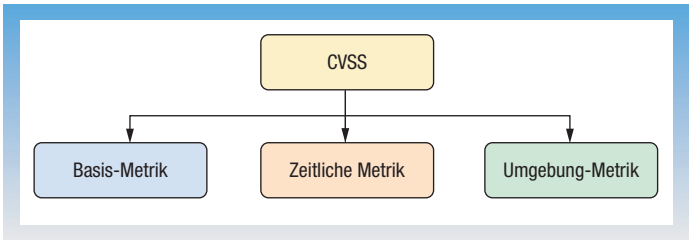
Bewertung von Sicherheitslücken

Quelle
Chip.de und dgc.org

Um die Schwere von Sicherheitslücken zu bewerten, gibt es seit 2005 das Common Vulnerability Scoring System (CVSS). Ende 2023 kam die neue Version des Standards heraus.



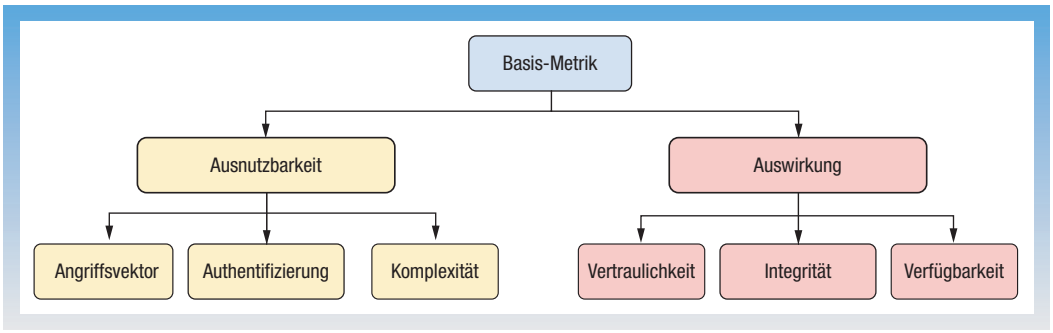
Bilder: Andreas Wisler

Der CVSS-Score besteht aus den drei Hauptkategorien Basis, Zeit und Umgebung.

Das standardisierte System zur Bewertung von Sicherheitslücken existiert seit 2005 und ist mehrfach an aktuelle Anforderungen angepasst worden. CVSS verwendet eine Reihe von Metriken, um die Auswirkungen einer Schwachstelle auf Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu bewerten sowie zusätzliche Faktoren wie den Grad der Zugriffskontrolle, die Komplexität der Ausnutzung und die erforderlichen Benutzerprivilegien. Basierend auf diesen Metriken wird jeder Schwachstelle ein numerischer Score zugewiesen, der die Schwere der Schwachstelle widerspiegelt. CVSS-Scores reichen von 0 bis 10, wobei höhere Werte auf schwerwiegendere Schwachstellen hinweisen. Darüber hinaus bietet CVSS eine umfassende Methode zur Dokumentation und Kommunikation von Schwachstellen, indem es eine standardisierte Sprache und Metriken verwendet, die von Sicherheitsfachleuten weltweit verstanden werden können. Dies erleichtert die Zusammenarbeit und den Informationsaustausch über Schwachstellen zwischen verschiedenen Organisationen und fördert eine effiziente und konsistente Reaktion auf Sicherheitsvorfälle.

CVSS definiert drei grundlegende Metriken. Am häufigsten wird die Basisbewertung verwendet, die die grundlegenden Eigenschaften einer Schwachstelle abbilden soll: etwa, wie einfach sie sich ausnutzen lässt und welche Auswirkungen sie hat.

Um festzustellen, wie schwer der Grad einer Schwachstelle wiegt und wie hoch der CVSS-Score entsprechend ausfällt, müssen bei der Berechnung verschiedene Kriterien berücksichtigt werden. Der Score besteht im Grunde aus drei Hauptkategorien: Basis, Zeit und Umgebung:



Die Basis-Metrik.

ZUM AUTOR
Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Basis-Metrik

Die Basis-Metrik beschreibt, wie gefährlich eine IT-Sicherheitslücke ist und wie hoch das Potenzial ist, dass diese für Cyberangriffe ausgenutzt werden kann. Zur Berechnung werden die grundlegenden technischen Merkmale einer Schwachstelle herangezogen: Die Ausnutzbarkeit beschreibt zum Beispiel, unter welchen Voraussetzungen ein Angriff erfolgen kann. Mit der Auswirkung lässt sich das Ausmass eines Schadens ermitteln.

Die Basis-Metrik wird für jede Schwachstelle einmal festgelegt – in der Regel von der Person, die die Schwachstelle entdeckt, dem Hersteller des Produkts oder IT-Spezialisten.

