Presseinformation

Sicherheitslagebericht: KI-Einsatz durch Cyberkriminelle weiter auf dem Vormarsch

Trend Micro warnt zudem vor Zunahme von Angriffen auf gefährdete Cloud-Anwendungen

Garching bei München, 20. August 2024 – Trend Micro, einer der weltweit führenden Anbieter von Cybersicherheitslösungen, fasst in seinem aktuellen Lagebericht die wichtigsten IT-Sicherheitstrends im ersten Halbjahr 2024 zusammen. Trotz einiger erfolgreicher Operationen von Strafverfolgungsbehörden gegen Ransomware und Phishing bleibt das Bedrohungsniveau hoch. Cyberkriminelle haben aus den jüngsten Erfolgen der Polizei gelernt und passen ihre Taktiken an. Dabei setzen sie neben altbewährten Angriffsmethoden zunehmend auf Künstliche Intelligenz (KI) und nutzen globale Ereignisse wie die Olympischen Spiele und nationale Wahlen für ihre Zwecke aus.

Auch im ersten Halbjahr 2024 bleibt ein Hauptziel von Cyberkriminellen, schnelle, unauffällige und gleichzeitig ausgeklügelte Bedrohungen und Kampagnen zu entwickeln. Der japanische Cybersecurity-Spezialist beobachtete in der ersten Jahreshälfte wie Cyberkriminelle auf falsch konfigurierte und ungeschützte Assets abzielten, um heimlich in Systeme einzudringen und sensible Daten zu stehlen. Insgesamt dominiert der Zugriff auf gefährdete Cloud-Anwendungen die Liste der Risikoereignisse in der ersten Jahreshälfte von 2024. In vielen Fällen setzte auch ein fehlender Endpoint-Schutz auf nicht verwalteten Geräten Unternehmen unnötigen Risiken aus.

Trotz Erfolgen der Strafverfolgungsbehörden bleibt Bedrohungslage komplex

Die Ransomware-Familie mit den meisten Datei-Erkennungen war in der ersten Jahreshälfte 2024 LockBit, wobei die Erkennungszahlen in Folge der Polizeiaktion „Operation Cronos“ massiv zurückgingen. Finanzinstitute waren am stärksten von Ransomware-Angriffen betroffen, dicht gefolgt von Unternehmen der Technologiebranche.

Ungeachtet der erfolgreichen Strafverfolgungsmaßnahmen im ersten Halbjahr 2024 bleibt die Bedrohungslage komplex:

- **LockBit:** Trotz erheblicher Disruption und Sanktionen versucht LockBit, seine Position zu halten. Trend Micro analysierte eine neue Version, LockBit-NG-Dev, die in .NET geschrieben ist und plattformunabhängig sein könnte.

- **Dropper-Malware-Netzwerke**: Auch nach der Zerschlagung von Botnetzen wie IcedID und Trickbot finden Ransomware-Gruppen weiterhin

Wege, Systeme zu infiltrieren, etwa durch die Ausnutzung kritischer Schwachstellen, den Missbrauch von Tools zur Fernüberwachung und -verwaltung (RMM), Bring-Your-Own-Vulnerable-Driver (BYOVD)-Angriffe sowie die Verwendung benutzerdefinierter Shell-Skripte.

- **Neue Werkzeuge und Taktiken:** Sowohl staatlich unterstützte Akteure als auch Cyberkriminelle setzten kompromittierte Router als Anonymisierungsebene ein. Während Gruppen wie Sandworm eigene Proxy-Botnets verwenden, greifen andere wie APT29 auf kommerzielle Proxy-Netzwerke zurück. Die APT-Gruppe Earth Lusca nutzte in einer untersuchten Kampagne die angespannten Beziehungen zwischen China und Taiwan als Social-Engineering-Köder, um gezielt Opfer zu infizieren.

