CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

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

WISSENS-UPDATE

Ausblick 2024: Die fünf wichtigsten Malware-Trends

Künstliche Intelligenz (KI) ist die unberechenbarste Bedrohung für die Cyber-Sicherheit im kommenden Jahr. Die Technologie eröffnet Cyber-Kriminellen eine ganze Palette an neuen Möglichkeiten. Zudem rückt 2024 eine Reihe von unterschätzten Angriffsvektoren in den Vordergrund: APIs, IoT-Geräte, Cloud-Dienste und Kollaborationsplattformen.

1. KI bedroht die Cyber-Sicherheit

Künstliche Intelligenz (KI) leistet in der Abwehr von Cyber-Angriffen seit geraumer Zeit nützliche Dienste. Nun wechselt KI die Seite: Mit dem Erfolg von Sprachmodellen wie Chat-GPT ist die Technologie im Alltag angekommen und steht damit auch Cyber-Kriminellen frei zur Verfügung. In ihren Händen wird das praktische Werkzeug zur vielseitig einsetzbaren Waffe.

Die Bandbreite an Bedrohungen ist gross: KI unterstützt Phishing, da sich einschlägige Mails schneller formulieren und personalisieren lassen. Deepfakes eröffnen neue Möglichkeiten, um Mitarbeitende mit gefälschten Videos, Fotos oder Tonaufnahmen zur Preisgabe von vertraulichen Informationen oder zur Ausführung von Zahlungen zu bewegen. Auch bei der Entwicklung von Malware kann die Technologie hilfreich sein. Die grösste Sorge ist, dass KI die Automatisierung der Cyber-Angriffe vorantreibt.

2. APIs werden zum grössten Angriffsvektor

Application Programming Interfaces (APIs) sind das Rückgrat des Internets. Über 80 Prozent des gesamten Traffics läuft mittlerweile über APIs. Die Programmierschnittstellen ermöglichen es unabhängigen Anwendungen, miteinander zu kommunizieren und Daten auszutauschen.

Gleichzeitig bieten sie Cyber-Kriminellen aber auch eine Angriffsfläche, um Daten zu entwenden oder eine Distributed-Denial-of-Service-Attacke (DDoS) auszuführen.

Das Beratungsunternehmen Gartner sagte bereits 2021 in einer **Prognose** voraus, dass APIs bis 2024 zum grössten Angriffsvektor aufsteigen werden. Tatsächlich sorgten API-Angriffe in den letzten Monaten immer wieder für Schlagzeilen, zum Beispiel die Attacke auf T-Mobile Anfang 2023. Den Angreifern gelang es, persönliche Daten von 37 Millionen Kundinnen und Kunden zu entwenden. Dass solche Datenpannen inzwischen gang und gäbe sind, zeigt die Studie **State of API Security** von Traceable: 60 Prozent der Unternehmen haben in den letzten zwei Jahren ein Datenleck im Zusammenhang mit APIs festgestellt.

3. Das IoT-Gerät unter Dauerbeschuss

Das Internet of Things (IoT) wächst kontinuierlich. 2025 soll es bereits achtmal so viele vernetzte Geräte geben wie Menschen auf der Welt. Unternehmen und Behörden tragen massgeblich zum raschen Wachstum des IoT-Marktes bei. Die Netzwerke grösserer Organisationen umfassen meist mehrere tausend vernetzte Geräte. Viele davon sind nur ungenügend gesichert und diese Schlupflöcher wissen Cyber-Kriminelle auszunutzen.

2023 haben die Angriffe auf IoT-Geräte erneut stark zugenommen. Der **Enterprise IoT and OT Threat Report** des US-amerikanischen Cyber Security-Anbieters Zscaler stellte im ersten Halbjahr 2023 eine Zunahme der Angriffe um 400 Prozent im Vergleich mit der Vorjahresperiode fest. Mittlerweile sind mehr als die Hälfte der Unternehmen jede Woche mit Angriffsversuchen auf IoT-Geräte konfrontiert. Zu diesem Ergebnis kommt eine **Studie** des israelischen Unternehmens Check Point.

4. Die Risiken in der Cloud nehmen zu

Die Cloud gilt gemeinhin als sicher. Schliesslich investieren die führenden Anbieter viel in die Sicherheit ihrer Lösungen. Dennoch können sich Unternehmen nicht blind auf Cloud-Lösungen verlassen. Die grössten Risiken lauern aufseiten der Nutzerinnen und Nutzer: Eine fehlerhafte Konfiguration der Cloud-Dienste oder ein mangelhaftes Zugriffsmanagement können fatale Folgen haben.

Die **Cloud Security Study** von Thales zeigt, dass der Angriffsvektor an Bedeutung gewinnt: Verzeichneten im Vorjahr noch 35 Prozent der Unternehmen eine Datenpanne in der Cloud, waren es 2023 bereits 39 Prozent. Dabei hat der Anteil sensitiver Daten in der Cloud stark zugenommen, wobei weniger als die Hälfte dieser Daten adäquat verschlüsselt ist. Und da die meisten Unternehmen bereits mehrere Clouds verwenden – Stichwort Multicloud – multiplizieren sich auch die Risiken.

5. Phishing verlagert sich auf Teams, Zoom & Co.

Mit der Pandemie hat sich die Kommunikation von Unternehmen auf Plattformen wie Microsoft Teams oder Zoom verlagert. Damit sind Kollaborationsplattformen ins Visier von Cyber-Kriminellen geraten. E-Mail blieb dabei zunächst der dominierende Angriffsvektor: Betrüger verschickten täuschend echte Einladungen im Namen der Plattformen und brachten die Opfer dazu, sensible Informationen preiszugeben.

In jüngster Zeit mehren sich jedoch die Fälle, bei denen Phishing auf den Plattformen selbst betrieben wird. Im Juni 2023 wurde in Microsoft Teams eine Schwachstelle entdeckt, die es externen Personen erlaubt, Dateien direkt in den Chat von Organisationen zu stellen. Ein Hacker publizierte im Juli schliesslich das Tool TeamsPhisher. Dieses erlaubt es Angreifern, mit minimalem Aufwand Phishing auf der Plattform zu betreiben. Alles was es dafür braucht, ist eine Datei mit Malware, eine Chat-Nachricht und eine Liste von Empfängern.

Beginnen Sie heute und schützen Sie Ihre IT-Systeme vor Malware.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre Sicherheitsbedürfnisse, um gegen Malware gefeit zu sein.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.