„Das Gesamtproblem besteht darin, dass wir nicht schnell genug vorankommen und die Kriminellen geschickter und agiler sind als unsere Regierungen und Sicherheitsrichtlinien. Unternehmen auf der ganzen Welt unterschätzen ihr Sicherheitsrisiko und investieren zu wenig in die Verbesserung ihrer Cybersicherheitslage."

# Wenn der Schutz des Normalbürgers nicht gelingt, haben wir versagt

*Sophos Field CTO Chester Wisniewski zu Stand und Zukunft der Cybersicherheits-Lage:*
*:*

- *Cyberkriminelle sind deutlich agiler als unsere Regierungen, Unternehmen und Sicherheitsrichtlinien*
- *Beim Internet der Dinge, den betrieblichen Sicherheitstools und einem Großteil der Unternehmenssoftware kommt Security immer noch zu kurz*
- *KI steckt in der Cyberkriminalität aktuell noch in den Kinderschuhen*

*Von Chester Wisniewski, Field CTO bei Sophos*

**Geschichte wiederholt sich, doch die Agilität der Angreifenden wächst**
Wenn uns die Geschichte etwas gelehrt hat, ist es die Erkenntnis, dass sich viele Dinge wiederholen. Entsprechend wird die Bedrohungslandschaft im Jahr 2024 sehr ähnlich zu der im Jahr 2023 sein – allerdings mit einem entscheidenden Unterschied: Cyberattacken werden noch effizienter und sind vermehrt mit opportunistischen Wendungen verknüpft. Denn Kriminelle haben fast immer nur das schnelle Geld im Sinn und werden weiterhin mit Datenverschlüsselungen oder der Androhung von Datenveröffentlichungen Lösegelder erpressen, um ihren Reichtum zu vermehren.

Wo wir viel Bewegung sehen, ist die Frage, was die kriminellen Aktivitäten am einfachsten ermöglicht und wie variabel die Cyberkriminellen agieren. Jahr für Jahr beobachten wir einen stetigen Wechsel zwischen der Ausnutzung von Zero-Day-Schwachstellen und der Verwendung gestohlener Zugangsdaten, um sich in die Netzwerke der Opfer einzunisten. Wenn eine neue Schwachstelle verfügbar und leicht auszunutzen ist – wie kürzlich zum Beispiel bei Citrix Bleed – dann wird sie auf Teufel komm raus ausgebeutet. Sobald allerdings ein Großteil der potenziellen Opfersysteme gepatcht ist oder bereits kompromittiert wurde, kehren die Angreifer wieder auf die etwas weniger effiziente Methode des Anmeldedatendiebstahls zurück – getreu dem Motto „Wir brechen nicht mehr ein, wir loggen uns ein."

**Lieferketten und „As a Service"-Angebote zunehmend im kriminellen Fokus**
Da Unternehmen zunehmend die Multifaktor-Authentifizierung einführen, haben Kriminelle damit begonnen, noch smartere Umgehungsmöglichkeiten zu entwickeln und sich stattdessen zum Beispiel dem Diebstahl von Cookies und Sitzungscookies zugewandt. In Kombination mit bösartigen Proxy-Servern wie Evilginx, Social-Engineering-Angriffen und sogenannten MFA-Fatigue-Angriffen entsteht so eine hocheffektive Angriffsmischung. Gruppen wie LAPSU$ oder Scattered Spider haben mit ihren erfolgreichen Attacken auf große Markennamen 2022 und 2023 die Aufmerksamkeit aller auf sich gezogen und Blaupausen geschaffen, die wahrscheinlich noch mehr Kriminelle dazu inspirieren, sich mit diesen Playbooks in Netzwerke zu schleichen.

Zunehmend im Fokus der Angriffe stehen dabei auch Lieferketten und „As a Service"-Angebote. Schon 2023 erfolgten immer mehr Attacken nicht über das anvisierte Unternehmen direkt, sondern einen Geschäfts- oder Servicepartner. Ob durch die Kompromittierung von Managed Service Providern (MSPs), File-Sharing-Appliances oder durch Authentifizierungsanbieter – manchmal ist der einfachste Weg zum Einbruch die Hintertür. Da Unternehmen eigene Netzwerke weiter härten und gleichzeitig mehr „As-a-Service"-Modelle einführen, können wir davon ausgehen, dass diese indirekten Angriffe 2024 zunehmen.