Zeitliche Metrik

Die zeitliche Metrik fasst zeitliche Veränderungen zusammen, die Einfluss auf die Gefährdung durch bestimmte Sicherheitslücken haben können. Diese Metrik kann sich zum Beispiel erhöhen, wenn mit einer Wahrscheinlichkeit definiert wird, ab wann eine zuvor nur beschriebene Schwachstelle tatsächlich auftritt. Über einen sogenannten Report Confidence bestätigen Hersteller diese Schwachstelle und benennen sie anhand einer eindeutigen CVE (siehe nachfolgend). Um den zeitlichen Einfluss positiv zu beeinflussen, stellen viele Hersteller zusätzlich einen Patch zur Behebung des Problems zur Verfügung und senken somit die Bewertung.

Umgebungs-Metrik

Mit der Umgebungs-Metrik lassen sich die Werte konkret an die eigene IT-Architektur und Systemumgebung anpassen. Dafür ist es wichtig im Vorfeld zu analysieren, welche Systeme für einen störungsfreien Betrieb dringend notwendig sind. Diese werden in der Berechnung als relevante Faktoren berücksichtigt. Welche Massnahmen sind notwendig und bereits im Einsatz, um die eigene IT-Sicherheit zu erhöhen und vertrauliche Informationen zu schützen? Je nachdem, wie stark die Schutzziele durch einen Cyberangriff verletzt werden könnten, erhöht sich der CVSS-Score oder kann nachträglich abgesenkt werden.

Hinweis: Das Forum of Incident Response and Security Team hat unter www.first.org/cvss/v4-0/ alle Teilwerte ausführlich beschrieben. Unter www.first.org/cvss/calculator/4.0 ist zudem ein Rechner zu finden. Die verschiedenen Werte können ausgewählt und definiert werden.

Das Resultat wird in folgende Kategorien unterteilt:

Basis-Wert	Sicherheitseinstufung
0	keine
0,1 bis 3,9	niedrig
4,0 bis 6,9	mittel
7,0 bis 8,9	hoch
9,0 bis 10	kritisch

Weil die Kürzel recht ähnlich aussehen, wird CVSS manchmal mit CVE verwechselt. Die Common Vulnerabilities and Exposures sind aber nur ein vereinheitlichtes Bezeichnungssystem für Schwachstellen, damit diese nicht mehrfach geführt werden. Eine Sicherheitsbewertung gibt es bei CVE nicht.

Während mit dem CVSS Risikofaktoren im IT-Bereich bewertet werden können, wird das Common Vulnerabilities and Exposure (CVE) genutzt, um bekannte Schwachstellen und Sicherheitslücken eines Systems oder Produkts eindeutig zu benennen. Mit einem festgelegten Muster sorgt das CVE-System dafür, dass es bei der Benennung der Gefahren zu keinen Dopplungen oder Verwechslungen kommt. Der Name setzt sich dabei aus dem Kürzel CVE, der Jahreszahl, in der das Problem entdeckt wird, sowie einer fortlaufenden Nummer zur genauen Identifizierung der Schwachstelle zusammen.

Die CVE sind in einer öffentlich zugänglichen Datenbank verfügbar, die von der Cybersecurity-Community verwendet wird, um Sicherheitslücken zu verfolgen, zu referenzieren und zu beheben. Die CVE-Datenbank wird von der gemeinnützigen Organisation MITRE Corporation verwaltet (siehe www.mitre.org/) und enthält Informationen über Sicherheitslücken in einer Vielzahl von Software- und Hardwareprodukten. Jede CVE-Eintragung enthält Details zur Schwachstelle, einschliesslich einer Beschreibung des Problems, der betroffenen Software oder Hardware, potenziellen Auswirkungen und Informationen darüber, wie die Schwachstelle behoben oder gemildert werden kann. Die Verwendung von CVE-Nummern erleichtert damit im Unternehmen die Koordination von Sicherheitspatches und die Priorisierung von Sicherheitsmassnahmen. Darüber hinaus unterstützt es Forscher bei der Analyse von Trends in der Sicherheitslandschaft und ermöglicht es Unternehmen, proaktiv gegen bekannte Schwachstellen vorzugehen, um ihre Systeme vor Cyberangriffen zu schützen.

Fazit

Mit CVSS steht eine einheitliche Berechnungsweise von Schwachstellen zur Verfügung. Bei hohen Werten muss schnell reagiert und der hoffentlich bereits verfügbare Patch eingespielt werden. Um Schwachstellen in Software zu suchen, kann die CVE-Datenbank genutzt werden, in welcher alle bekannt gewordenen Schwachstellen strukturiert abrufbar sind.