Akteure reizen Grenzen von KI weiter aus

Trend Micro beobachtete, dass Bedrohungsakteure Malware in legitimer KI-Software verstecken, kriminelle LLMs (Large Language Models) betreiben und sogar Jailbreak-as-a-Service-Angebote verkaufen. Letztere ermöglichen es Cyberkriminellen, generative KI-Bots so auszutricksen, dass sie Fragen beantworten, die gegen ihre eigenen Richtlinien verstoßen – besonders, um Malware und Social-Engineering-Köder zu entwickeln. Auch Deepfake-Angebote haben die Akteure verfeinert, um virtuelle Entführungen durchzuführen, gezielten Betrug in Form von BEC (Business-E-Mail-Compromise) zu begehen und KYC (Know-Your-Customer)-Kontrollen zu umgehen. Für Letzteres wurde zudem Malware entwickelt, die biometrische Daten abfängt.

„Die Cybersicherheit hat sich in den vergangenen Jahren weiterentwickelt, um den zunehmend komplexen und gezielten Angriffen gewachsen zu sein“, erklärt Udo Schneider, Governance, Risk & Compliance Lead Europe bei Trend Micro. „In den kommenden Jahren wird es für die Sicherheitsbranche unerlässlich werden, proaktiv zu agieren. Geschäftsführungen und Sicherheitsteams müssen die sich ständig verändernden Bedrohungen und Risiken mit einem resilienzorientierten, datengestützten Ansatz und einer umfassenden Strategie zum (Cyber) Risk Management bewältigen.“

Weitere Informationen

Eine detaillierte Zusammenfassung der Ergebnisse liefert der deutschsprachige Blog von Trend Micro:
https://www.trendmicro.com/de_de/research/24/h/halbjahres-cybersicherheitsreport-grenzen-ausreizen.html

Den vollständigen *Trend Micro 2024 Midyear Cybersecurity Threat Report* finden Sie in englischer Sprache hier:
https://www.trendmicro.com/vinfo/de/security/research-and-analysis/threat-reports/roundup/pushing-the-outer-limits-trend-micro-2024-midyear-cybersecurity-threat-report

Über Trend Micro
Trend Micro, einer der weltweit führenden Anbieter von Cybersicherheit, hilft dabei, eine sichere Welt für den digitalen Datenaustausch zu schaffen. Basierend auf jahrzehntelanger Expertise in IT-Sicherheit und Künstlicher Intelligenz, globaler Bedrohungsforschung und beständigen Innovationen schützt unsere KI-gestützte Cybersecurity-Plattform hunderttausende Unternehmen und Millionen von Menschen über Clouds, Netzwerke, Geräte und Endpunkte hinweg.

Trend Micros Plattform ist führend in Cloud- und Enterprise-Cybersecurity und bietet fortschrittliche Verteidigungstechnologien für Umgebungen wie AWS, Microsoft und Google. Zentrale Sichtbarkeit ermöglicht es Unternehmen, Angriffe schneller zu erkennen und besser darauf zu reagieren.

Mit 7.000 Mitarbeitern in 70 Ländern ermöglicht Trend Micro Unternehmen, ihre vernetzte Welt zu vereinfachen und zu schützen. Die deutsche Niederlassung von Trend Micro befindet sich in Garching bei München. In der Schweiz kümmert sich die Niederlassung in Wallisellen bei Zürich um die Belange des deutschsprachigen Landesteils, der französischsprachige Teil wird von Lausanne aus betreut; Sitz der österreichischen Vertretung ist Wien. https://www.trendmicro.com/de_de/business.html

Pressekontakt:
Akima Media GmbH
Christina Rottmair
Hofmannstraße 54
D-81379 München
Telefon: +49 (0) 89 17959 18 – 0
Fax: +49 (0) 89 17959 18 – 99
E-Mail: trendmicro@akima.de
Internet: www.akima.net

Unternehmenskontakt:
Trend Micro Deutschland
Tobias Grabitz
Parkring 29
D-85748 Garching bei München
Telefon: +49 (0) 89 839 329 – 737
Fax: +49 (0) 89 839 329 – 799
E-Mail: tobias_grabitz@trendmicro.com
Internet: www.trendmicro.com