Media Alert von Check Point Software:

Cyberangriffe auf Schweizer Organisationen stiegen 2022 um 61 Prozent

San Carlos, Kalifornien – 9. Januar 2023 – Den Daten der Sicherheitsforscher von Check Point Research (CPR) zufolge, sind im vergangenen Jahr die Cyberangriffe auf Schweizer Organisationen im Vergleich zu 2021 um 61 Prozent gestiegen. Auf die Fertigungsindustrie (752), das Finanzwesen (623) sowie Regierung und Militär (569) entfielen dabei wöchentlich im Schnitt am meisten Attacken, wie der Branchenvergleich zeigt.

Country	Industry	Rank	Avg. Weekly Attacks Per Organization in 2022	Change from 2021
Switzerland	Manufacturing	1	752	-24 %
Switzerland	Finance/Banking	2	623	+120 %
Switzerland	Government/Military	3	569	+52 %
Switzerland	Healthcare	4	455	+78 %
Switzerland	Communications	5	397	+200 %

Die wichtigsten Statistiken zu den weltweiten Cyberangriffstrends 2022:

- Das weltweite Volumen von Cyberangriffen erreichte im 4. Quartal mit durchschnittlich 1’168 wöchentlichen Angriffen pro Unternehmen ein Allzeithoch.
- Die Top 3 der am häufigsten angegriffenen Branchen im Jahr 2022 waren Bildung/Forschung, Regierung und Gesundheitswesen.
- Nordamerika (+52%), Lateinamerika (+29%) und Europa (+26%) verzeichneten 2022 den grössten Anstieg an Cyberangriffen im Vergleich zu 2021.

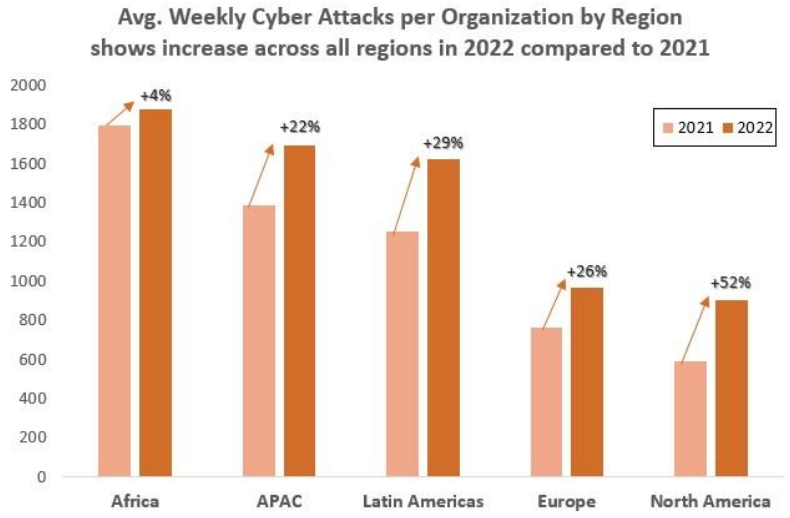

Abbildung 1: Steigerung der wöchentlich erfassten Cyberangriffe per Region in 2022 verglichen mit 2021 (Quelle Check Point Software Technologies Ltd. 2023)

