Die wichtigsten Erkenntnisse aus dem Attack Intelligence Report 2024

Die Welt der Cybersicherheit hat sich verändert. Seit Ende 2020 konnte Rapid7 einen enormen Anstieg von Zero-Day-Angriffen, Ransomware-Attacken und Massenkompromittierungen beobachten, von denen viele Unternehmen weltweit betroffen sind. Das Verhalten der Angreifer hat sich dabei weiterentwickelt. Sowohl staatlich gesponserte Angreifer als auch Ransomware-Gruppen setzen komplexe Zero-Day-Exploit-Ketten und neuartige Persistenzmechanismen ein. Da die Angriffsfläche in globalen Cloud- und On-Premise-Umgebungen weiter zunimmt, sind Unternehmen mehr denn je gefordert, Sicherheit zu einem zentralen Bestandteil ihrer Geschäftsstrategie zu machen.

Nachfolgend sind wichtige Erkenntnisse aus dem Rapid7 Attack Intelligence Report 2024 aufgeführt.

Zero-Day-Angriffe und Ausnutzung von Netzwerk-Edge-Geräten

Zum zweiten Mal innerhalb von drei Jahren wurden mehr Massenkompromittierungen durch Zero-Day-Schwachstellen als durch N-Day-Schwachstellen verursacht. Das bedeutet, dass viele Angriffe stattfinden, bevor Unternehmen überhaupt merken, dass sie angreifbar sind. Auch die Art und Weise dieser Massenkompromittierungen hat sich verändert. Anstatt das bekannte Muster „viele Angreifer, viele Ziele“ zu verfolgen, erfolgte fast ein Viertel (23 %) der weit verbreiteten CVEs-Bedrohungen aus gut geplanten, hoch orchestrierten Zero-Day-Angriffen, bei denen ein einzelner Angreifer Dutzende oder Hunderte von Organisationen kompromittiert hat – oft unter Verwendung proprietärer Exploits oder Backdoors.

Die Zahl der groß angelegten Kompromittierungen, die auf die Ausnutzung von Netzwerk-Edge-Geräten zurückzuführen sind, hat sich 2023 fast verdoppelt. 36 % der von Rapid7 verfolgten, weit verbreiteten Schwachstellen treten in Netzwerk-Edge-Technologien auf. 60 % davon waren Zero-Day-Angriffe. Netzwerk-Edge-Technologien sind für den Betrieb vieler moderner Netzwerke unverzichtbar, stellen aber auch eine erhebliche Schwachstelle in unserer kollektiven Cybersicherheitsverteidigung dar, wie die jahrelange Historie von Angriffen zeigt.

Ransomware bedeutet Big Business

Ransomware-Zahlungen sollen im Jahr 2023 weltweit die Marke von 1 Milliarde Dollar überschrittenhaben – und das sind nur die Zahlungen, die uns bekannt sind. Ransomware-Gruppen erzielen zweistellige Millionenprofite, indem sie Unternehmen mit doppelten Erpressungsangriffen attackieren.

Unsere Analyse ergab außerdem eine Zunahme von „Smash-and-Grab“-Angriffen, die auf Dateiübertragungslösungen abzielten. Bei diesen Angriffen versuchten die Angreifer, schnell Zugriff auf vertrauliche Daten zu erhalten und diese so schnell wie möglich abzuziehen. Während es sich bei den meisten von Rapid7 beobachteten Ransomware-Vorfällen noch um „traditionelle“ Angriffe handelte, bei denen Daten verschlüsselt wurden, werden „Smash-and-Grab“-Erpressungen immer häufiger.

Rapid7 Labs konnte über

5.600

Ransomware-Vorfälle verfolgen,

die zwischen Januar 2023 und Februar 2024 gemeldet wurden. Die Dunkelziffer dürfte bedeutend höher liegen, da viele Ransomware-Angriffe immer noch nicht gemeldet werden.

Die MFA (Multi-Faktor-Authentifizierung) stellt für viele Organisationen immer noch eine Lücke dar

VPNs und virtuelle Desktop-Infrastrukturen waren die führenden Ziele der Vorfälle, die durch korrekt implementierte MFA hätten verhindert oder verlangsamt werden können. Die Ausnutzung von Schwachstellen war auch ein häufiger erster Zugriffsvektor bei den Vorfällen, auf die Rapid7 MDR 2023 und Anfang 2024 reagierte.

Wie können sich Organisationen schützen?

Die Implementierung und Durchsetzung der Multi-Faktor-Authentifizierung sollte für Sicherheitsteams oberste Priorität haben. Da über 40 % der Vorfälle auf einen fehlenden MFA-Schutz zurückzuführen sind, empfehlen wir dies als wichtigste zu ergreifende Maßnahme. Auch im heutigen Bedrohungsklima müssen wir unbedingt proaktiv und aggressiv die im Internet zugängliche Angriffsfläche reduzieren.

Angesichts der weit verbreiteten Angriffe auf Dateiübertragungstechnologien empfehlen wir Unternehmen außerdem, Maßnahmen zu ergreifen, um die Daten-Exfiltration schneller zu erkennen und zu verhindern. Dazu gehören die Überwachung oder Sperre bekannter Filesharing-Websites oder Datenübertragungsprogramme, die Warnung vor (oder Einschränkung von) großen Datei-Uploads und ungewöhnlichen Zugriffen auf Cloud-Speicher sowie die Implementierung von Ausgangsfilterung.

Und schließlich ist ein robustes Programm zur Verwaltung von Schwachstellen wie immer eine Kernkomponente jeder Sicherheitsstrategie, sowohl in der Cloud als auch vor Ort. Die Bedeutung eines soliden Schwachstellen- und Patch-Managements ist heute noch genauso wichtig, da die Bedrohungsakteure ihre Techniken und Vorgänge weiterentwickelt haben. Ganz im Gegenteil: Diese grundlegenden Praktiken gehören zu den besten proaktiven Schritten, die Unternehmen ergreifen können, um die Anfälligkeit für moderne Bedrohungen zu minimieren.

Zusätzliche Ressourcen

Wenn eine neue Bedrohung auftaucht, finden Sie Rapid7-Anleitungen im Abschnitt Neu auftretende Bedrohungen des Rapid7-Blogs zusammen mit den entsprechenden Informationen für Rapid7-Kunden. Forscher und Community-Mitglieder von Rapid7 veröffentlichen auf der offenen Forschungsplattform AttackerKB von Rapid7 Schwachstellenanalysen. Diese Analysen umfassen häufig stichprobenhaften Code und Indikatoren zum Machbarkeitsnachweis für eine Kompromittierung sowie Exploit-Zeitpläne und Analysen der Angriffskette. Die Zero-Day-Schwachstellenforschung von Rapid7 wird hier regelmäßig veröffentlicht.

Mehr als

40 %

der Vorfälle, die Rapid7s Managed Detection and Response Teams im Jahr 2023 verzeichnete, waren auf eine fehlende oder nicht durchgesetzte Multi-Faktor-Authentifizierung (MFA) zurückzuführen.

RAPID7

PRODUKTE

Cloud Security
XDR und SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestrierung & Automatisierung
Managed Services

KONTAKT

rapid7.com/contact

Hier erfahren Sie mehr und können eine kostenlose Testversion anfordern:
rapid7.com/try/insight