Cybertrends 2025:
Kriminelle Nebelkerzen und demokratisierte Cyberattacken

Was bedeutet 2025 für unsere Cybersicherheit? Welche Cyberattacken werden häufiger, welche Branchen stehen besonders im Visier und welche Rolle spielt KI?

Von Michael Veit, Technology Evangelist bei Sophos

In der Cybersicherheit haben die letzten Jahre gezeigt, dass man mit allem rechnen muss. Da niemand in die Zukunft sehen kann, lohnt jedoch eine Rückschau auf 2024, um Entwicklungen zu bewerten, mögliche Szenarien für die Zukunft zu antizipieren und um sich anzupassen und mit Zuversicht in ein neues Jahr zu blicken. Die Security ist gut aufgestellt, aber Wachsamkeit ist und bleibt oberstes Gebot. Denn die Kriminellen sind zunehmend opportunistisch, was ihre Beute, Auftraggeber und Unterstützer anbelangt.

Was also können wir in der Cybersicherheit von 2025 erwarten?

1. Angreifer fokussieren sich verstärkt auf die Cloud
Da immer mehr Unternehmen ihre Geräte mit Endpoint Detection and Response (EDR) schützen und die Verbreitung der Multi-Faktor-Authentifizierung (MFA) zunimmt, gehen Ransomware-Angreifer verstärkt dazu über, Cloud-Ressourcen ins Visier zu nehmen, die normalerweise nicht über MFA verfügen. Der „Preis“ für Kriminelle besteht nicht mehr in Passwörtern, sondern in Authentifizierungs-Tokens und Browser-Cookies.

2. Generative KI sorgt für „Demokratisierung“ cyberkrimineller Aktivitäten
Tools und Verfahren, die professionelle Cyberkriminelle nutzen, werden von vielen GenKI-Plattformen als Trainingsdaten verwendet. Dies bedeutet, dass bestimmte cyberkriminelle Aktivitäten „demokratisiert“ wurden und geringqualifizierte, opportunistische Angreifer nun ohne großen Aufwand zum Beispiel einen Phishing-Köder oder Ransomware-Code erstellen können. Aufgrund der fehlenden Professionalität haben diese Attacken zwar eine geringe Erfolgsquote, sie tragen aber aufgrund ihrer Masse dazu bei, die Ressourcen der Verteidiger zu binden und damit den Weg für die Profi-Angreifer freizumachen.

3. Cyberkriminelle zünden zunehmend Nebelkerzen
Cyberkriminelle nutzen zunehmend Ablenkungsmanöver, um ihre eigentlichen Hauptaktivitäten zu verschleiern und für Störungen und Verwirrung bei der Verteidigung zu sorgen. Kleinere Angriffsoperationen binden die Reaktionsressourcen und führen zu einer Minderung der Gesamteffektivität des Abwehrsysteme. Dies führt zu einem Ungleichgewicht zwischen den Guten und den Bösen, selbst bei gut aufgestellter Cybersicherheit.

4. Angriffe auf die Lieferkette haben stärkere Auswirkungen
Angriffe auf die Software-Lieferkette, deren Folgen weit über das Business einzelner Unternehmen hinausgehen, bilden ein immer wichtigeres Element in den Angriffsstrategien der Cyberkriminellen. Sie wollen möglichst viel Druck aufbauen, um damit ihren Lösegeldforderungen noch mehr Gewicht zu verleihen sowie die erpressten Summen zu erhöhen.

5. Komplexe Cyberattacken nutzen LLM-Multiagentensysteme
Auch Cyberkriminelle profitieren von der aktuellen Entwicklung bei der Nutzung von LLMs, die darin besteht, Modelle miteinander zu verketten, um komplexere Aufgaben zu erstellen. Anstatt beispielsweise nur ChatGPT zu nutzen, um eine Codezeile zu schreiben, können

Cyberkriminelle jetzt mehrere LLMs kombinieren, um umfangreichere Projekte wie KI-generierte Websites, Videos oder Deepfakes zu erstellen.

6. Cyberkriminelle streben nach mehr ROI
Die Ausbeutung nach der erfolgreichen Infiltration eines Unternehmens ist kein eingleisiger Prozess mehr. Angreifer setzten zunehmend auf einen „Double-Dip"-Ansatz. Wenn sie beispielsweise Kryptowährungen stehlen, werden zudem Cookies oder Ausweisdokumente geraubt, um diese für weitere Straftaten zu verwenden.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de