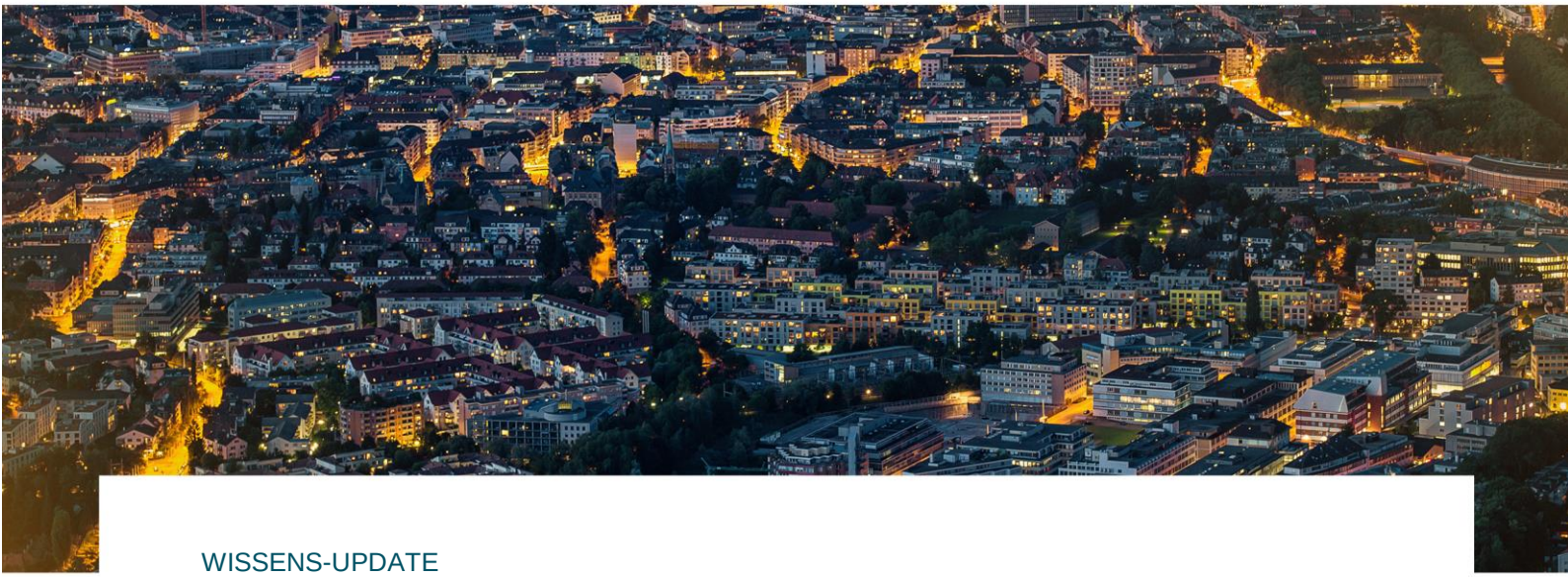
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WISSENS-UPDATE

Ausblick 2023: Die fünf wichtigsten Malware Trends

CyOne Security | Steinhausen, 03. Januar 2023

Die Bedrohung durch Malware wächst: Ransomware as a Service (RaaS) und IoT-Malware dürften 2023 bei Unternehmen und Behörden erneut verheerende Schäden anrichten. Gleichzeitig geraten Mailserver vermehrt ins Visier und die Vielfalt an Malware-Familien wächst unaufhaltsam. Mit Drone Hacking hält zudem ein möglicher neuer Trend Einzug.

