Erkenntnisse aus der Chefetage: 2022 Bericht zur Schwachstellenanalyse

Die Bedrohungslandschaft ist heute eine völlig andere als noch vor fünf Jahren. Das Ökosystem der Cyberkriminalität floriert und ist komplex, vielfältig und auf Kosten der globalen Unternehmen äußerst profitabel. Ransomware-Gruppen und Access-Broker sind neben Botnet-Betreibern und staatlich unterstützten Bedrohungsakteuren zu einer wachsenden Cybercrime-Wirtschaft geworden, deren weitreichende Taktiken und Angriffsziele kaum ein Unternehmen unberührt lassen, unabhängig von seiner Größe oder Branchenzugehörigkeit.

Ein anhaltend hohes Bedrohungsklima

- Das Jahr 2021 war ein Rekordjahr hinsichtlich der Geschwindigkeit und des Ausmaßes von Cyberbedrohungen: Im Durchschnitt ereigneten sich alle 11 Tage massive Angriffe. 2022 gab es einen leichten Rückgang bei den Zero-Day-Exploits und Massenangriffen. Allerdings bleibt der seit mehreren Jahren zu beobachtende Trend der zunehmenden Geschwindigkeit und Größenordnung von Angriffen insgesamt bemerkenswert konstant.
- Mit der zunehmenden Weiterentwicklung der Geschäftsmodelle und des Angriffsverhaltens von Cyberkriminellen gehen wir davon aus, dass die Makrotrends im Jahresvergleich weiterhin nur geringen Schwankungen unterliegen werden. Diese Variabilität ermöglicht zwar eine nuancierte Analyse der Gegenspieler und ihrer Beweggründe, trägt aber nur wenig dazu bei, das anhaltend erhöhte Risikoklima für globale Unternehmen zu mildern.

Ausgereifte Cyberbedrohungen sind den Sicherheitsteams oft weit voraus

- Das Zeitfenster zwischen der Erkennung neuer Schwachstellen und deren Ausnutzung in Angriffen wird immer kürzer. Im Jahr 2022 wurden 56% der Schwachstellen in unserem Bericht innerhalb von sieben Tagen nach ihrer Entdeckung ausgenutzt, und mehr als 40% der umfassenden Angriffe begannen mit einem Zero-Day-Exploit. Das bedeutet, dass die Sicherheitsteams ein immer kleineres oder schlichtweg nicht vorhandenes Zeitfenster haben, um neue Schwachstellen zu beheben und erfolgreiche Angriffe zu verhindern. Und das wiederum belastet die ohnehin schon knappen Sicherheitsressourcen vieler Unternehmen erheblich.
- Vorteilhaft ist daher ein durchdachtes Notfall-Patching-Verfahren sowie ein allgemein robustes Verfahren zur Abwehr von Vorfällen. Es wäre jedoch unrealistisch zu erwarten, dass Teams, die immer noch mit der Bereitstellung von Ressourcen für grundlegende Sicherheitsaktivitäten zu kämpfen haben, über solide Notfallverfahren verfügen. Sicherheitsteams müssen in der Lage sein, grundlegende Sicherheitsprogramme wie proaktives Asset- und Schwachstellen-Management umzusetzen, bevor sie effektiv auf eine Krise reagieren können.

Technologie kann nur mit Fachwissen effektiv sein

- Mit der zunehmenden Verbreitung der Cloud und der immer komplexer werdenden Technologie-Stacks wächst auch die mögliche Angriffsfläche, was Angreifern mehr Möglichkeiten zur Kompromittierung von Unternehmensnetzwerken bietet. Technologie-Lösungen sind ein notwendiger Bestandteil jeder Sicherheitsstrategie eines Unternehmens, doch die Bekämpfung und Abwehr moderner Cyber-Bedrohungen erfordert fast immer menschliche Fachkenntnisse zusätzlich zu den Technologien, die Transparenz und Schutz für die gesamte Cloud- und

On-Premise-Umgebung eines Unternehmens bieten. Unternehmensleiter dürfen nicht davon ausgehen, dass Technologie allein die Lösung für komplexe Angriffsmuster ist. Sie sollten prüfen, inwieweit ihr Unternehmen zur Umsetzung von Sicherheitsmechanismen in der Lage ist, die Angreifer erkennen und abwehren können.

Empfehlungen für die C-Suite und die Führungsetage

- In der Bedrohungslandschaft von heute sehen sich Sicherheitsteams häufig dazu gezwungen, reaktiv zu handeln, was die Effizienz und Tragfähigkeit von Sicherheitsprogrammen beeinträchtigt. Vorstände und Führungskräfte profitieren davon, dass sie einen Einblick in die Herausforderungen von Sicherheitsprogrammen und die potenziellen Auswirkungen einer Beeinträchtigung dieser Programme erhalten.
- Die schwierigen makroökonomischen Bedingungen in den Jahren 2022 und 2023 haben den Druck auf das Risikomanagement weiter erhöht. Die Teams müssen die Effizienz steigern und gleichzeitig die Integrität sensibler Daten und Geschäftsabläufe bewahren. Insbesondere in einem unbeständigen makroökonomischen Klima kann die anhaltende Ressourcenknappheit zu einer unbemerkten Anhäufung von Risiken und einem Verlust an technischem Fachwissen führen, das für wirksame Sicherheitsverfahren, darunter auch die Abwehr von Zwischenfällen, erforderlich ist.
- Verantwortliche in Unternehmen sollten die zunehmende Verbreitung von Sicherheitsbedrohungen und die Allgegenwärtigkeit von sowohl komplexen als auch „banalen" Angriffen auf Unternehmensnetzwerke ernst nehmen. Sicherheitsmetriken und Risikomodelle sollten auf den Unternehmenskontext abgestimmt sein und in die allgemeine strategische Planung einfließen. Im Idealfall wird die Sicherheit als konzernweite Aufgabe betrachtet, die nicht nur von einzelnen Funktionsbereichen getragen wird.
- Akzeptable Risiken sind Risiken, die klar definiert sind: Vorstände und Führungskräfte sollten ein umfassendes und nachvollziehbares Verständnis dafür haben, wie sich die eingeschränkten Ressourcen des Sicherheitsprogramms sowie die Realität des Bedrohungsklimas auf die Aufrechterhaltung des Geschäftsbetriebs auswirken können – einschließlich der Vertraulichkeit von geistigem Eigentum und der Integrität sensibler Daten und Lieferketten. Es ist grundsätzlich nachvollziehbar, dass Vorstände und Geschäftsführer Risiken im Rahmen von Unternehmensentscheidungen in Kauf nehmen, solange diese in einen bestimmten Kontext gestellt und explizit benannt werden.

Lesen Sie den vollständigen Bericht zur Schwachstellenanalyse für 2022 von Rapid7

BERICHT HERUNTERLADEN