Veröffentlicht auf Presseportal Schweiz - Presse und Medienmitteilungen (https://www.presseportal-schweiz.ch)

10.05. 2023

Cyberkriminalität: Geopolitische Spannungen beeinflussen Bedrohungslandschaft massiv

Von PPS

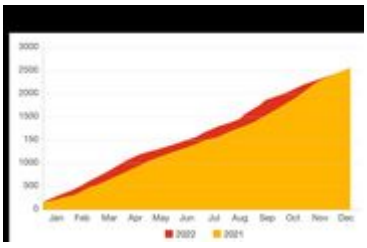

Bild Rechte
PricewaterhouseCoopers AG

- Die Spannungen nehmen weltweit zu – wirtschaftliche Sicherheit wird gleichbedeutend mit nationaler Sicherheit
- Fast die Hälfte aller finanziell motivierten Attacken waren Ransomware-Angriffe
- Log4Shell-Schwachstelle hat ca. 93% der Cloud-Umgebungen von Unternehmen getroffen
- Ransomware-Angriffe konzentrierten sich vorwiegend auf fünf Branchen

(Zürich)(PPS) Das Jahr 2022 war geprägt von diversen geopolitischen Spannungen und Bedrohungsakteuren. Aber auch die Suche nach Lösungen für die Log4Shell-Schwachstelle beschäftigte Unternehmen stark. Dies zeigt die aktuelle Studie «**Year in Retrospect**» von PwC. Im Kampf um politische, territoriale und wirtschaftliche Vormachtstellungen setzen einige Staaten gezielt auf offensive Taktiken und Technologien der Cyberkriminalität.

Geopolitischer Einfluss auf Bedrohungslandschaft

Im Jahr 2022 spiegelten sich in der Cyber-Bedrohungslandschaft reale Ereignisse und geopolitische Spannungen wider, wobei die russische Invasion der Ukraine ein Grossteil des Jahres prägte. Das Jahr war gekennzeichnet vom Zusammentreffen verschiedener Angriffsarten und -motiven in einem Strudel aus Sabotage, Spionage und Hacktivismus. Nach Kriegsausbruch in der Ukraine setzten russische Akteure vor allem auf Sabotageversuche, die meist auf dem Einsatz von Wiper-Malware basierten. Dies hatte zum Ziel, Daten nicht nur zu verschlüsseln, sondern permanent zu löschen. Der Einsatz konzentrierte sich weitgehend auf die unmittelbare Konfliktzone, also auf die Ukraine und die von Russland annektierten Gebiete. Sabotage- und Spionageangriffe waren aber auch in anderen Weltregionen wie dem Iran oder China in grosser Zahl feststellbar. Die potenziell zerstörerische Natur der Angriffe und Absichten der Bedrohungsakteure dienen als warnendes Beispiel für einen sich ausbreitenden Trend im Hacktivismus, der mit der Fortsetzung des Krieges oder anderen Konflikten zunehmen könnte.

Anzahl Ransomware-Angriffe stagniert auf hohem Niveau

Im Jahr 2022 wurden rund 2’500 Opfer auf Ransomware-Leak-Seiten gemeldet, was einem leicht tieferen Wert als im Jahr 2021 entspricht. Dennoch überragen die Werte der beiden Jahre die 1'330 ausgewerteten Fälle auf Leak-Seiten im Jahr 2020 deutlich. Während die Auswertungen von 2020 bis 2021 einen kontinuierlichen Anstieg der Opferzahlen von Ransomware-Angriffen ergab, deutet die Gesamtzahl der gefunden Fälle auf Leak-Seiten zwischen 2021 und 2022 auf eine Stagnation hin. Das Jahr 2022 stellte das Ransomware-Ökosystem aber auch vor erhebliche Herausforderungen: der Krieg in der Ukraine, Strafverfolgungsmassnahmen gegen Ransomware-Bedrohungsakteure, die Volatilität von Kryptowährungen aber auch Spaltungen prominenter Ransomware-Gruppen durch interne Leaks und Konflikte machten den Gruppen zu schaffen.

