bedrohungslandschaft völlig verändert hat. Die Malware, die Daten verschlüsselt, hat sich zu einer Waffe in den Händen von Angriffsgruppen entwickelt, die sogar Regierungen bedrohen. In diesem Bericht stellt CPR fest, dass weltweit im wöchentlichen Durchschnitt 1 von 40 Organisationen von Ransomware betroffen ist – ein Anstieg von 59 Prozent. In Europa liegt der wöchentliche Durchschnitt der betroffenen Unternehmen – ähnlich wie im Vorjahr – bei 1 von 66.

Ransomware-Angriffe nach Branchen: Einzel- und Grosshandel im Visier
Der Einzel- und Grosshandel verzeichnete den grössten Anstieg der Ransomware-Angriffe mit einem alarmierenden Zuwachs von 182 Prozent. Darauf folgt das Vertriebswesen mit einem Anstieg von 143 Prozent und das Regierungs-/Militärwesen mit einem drastischen Anstieg von 135 Prozent, weswegen 1 von 24 Organisationen wöchentlich von Ransomware betroffen ist.

Industrie/Sektor	Wöchentlich betroffene Organisationen	Veränderung zum Vorjahr
Am meisten betroffen		
Einzelhandel/Grosshandel	1 von 53	+182 %
Vertriebshändler	1 von 47	+143 %
Regierungen/Militär	1 von 24	+135 %
Am geringsten betroffen		
Versicherung/Recht	1 von 81	+1 %
Unternehmensberatungen	1 von 87	-17 %
Software-Hersteller	1 von 74	-34 %

Abbildung 2: Verhältnis der Ransomware-Angriffe pro Branche

Angriffe nach Region
Die Forscher stellten fest, dass Afrika im zweiten Quartal 2022 die am stärksten angegriffene Region war, mit durchschnittlich 1760 wöchentlichen Angriffen pro Unternehmen. Das entspricht einem Anstieg von 3 Prozent. Nach Afrika verzeichneten Asien und Lateinamerika erstaunliche Zahlen von durchschnittlich 1’680 bzw. 1’600 Angriffen, was einen Anstieg von 25 Prozent bzw. 29 Prozent bedeutet.

Region	Wöchentliche Angriffe pro Organisation	Veränderung zum Vorjahr
Afrika	1’758	+ 3 %
Asien	1’684	+ 25 %
Lateinamerika	1’602	+ 29 %
Europa	963	+ 26 %
Asien und Ozeanien	937	+ 82 %
Nordamerika	854	+ 54 %

Wie man den nächsten Angriff verhindert
Mega-Cyber-Attacken wie SolarWinds und Log4J waren nicht unvermeidlich. Mit den richtigen Massnahmen können verheerende Folgen solcher Angriffe vermieden werden. Um die nächsten Bedrohungen wirklich bekämpfen zu können, müssen Unternehmen ihre Sichtweise auf IT-Sicherheit ändern und einige Leitprinzipien befolgen.

1. **Prävention vor Erkennung:**

Es stimmt nicht, dass Angriffe nicht verhindert werden können. Angriffe können nicht nur blockiert, sondern auch verhindert werden, einschliesslich Zero-Day-Angriffen und unbekannter Malware. Mit den richtigen Technologien können die meisten Angriffe abgewehrt werden, ohne den normalen Geschäftsablauf zu stören.

2. **Bedrohungsdaten auf dem neuesten Stand halten**

Wenn ein Unternehmen über finanzielle, persönliche, intellektuelle oder nationale Werte verfügt, ist ein umfassenderer Ansatz für die IT-Sicherheit die einzige Möglichkeit, sich vor den derzeitigen Angreifern zu schützen. Eine der effektivsten Sicherheitslösungen ist die Bedrohungsanalyse.

3. **Implementierung der fortschrittlichsten Technologien**

Es gibt viele wirkungsvolle Technologien und Ideen, wie maschinelles Lernen, Sandboxing, Erkennung von Anomalien, Entwaffnung von Inhalten und zahlreiche andere, welche dazu beitragen, den nächsten Cyber-Angriff zu verhindern. Jede dieser Technologien kann in bestimmten Szenarien sehr effektiv sein. Starke Lösungen integrieren eine breite Palette von Technologien, um Angriffe in IT-Umgebungen zu bekämpfen.

