IN ZAHLEN:

Die moderne Schwachstellen-Landschaft

ninjaOne

Anstieg von CVEs um

275% seit 2024

Der DBIR-Bericht 2025 von Verizon wies für das Jahr 2024 einen erstaunlichen Anstieg der erfolgreichen Ausnutzung von Schwachstellen um 180 % aus. Ein zweiter, am 23. April 2025 veröffentlichter, Bericht zeigte einen weiteren Anstieg um 34 %.

Dies entspricht täglich 132 neuen Schwachstellen und Sicherheitslücken (CVEs), von denen 33 % der CVEs als hoch oder bedenklich eingestuft werden.

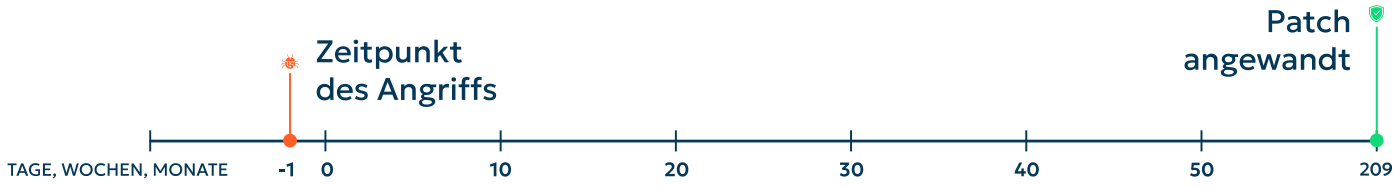
Verizon berichtet:

Nur 54 % der Schwachstellen werden innerhalb von 32 Tagen behoben.

Besorgniserregender ist jedoch, dass die durchschnittliche Patching-Zeit 209 Tage beträgt.

Auf Unternehmenssoftware entfielen 44 % aller Zero-Day-Exploits im Jahr 2024 und 48 % im Jahr 2025

50 % bis 61 % aller neuen Schwachstellen werden innerhalb von 48 Stunden nach Bekanntwerden ausgenutzt.



Der Zeitpunkt Null ist der Zeitpunkt, an dem ein Patch verfügbar gemacht wird. Angreifer nutzen oft Schwachstellen aus, bevor es Patches gibt, während Unternehmen bis zu **209 Tage** brauchen, um diese Patches bereitzustellen.

Angriffsvektoren

Das Ausnutzen von Schwachstellen ist inzwischen ebenso verbreitet wie Phishing- oder Passwortangriffe. Tatsächlich stellte Verizon fest, dass:

die Ausnutzung von Schwachstellen um das

8-fache von 3 % auf 22 %

angestiegen ist.

Eine bessere Lösung

NinjaOne Vulnerability Management mit Echtzeit-Analyse eliminiert die Scan-Zyklen vollständig und liefert stets aktuelle Informationen über Schwachstellen ohne Störung der Endpunkt-Produktivität. Kombiniert mit NinjaOne Autonomous Patch Management schafft dies ein geschlossenes System zur Risikoabwehr. Schwachstelleninformationen fließen direkt in KI-gesteuerte Patch-Workflows ein und beschleunigen die Behebung, während sie das Betriebsrisiko senken.

Erfahren Sie mehr unter
ninjaone.com/de/schwachstellenmanagement/