Die untersuchten Angriffe konzentrierten sich primär auf fünf Branchen: Industrielle Fertigung, Dienstleistungen, Finanzwesen, Transport und Logistik und Handel. Sie verzeichneten rund 50% der untersuchten Ransomware-Attacken, wobei die industrielle Fertigung und Dienstleistungsbetriebe die beliebtesten Ziele darstellten. Die Ransomware-Angriffe werden initial grösstenteils opportunistisch und

automatisiert ausgeführt. «Der Entscheid, Daten von Unternehmen aus bestimmten Branchen zu verschlüsseln und die Opfer zu erpressen, liegt oftmals in der Natur der Dienstleistungen. Hohe Kosten im Falle eines Betriebsausfalls, wie zum Beispiel einer stillgelegten Produktionslinie, sowie vergleichsweise geringe Sicherheitsanforderungen und -vorschriften machen Unternehmen aus gewissen Branchen verwundbar», erklärt Johannes Dohren, Partner und Leiter Threat Intelligence bei PwC Schweiz.

Cloud-Umgebungen vermehrt im Fokus

Angreifende nutzten wie schon im letzten Jahr Zero-Day-Schwachstellen für eine grosse Zahl von Attacken. Allen voran die Log4Shell-Schwachstelle – diese hat ca. 93 % der Cloud-Umgebungen von Unternehmen und damit Hunderte Millionen von Computern getroffen. Bei immer mehr Attacken rückten Privileged Access Management (PAM)-Systeme in den Mittelpunkt, die in vielen Fällen mit Hilfe von Social Engineering-Techniken und durch allgemeine Schwachstellen oder Fehlkonfigurationen (wie fehlende Multi-Faktor-Authentifizierung) verwundbar blieben. «Wir gehen davon aus, dass die Bedrohungslandschaft im Jahr 2023 u.a. durch Angriffe auf Identiy- und Privileged Access Technologien dominiert wird, da ein breites Spektrum von Bedrohungsakteuren sich weiterentwickelt und Techniken zur Umgehung von Sicherheitsmechanismen einsetzt», schätzt Johannes Dohren ein.

Kompletter Report: https://www.pwc.ch/en/insights/cybersecurity/threat-intelligence-report...

Über den Bericht

Der Bericht «Year in Retrospect» bewertet jährlich die aktuelle Lage im Hinblick auf Cyberkriminalität, regionale Aktivitäten sowie Bedrohungsakteure und -trends. Dieser Bericht analysiert die übergreifenden und thematischen Trends aus dem Jahr 2022 und untersucht, inwieweit verschiedene Branchen Cyberbedrohungen ausgesetzt sind.

Über die Organisation:

Über PwC

PwC Schweiz ist das führende Prüfungs- und Beratungsunternehmen in der Schweiz. Der Zweck von PwC ist es, das Vertrauen in der Gesellschaft aufzubauen und wichtige

Probleme zu lösen. Wir sind ein Netzwerk von Firmen, das in 152 Ländern rund 328'000 Mitarbeitende beschäftigt. Diese setzen sich dafür ein, in den Bereichen Wirtschaftsprüfung, Beratung , Recht und Steuern erstklassige Dienstleistungen zu erbringen. PwC Schweiz hat über 3’480 Mitarbeitende und Partner:innen an 14 verschiedenen Standorten in der Schweiz sowie einem im Fürstentum Liechtenstein. Erfahren Sie mehr und sagen Sie uns, was für Sie wichtig ist, unter pwc.ch. «PwC» bezieht auf das PwC-Netzwerk und/oder eine oder mehrere seiner Mitgliedsfirmen, von denen jede ein eigenständiges Rechtssubjekt ist. Nähere Angaben dazu finden Sie unter pwc.com/structure

Pressekontakt:

PricewaterhouseCoopers AG
Birchstrasse 160
Postfach
CH-8050 Zürich

Bianca Helbling
PwC | External Relations Consultant
Mobile: +41 58 792 41 02
Email: bianca.helbling @ pwc.ch

Kategorie
IT & Software & Neue Medien
