Die Krux mit der Priorisierung von Patches

Sophos X-Ops gibt Einblick in die Priorisierung von Schwachstellen und Patches mit unterschiedlichen Methoden und zeigt die potenziellen Stolpersteine und Alternativen.

Die Zahl der bekannten neuen Schwachstellen, auch Common Vulnerabilities and Exposures (CVE) genannt, nimmt jährlich zu. In 2022 waren es 25.277, in 2023 bereits 29.065 CVEs. Es ist davon auszugehen, dass es 2024 nochmals mehr waren. Die Schwierigkeit für IT-Profis liegt darin, die Schwachstellen zu priorisieren, um sie dann zu patchen. Sophos X-Ops gibt in einem zweiteiligen Bericht (Part 1 und Part 2) tiefe Einblicke in die Möglichkeiten der Bewertung und Priorisierung.

Evergreen CVSS
Laut FIRST bietet das Common Vulnerability Scoring System (CVSS) eine Methode zur Erfassung der wichtigsten Merkmale einer Schwachstelle. Es bietet seit vielen Jahren eine numerische Einstufung des Schweregrads von Schwachstellen zwischen 0,0 und 10,0 und wird nicht nur häufig für die Priorisierung verwendet, sondern ist auch in einigen Branchen und Behörden vorgeschrieben, darunter die Payment Card Industry (PCI).

Die Skala für die Einstufung der Schwachstelle ist:
Keine: 0,0
Gering: 0,1 - 3,9
Mittel: 4,0 - 6,9
Hoch: 7,0 - 8,9
Kritisch: 9,0 - 10,0

Die Krux dabei ist, dass mit CVSS zwar der Schweregrad der Schwachstelle eingestuft werden kann, jedoch nicht, welche CVEs die Bedrohungsakteure in Zukunft ausnutzen werden oder wann. Daher ist die Priorisierung der Patches nach CVSS allein nicht zwingend zielgerichtet. Die Forschungsergebnisse von Howlands mit einer Stichprobe von über 28.000 CVEs beispielsweise zeigen, dass Schwachstellen mit einem CVSS Score von 7 am ehesten als Waffe eingesetzt werden. Bei Schwachstellen mit einer Bewertung von 5 ist die Wahrscheinlichkeit, größer als bei Schwachstellen mit einer Bewertung von 6, und bei Schwachstellen mit einer Bewertung von 10 - kritische Schwachstellen - ist die Wahrscheinlichkeit, dass für sie ein Exploit entwickelt wird, geringer als bei Schwachstellen mit einer Bewertung von 9 oder 8. Mit anderen Worten: Es scheint keine eindeutige Korrelation zwischen der CVSS-Bewertung und der Wahrscheinlichkeit einer Ausnutzung zu bestehen.

Zusätzliche alternative Priorisierung mit EPSS
Ein weiteres Beispiel für die Priorisierung von Patches ist das Exploit Prediction Scoring System (EPSS). Es liefert im Gegensatz zum Schweregrad einer Schwachstelle mit CVSS einen Wahrscheinlichkeitswert für Ausnutzung einer bestimmten Schwachstelle. Allerdings – darauf weisen die Spezialisten von Sophos X-Ops eindringlich hin - misst es weder die Wahrscheinlichkeit, dass ein Unternehmen speziell angegriffen wird, noch die Auswirkungen eines erfolgreichen Angriffs oder die Aufnahme einer Schwachstelle in das Toolkit (z. B.) eines Wurms oder einer Ransomware-Bande.

Kombination von Priorisierungs-Alternativen

Neben CVSS und EPSS existieren weitere Möglichkeiten der Priorisierung beispielsweise mit SSVC und dem KEV Catalog. Es ist nicht überraschend, dass es keine vollkommen perfekte Lösung oder Kombination von Priorisierungslösungen gibt, die alle Priorisierungsprobleme lösen. Die Kombination von Priorisierungsmöglichkeiten ist jedoch fast immer besser als die Verwendung nur eines einzelnen Systems. Eine Priorisierung geht zudem über geeignete Tools hinaus. Das Schwachstellenmanagement und die Priorisierungsentscheidungen basieren idealerweise auf einer Vielzahl von Quellen, darunter Bedrohungsdaten, Schwachstellen, Sicherheitslage, Kontrollen, Risikobewertungen, Ergebnisse von Pentests oder Sicherheitsaudits.

Details zu den Schwachstellen- und Patch-Priorisierungsmöglichkeiten sind in den Reports von Matt Wixey, Principal Technical Editor and Senior Threat Researcher bei Sophos, beschrieben.

Hier geht es zu den Report Teil I und II:
Teil 1:
https://news.sophos.com/en-us/2024/12/27/prioritizing-patching-a-deep-dive-into-frameworks-and-tools-part-1-cvss/
Teil 2:
https://news.sophos.com/en-us/2024/12/30/prioritizing-patching-a-deep-dive-into-frameworks-and-tools-part-2-alternative-frameworks/

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, Senior PR-Manager EMEA Central
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