Omer Dembinsky, Data Group Manager bei Check Point Software erklärt: «Cyberangriffe nehmen weltweit zu. 2022 hat es global 38 Prozent mehr Cyberangriffe pro Woche auf Unternehmensnetze gegeben als in 2021. Mehrere Trends bei Cyber-Bedrohungen treten gleichzeitig auf und sind für diese Entwicklung verantwortlich. Zum einen entwickelt sich das Ransomware-Ökosystem weiter und wächst mit kleineren, agileren kriminellen Gruppen. Zweitens weiten sie ihre Ziele aus und nehmen mit Phishing-Exploits Kollaborationstools wie Slack, Teams, OneDrive und Google Drive ins Visier. Dabei handelt es sich um eine ergiebige Quelle für sensible Daten, da die meisten Mitarbeiter von Unternehmen nach wie vor aus der Ferne arbeiten. Drittens sind akademische Einrichtungen nach der raschen Digitalisierung, die sie als Reaktion auf die COVID-19-Pandemie vorgenommen haben, zu einem beliebten Tummelplatz für Cyberkriminelle geworden. Tatsächlich war der Bildungs-/Forschungssektor die am häufigsten angegriffene Branche weltweit und verzeichnete 2022 einen Anstieg von 43 Prozent im Vergleich zu 2021, mit durchschnittlich 2'314 Angriffen pro Organisation pro Woche. Viele Bildungseinrichtungen waren auf die unerwartete Verlagerung zum Online-Lernen schlecht vorbereitet, was Hackern reichlich Gelegenheit bot, mit allen Mitteln in Netzwerke einzudringen. Schulen und Universitäten stehen ausserdem vor der besonderen Herausforderung, mit Kindern und jungen Erwachsenen umzugehen, von denen viele ihre eigenen Geräte benutzen, an gemeinsamen Orten arbeiten und sich oft mit öffentlichen WLANs verbinden, ohne an die Sicherheitsimplikationen zu denken.»

Um sich zu schützen, ist es unerlässlich, zuerst an die Prävention und nicht an die Erkennung zu denken. Es gibt mehrere bewährte Praktiken und Massnahmen, die ein Unternehmen ergreifen kann, um seine Anfälligkeit für den nächsten Angriff oder die nächste Sicherheitsverletzung zu minimieren, die folgenden vier Cybersecurity-Tipps unterstützen IT-Sicherheitsteams bei ihrer Arbeit.

Vier Cybersecurity-Tipps:

1. **Cybersecurity-Awareness-Training**: Häufige Schulungen zum Thema Cybersicherheit sind entscheidend für den Schutz des Unternehmens vor Ransomware. Diese Schulungen sollten die Mitarbeiter zu folgenden Massnahmen anleiten:
    a. Nicht auf bösartige Links klicken
    b. Niemals unerwartete oder nicht vertrauenswürdige Anhänge öffnen
    c. Keine persönlichen oder sensiblen Daten an Phisher weitergeben
    d. Die Legitimität von Software überprüfen, bevor sie heruntergeladen wird
    e. Niemals ein unbekanntes USB-Gerät an den Computer anschliessen
    f. Ein VPN verwenden, wenn man sich über ein nicht vertrauenswürdiges oder öffentliches Wi-Fi verbindet
2. **Up-to-Date Patches:** Computer und Server auf dem neuesten Stand zu halten und Sicherheits-Patches anzuwenden, insbesondere solche, die als kritisch eingestuft sind, kann dazu beitragen, die Anfälligkeit eines Unternehmens für Ransomware-Angriffe zu verringern.
3. **Die Software aktualisiert halten:** Ransomware-Angreifer finden manchmal einen Einstiegspunkt in Anwendungen und Software, bemerken Schwachstellen und nutzen sie aus. Glücklicherweise suchen einige Entwickler aktiv nach neuen Schwachstellen und schliessen diese mit Patches aus. Wer diese Patches nutzen möchte, muss eine Strategie für die Patch-Verwaltung haben und sicherstellen, dass alle Mitglieder des Teams immer auf dem neuesten Stand sind.

4. **Vorbeugung statt nachträglicher Erkennung:** Viele behaupten, dass es immer Cyberangriffe geben wird und dass es keine Möglichkeit gibt, sie zu verhindern. Daher bleibt nur, in Technologien zu investieren, die den Angriff erkennen, wenn er bereits in das Netz eingedrungen ist und den Schaden so schnell wie möglich zu mindern. Das Gegenteil ist richtig. Angriffe können nicht nur blockiert, sondern auch verhindert werden – einschliesslich Zero-Day-Angriffen und unbekannter Malware. Mit den richtigen Technologien können die meisten Attacken, selbst die fortschrittlichsten, verhindert werden, ohne den normalen Geschäftsablauf zu unterbrechen.

Pressekontakte:
Check Point Software Technologies
Alvaro Amato
Country Manager Schweiz

Jenni Kommunikation AG
Sylvana Zimmermann
Tel: +41 44 388 60 80
E-Mail: sylvana.zimmermann@jeko.com

