RAPID7

rapid7.com

2024 Attack Intelligence Report:

Erkenntnisse aus vier Jahren Schwachstellen- und Exploit-Daten

Im Attack Intelligence Report 2024 untersucht Rapid7 Schwachstellendaten und Angreiferverhalten aus vier Jahren, um Sicherheitsexperten zu helfen, die Risiken, Motive und Taktiken der Bedrohungsakteure der heutigen Cyberbedrohungen zu erkennen. Nachfolgend einige der wichtigsten Erkenntnisse:

Eine hohe Anzahl an Zero-Day-Angriffen ist zur Norm geworden

Die durchschnittliche Zeit bis zum Bekanntwerden eines Angriffs für CVEs, die Rapid7 ab 2020 analysiert hat

Ein Tag

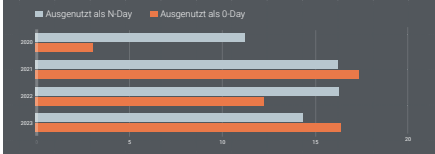
53% der CVE-basierten Massenkompromittierungen, die Rapid7 zwischen Januar 2023 und Februar 2024 verfolgt hat, entstanden durch Zero-Day-Exploits

Die Zahl der Exploits von Netzwerk-Edge-Geräten nahm explosionsartig zu – sogar noch stärker als in den vergangenen Jahren.

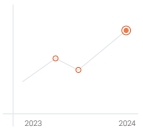
36% der 2023 weit verbreiteten Bedrohungen betreffen die **Netzwerk-Perimeter-Technologie**

60% der von Rapid7 analysierten Schwachstellen in Netzwerk- und Sicherheits-Appliances werden als **Zero-Day-Appliances ausgenutzt**

Weit verbreitete, Bedrohungen ausgesetzte CVEs 2020–2024



Ransomware-Operationen sind schneller, heftiger und verheerender als je zuvor



Rapid7 Labs verfolgte **zwischen Januar 2023 und Februar 2024 über 5.600 Ransomware-Vorfälle***

*Diese Zahl spiegelt keine Vorfälle wider, die nicht gemeldet wurden

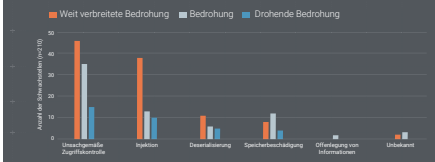
Die Anzahl der neuen Ransomware-Familien ist um mehr als die Hälfte zurückgegangen, was darauf hindeutet, dass bereits bestehende Modelle und Funktionen für Angreifer rentabel bleiben

Die Ursachenanalyse zeigt, dass Angreifer Exploits für einfache Schwachstellenklassen bevorzugen

75%

75 % der beachtenswerten CVEs, die Rapid7 seit 2020 analysiert hat, haben unsachgemäße Zugriffskontroll- und Injektionsprobleme als Hauptursachen

Schwachstellenklassen und Bedrohungsstatus 2020-2024



Was tun wir dagegen?

Wie erhöhen wir unsere Widerstandsfähigkeit und Bereitschaft gegenüber den heutigen Cyberbedrohungen? Einige Hinweise:

40% der Vorfälle waren auf eine fehlende oder uneinheitliche MFA zurückzuführen. Machen Sie die MFA zur obersten Priorität

Wenden Sie die Prinzipien der geringsten Privilegien an: Auflistung des Standards zulassen; granulare Zugriffskontrolle implementieren; Benutzer regelmäßig überprüfen und entfernen

Implementieren Sie in der Cloud und vor Ort ein starkes proaktives Schwachstellen-Risikomanagement-Programm

Erstellen Sie Zero-Day-Patching-Verfahren für unternehmenskritische Technologien, insbesondere für Netzwerk-Edge-Geräte

Die Verdoppelung einer Offsite-Backup-Strategie hilft Unternehmen, widerstandsfähiger gegen potenzielle Ransomware-Angriffe zu werden

Laden Sie den vollständigen Bericht herunter auf www.rapid7.com