**Noch steckt die KI in der Cyberkriminalität in den Kinderschuhen**

Überschaubar ist hingegen (noch) der Einfluss von Künstlicher Intelligenz auf Cyberattacken, während der konkrete Einsatz von KI durch Cyberkriminelle offenbar noch in den Kinderschuhen steckt, diskutieren Bedrohungsakteure bereits intensiv über das Potenzial für Social Engineering. Ein Beispiel dafür ist die aktuelle „Pig Buchtering"-Welle mit Romance Scams. Momentan macht sich die Technologie vor allem in der Verteidigung durch eine effizientere Ausführung der bestehenden Arbeit der Sicherheitsteams bemerkbar. KI ermöglicht eine bessere Erkennung von Anomalien in großen Datensätzen, da die Maschine alle Informationen auf einmal „sehen" und dabei helfen kann, die Aufmerksamkeit des Menschen auf Dinge zu lenken, die vom Normalen abweichen.

**Regierungen werden beginnen (müssen), Gegenmaßnahmen zu ergreifen**

Abseits der technologischen Entwicklung gehe ich davon aus, dass Regierungen auf der ganzen Welt substanziellere Maßnahmen ergreifen, um Ransomware-Gruppen entgegenzuwirken. Grund dafür ist, dass das tägliche Leben der Menschen zunehmend beeinträchtigt wird, wenn Krankenhäuser, Schulen, Anwaltskanzleien oder Banken aufgrund von Ausfallzeiten im Zusammenhang mit Cyberangriffen nicht arbeiten können. Wir erreichen einen Punkt, an dem die Menschen anfangen, effektivere Maßnahmen gegen Cyberkriminalität zu fordern. Es ist schwer abzuschätzen, was kommen wird und wie effektiv die Maßnahmen schlussendlich sein werden, aber es würde mich zum Beispiel sehr wundern, wenn nicht einige Länder versuchen würden, Lösegeldzahlungen zu verbieten, da die Ransomware-Epidemie weiterhin hohe wirtschaftliche Kosten mit sich bringt und Millionen in die Kriegskassen der Cyberkriminellen spült.

**Wenn der Schutz des Normalbürgers nicht gelingt, haben wir versagt**

Der immer größere Einfluss von Cyberattacken auf unser tägliches Leben stellt einen weiteren, wichtigen Erfolgsfaktor in den Fokus: Systeme müssen den Durchschnittsmenschen schützen, ohne dass dieser geschult werden oder darüber nachdenken muss. Wenn das nicht gelingt, haben wir versagt. Der aktuell wichtigste Handlungsbedarf besteht darin, das Passwort abzuschaffen und auf eine Phishing-resistente Authentifizierung wie Passschlüssel umzusteigen. Passschlüssel ermöglichen es einem Benutzer, zum Beispiel einfach den biometrischen Sensor auf seinem Mobilgerät zu verwenden, um sich bei seiner E-Mail, in sozialen Medien oder auf seinem bevorzugten Shop zu authentifizieren. Wenn wir die Komplexität eliminieren und Dinge wie Software-Updates weiterhin automatisierter gestalten, kann sich die breite Öffentlichkeit endlich zurücklehnen, entspannen und ihre Online-Zeit genießen, ohne Angst vor Hackerangriffen haben zu müssen.

**Frustrierend niedrige Sicherheit bei IOT-Geräten**

Aber auch in der digitalen Welt im Allgemeinen gibt es eine große Sicherheitsherausforderung. Nämlich die Verbreitung von immer mehr vernetzten Geräten und die frustrierend niedrige Qualität der darin enthaltenen Sicherheit. Während beim Schutz unserer Smartphones und Webbrowser große Fortschritte erzielt wurden, kommen solche Vorsichtmaßnahmen beim Internet der Dinge, den betrieblichen Sicherheitstools und einem Großteil der Unternehmenssoftware, von der unsere Welt abhängt, leider immer noch viel zu kurz. Es wird zu wenig in die Sicherung des Open-Source-Software-Ökosystems investiert, das die elementare Basis für unsere Cloud-Dienste und zunehmend jedes Gerät, das wir besitzen, ist.

Das Gesamtproblem besteht darin, dass wir nicht schnell genug vorankommen und die Kriminellen geschickter und agiler sind als unsere Regierungen und Sicherheitsrichtlinien. Unternehmen auf der ganzen Welt unterschätzen ihr Sicherheitsrisiko und investieren zu wenig in die Verbesserung ihrer Cybersicherheitslage.

**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