1. Ransomware as a Service (RaaS) ist die grösste Bedrohung

Ransomware ist gemäss dem Nationalen Zentrum für Cybersicherheit (NCSC) momentan die grösste Bedrohung für Schweizer Organisationen. 2023 dürfte sich daran nichts ändern, da die Variantenvielfalt rasant wächst. In der ersten Jahreshälfte 2022 hat sich die Zahl der von Fortinet identifizierten neuen Ransomware-Varianten im Vergleich zum vorangehenden Halbjahr fast verdoppelt: Der US-Cybersecurity-Anbieter dokumentierte in diesem Zeitraum über 10’000 neue Varianten – im zweiten Halbjahr 2021 waren es noch lediglich 5'400.

Rückenwind verleiht diesem bedenklichen Boom ein kriminelles Geschäftsmodell: Verschiedenste Gruppierungen stellen im Darknet Ransomware as a Service (RaaS) zur Verfügung, um Unternehmen oder Behörden zu erpressen. Die Software erlaubt es auch Anwendern ohne Programmierkenntnisse, Daten zu verschlüsseln und im Rahmen der sogenannten Double-Extortion-Strategie zu entwenden und zu veröffentlichen – Stichwort «Hack-and-leak».

2. IoT-Malware wird für Unternehmen und Behörden zum Problem

Die Botnet-Attacke mit der Malware Mirai, die im Jahr 2016 Websites wie Twitter und Netflix lahmlegte, machte es auf einen Schlag deutlich: Das Internet of Things (IoT) bietet neue Einfallstore für Cyber-Angriffe. Mit dem Internet verbundene Geräte wie Drucker oder Kameras sind meist unzureichend gegen Cyber-Attacken geschützt. Dabei nehmen Cyber-Kriminelle vermehrt auch die Infrastruktur von Unternehmen und Behörden ins Visier. Der Grund: Neben der Information Technology (IT) wird vermehrt auch die Operational Technology (OT) und damit zunehmend die kritische Infrastruktur mit IoT-Geräten ausgestattet.

Mittlerweile hat sich die Bedrohungslage weiter intensiviert. 2022 war ein Rekordjahr**,** wie ein aktueller **Report** aus den USA zeigt: Im ersten Halbjahr legten IoT-Angriffe um 77 Prozent zu. Mit weltweit insgesamt 57 Millionen Attacken wurden innert sechs Monaten fast so viele Vorfälle registriert wie im gesamten Vorjahr. Botnets wie MIRAI und Mozi legten in puncto Grösse und Aktivität deutlich zu. Dieser Trend dürfte sich 2023 aufgrund der rasant wachsenden IoT-Ökosysteme und der sich nur langsam verbessernden IoT-Sicherheitl fortsetzen.

Die Einsatzzwecke von IoT-Malware sind vielfältig. Früher haben Cyber-Kriminelle IoT-Geräte – wie bei der erwähnten Mirai-Attacke – verwendet, um mit einem Distributed Denial of Service (DDoS) die IT-Infrastruktur zu überlasten. Heute werden IoT-Schlupflöcher aber auch genutzt, um Ransomware einzuschleusen. Auf dem Vormarsch ist zudem Cryptojacking: Dabei werden IoT-Geräte ohne Befugnis genutzt, um Kryptowährungen «schürfen».

3. Mailserver rücken zunehmend in den Fokus

Forschende aus dem Bereich Cyber Security legen Ihren Fokus vermehrt auf Mailserver. Der Grund: E-Mail-Programme bieten eine enorme Angriffsfläche und bergen gleichzeitig grosse Mengen an potenziell interessanten Informationen. Vor allem für politisch motivierte Advanced Persistent Threats (APT) sind Mailserver attraktive Ziele. Die Akteure nutzen Schwachstellen systematisch aus, profitieren aber auch von der Ausgesetztheit der Systeme: Die grossen Software-Stacks und die vielen unterstützten Protokolle erleichtern Angriffe.

Die Marktführer haben den ersten Stresstest bereits hinter sich: Microsoft Exchange und Zimbra hatten in letzter Zeit beide mit kritischen Schwachstellen zu kämpfen, die von Angreifern ausgenutzt wurden, bevor Patches verfügbar waren. Der Sicherheitssoftware-Anbieter **Kaspersky** rechnet im kommenden Jahr mit der Ausnützung weiterer Schwachstellen. Die Experten gehen gar davon aus, dass 2023 das Jahr der «Zero Days» für alle grossen E-Mail-Programme werden wird.

