Retrospektive 2023:
Cyberkriminelle sind profitgierig, suchen den geringsten Widerstand und jede Hürde trägt dazu bei, dass sie weiterziehen

Faulheit als Strategie: Der Weg des geringsten Widerstands war für die Cyberkriminellen in 2023 der profitabelste

Statement von Chester Wisniewski, Director, Global Field CTO bei Sophos, zum Jahr 2023

Eine Wahrheit, die uns dieses Jahr erneut begegnet ist, hat mehr Nuancen als vielleicht erwartet: Nämlich wie faul Cyberkriminelle sind und wie agil sie gleichzeitig werden, wenn es darum geht, schnell auf Situation zu reagieren und von neuen Entwicklungen zu profitieren. Die Fälle, die in den letzten Monaten vom Sophos Incident Response Team bearbeitet wurden, zeigen deutlich, dass die Kriminellen ihr Fähnchen nach dem Wind richten und hauptsächlich zwischen der Verwendung gestohlener Anmeldedaten und der Ausnutzung ungepatchter Schwachstellen hin und her wechseln.
Das ist kein Wunder, denn warum sollten Angreifer sich unnötige Mühe machen und einen schwierigen Weg gehen, wenn ihre potenziellen Opfer es ihnen leicht machen? Ergo ist der einfachste Weg gleichzeitig der beliebteste. Wenn allerdings der Weg des geringsten Widerstands direkt mit der Verfügbarkeit hochkarätiger Exploits zu Beginn des Jahres verbunden war und jetzt deren Seltenheit Kriminelle dazu bewegt, zum Diebstahl von Anmeldedaten überzugehen, hilft uns dieses Wissen, eine effektive Verteidigung aufzubauen. Erstens sollten wir mehr Zeit darauf verwenden, alle extern anfälligen Systeme zu patchen und zweitens sollten wir eine Multifaktor-Authentifizierung auf allen von außen zugreifbaren Systemen etablieren. Mit jeder zusätzlichen Schutzfunktion können wir die Hürden für Angreifer erhöhen und das in zweifacher Hinsicht. Verteidigungsmaßnahmen schützen nicht nur, sie verursachen bei den Cyberkriminellen auch Kosten und schrecken daher viele Akteure in der stark profitgeprägten Szene ab.

Es gibt keine Zeit zu verlieren
Eine weitere wichtige Erkenntnis aus dem Jahr 2023 ist, dass wir bei der Verteidigung viel weniger oder am besten keine Zeit verlieren dürfen. Die durchschnittliche Zeitspanne, die ein Angreifer benötigt, um in ein Netzwerk einzudringen und die finale Phase seiner Attacke auszulösen, ist von zehn Tagen im Jahr 2022 auf acht Tage in den ersten sechs Monaten des Jahres 2023 gesunken – Tendenz weiter fallend. Daher müssen wir bei der Angriffserkennung und -reaktion noch schneller werden, um die Attacken so früh wie möglich zu unterbinden.
Allerdings haben auch die Cyberkriminellen verstanden, dass Schnelligkeit ein Trumpf für erfolgreiche Angriffe ist. Die Gruppierungen spezialisieren sich daher immer stärker auf bestimmte Teilaufgaben und kooperieren in komplexen Netzwerken, um ihre Ziele so schnell und effizient wie möglich zu erreichen. Erschwerend kommt hinzu, dass sie mit den riesigen gestohlenen Geldsummen immer mehr talentierte Hacker anlocken, um eine Verteidigung zu durchbrechen.

Und täglich grüßt das Einfallstor
Die wichtigste Lektion des Jahres 2023 ist, dass vieles, was falsch war, immer noch falsch ist. Zwar konnten wir einige wichtige Probleme, wie zum Beispiel das Ausnutzen von Flash und Java zur Kompromittierung von PCs oder die fehlende Internetverschlüsselung durch die fast

flächendeckende TLS-Nutzung lösen, aber leider gibt es immer noch zu viele leichte Ziele und Einfallstore für die Cyberkriminellen.

Wenn wir bildlich gesprochen Türen und Fenster unverschlossen lassen, müssen wir uns nicht wundern, wenn Eindringlinge plötzlich im Wohnzimmer stehen. Die Schritte, die unternommen wurden, um gemeinschaftlich unsere Sicherheit verbessern, funktionieren erwiesenermaßen. Jetzt müssen wir auf diesen Erfolgen aufbauen und es für Kriminelle immer schwieriger und kostspieliger machen, ihre Ziele zu realisieren. Entscheidende Erfolgsfaktoren dabei sind das schnelle und vollständige Patchen aller Systeme, eine starke Nutzer-Authentifizierung sowie effektive Überwachungs- und Wiederherstellungsservices rund um die Uhr.

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