4. **Aufrechterhaltung der Sicherheit**

- **Patching:** Unternehmen sollten sich darum bemühen, dass für alle Systeme und Software aktuelle Patches zur Verfügung stehen.
- **Segmentierung:** Netzwerke sollten segmentiert werden. Starke Firewall- und IPS-Schutzmassnahmen zwischen den Segmenten können verhindern, dass sich Infektionen über das Netzwerk ausbreiten.
- **Prüfung**: Die Richtlinien der Sicherheitsprodukte müssen sorgfältig geprüft sowie die Protokolle und Warnmeldungen zu Vorfällen kontinuierlich überwacht werden.
- **Tests**: Routinemässige Audits und Penetrationstests sollten für alle Systeme durchgeführt werden.
- **Least-Privilege-Prinzip**: Benutzer- und Software-Privilegien sollten auf ein Minimum beschränkt werden – Benutzer sollten nur die Zugriffsrechte haben, die sie wirklich brauchen

Somit zeigt die Studie von CPR: Jedes Unternehmen oder Land kann sofort Massnahmen zum Schutz vor IT-Attacken ergreifen. Von kontinuierlichen Datensicherungen gegen Ransomware über die Verringerung der Angriffsfläche bis hin zu einfachen Taten wie der ständigen Aktualisierung von Patches – die Umsetzung eines Aktionsplans für IT-Sicherheit wird beitragen, alle Arten von Angriffen letzten Endes zu verringern.

Alle Einzelheiten erfahren Sie hier: https://blog.checkpoint.com/2022/07/26/check-point-research-weekly-cyber-attacks-increased-by-32-year-over-year-1-out-of-40-organizations-impacted-by-ransomware-2/

Alle Berichte von Check Point finden Sie unter: https://blog.checkpoint.com/
Alle Berichte des Check Point Research Teams finden Sie unter: https://research.checkpoint.com/

Folgen Sie Check Point auf:
Twitter: https://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blog: https://blog.checkpoint.com
YouTube: https://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

Über Check Point Research
Check Point Research (CPR) bietet führende Cyber-Bedrohungsinformationen für Check Point Software-Kunden und die grössere Intelligenz-Community. Das Forschungsteam sammelt und analysiert globale Cyber-Angriffsdaten, die auf der ThreatCloud gespeichert sind, um Hacker fernzuhalten und gleichzeitig sicherzustellen, dass alle Check Point Produkte mit den neuesten Schutzmassnahmen aktualisiert werden. Das Forschungsteam besteht aus über 100 Analysten und Forschern, die mit anderen Sicherheitsanbietern, der Strafverfolgung und verschiedenen CERTs zusammenarbeiten.

Über Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. (www.checkpoint.com) ist ein führender Anbieter von Cyber-Sicherheitslösungen für Unternehmen und Regierungen weltweit. Die Lösungen des Check-Point-Infinity-Portfolios schützen Kunden gegen Cyber-Angriffe der 5. Generation mit einer in der Branche führenden Fangrate von Malware, Ransomware und anderen Bedrohungen. Infinity ruht auf drei Kernsäulen, die kompromisslose Sicherheit und Bedrohungsabwehr der Generation V in Konzern-Umgebungen bieten: Check Point Harmony für Remote-Benutzer; Check Point CloudGuard für die automatische Absicherung von Clouds; Check Point Quantum für den Schutz von Netzwerkperimetern und Rechenzentren – alles gesteuert durch das branchenweit umfassendste und intuitivste Unified Security Management. Check Point schützt über 100’000 Unternehmen jeder Grösse in der ganzen Welt.

Pressekontakte:
Check Point Software Technologies
Alvaro Amato
Country Manager Schweiz

Jenni Kommunikation AG
Luca Perler
Tel: +41 44 388 60 80
E-Mail: luca.perler@jeko.com