4. Drohnen und Satelliten geraten ins Visier von Hackern

Der Ukrainekrieg hat die Wichtigkeit von kommerziellen Drohnen in politischen Konflikten untermauert. Entsprechend gewinnt für die involvierten Akteure auch deren Manipulation an Bedeutung. Die Fachleute von **Kaspersky** prognostizieren denn auch eine Intensivierung von spezifischer Malware-Entwicklung mit dem Fokus, Drohnensteuerungen zu kompromittieren oder deren Datenübertragung zu beeinflussen, zum Beispiel den Kamera-Stream.

Darüber hinaus sehen die Cyber Security-Experten Drohnen aber auch als Mittel für eine neue Art von hybriden Proximity-Hacking-Angriffen, die physische und digitale Strategien kombinieren. Mögliche Angriffsszenarien umfassen Drohnen, die das Sammeln von WPA-Handshakes ermöglichen, welche zum Offline-Knacken von WLAN-Passwörtern verwendet werden. Auch das

Ablegen von mit Malware infizierten USB-Sticks in geschützten Bereichen wäre mit Drohnen möglich – mit der Absicht, dass jemand den Datenträger findet und an ein Gerät anschliesst.

Neben Drohnen geraten auch **Satelliten** vermehrt ins Visier von Cyber-Kriminellen. 2022 zeigte sich dies bereits mit aller Deutlichkeit: Beim Einmarsch Russlands in die Ukraine wurde das Satellitennetzwerk Viasat gehackt. Darauf funktionierte die Satellitenkommunikation in Osteuropa nicht mehr und es kam vielerorts zu Störungen der Internetverbindung. Auch in Mitteleuropa zeigten sich Auswirkungen, unter anderem funktionierten Windkraftanlagen in Deutschland nicht mehr.

5. Der Malware-Dschungel wächst unaufhaltsam

Totgesagte leben länger: Die Malware Emotet wurde im Januar 2021 von Europol unschädlich gemacht, doch seit einem guten Jahr treibt sie wieder ihr Unwesen. Das verdeutlicht, dass sich bekannte Malware-Varianten kaum stoppen lassen. Und laufend kommen Neue hinzu: Der US-Cybersecurity-Anbieter **SonicWall** identifizierte im ersten Halbjahr 2022 über 270'000 neue Malware-Varianten. Das sind 45 Prozent mehr als im Halbjahr zuvor – und entspricht rund 1'500 neuen Varianten pro Tag.

Gemäss Statistik des **Nationalen Zentrums für Cybersicherheit (NCSC)** lässt sich der Grossteil der im ersten Halbjahr 2022 in der Schweiz gemeldeten Malware-Angriffe der Familie AgentTesla zuordnen. Dabei handelt es sich um einen Trojaner, der Anmeldeinformationen exfiltriert, Tastatureingaben protokolliert, Zwischenablagedaten kopiert und Screenshots sammelt. Zu den Top 3 gehören zudem FormBook und SnakeKeyLogger, die ebenfalls auf Informationsdiebstahl spezialisiert sind.

Der beliebteste Angriffsvektor, um Malware einzuschleusen, bleibt Phishing. Dominant sind laut NCSC vor allem E-Mails mit falschen Paketankündigungen im Namen diverser Logistiker. Doch die Social Engineering-Taktiken von Cyber-Kriminellen werden immer raffinierter. Vermehrt werden auch gestohlene E-Mail-Konversationen mit Lieferanten oder Kunden als Köder genutzt – so etwa bei der Malware Qakbot, die in der Schweiz in den letzten Monaten häufig für Ransomware-Angriffe eingesetzt wurde.