



Cyber-Sicherheitsrat
Deutschland e.V.

Werkzeugkasten Cybersicherheit



Schwachstellenscan

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen, unklare Zuständigkeiten** und regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

Was wir dabei oft vergessen sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.

Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.



Hans-Wilhelm Dünn

Präsident

Cyber-Sicherheitsrat Deutschland e.V.

Schwachstellenscan – Was ist das?

Bei einem **Schwachstellenscan** (engl. Vulnerability Scan) werden Computernetzwerke und deren angeschlossenen Geräte mit einer dafür vorgesehenen **Software auf Schwachstellen untersucht**. Das Screening eines Systems dient dazu, die erhobenen Informationen mit bestehenden **Datenbanken** abzugleichen und so bekannte und teilweise geläufige Schwachstellen zu entdecken. Mithilfe des daraus erstellten **Schwachstellenberichts** können die bestehenden Verwundbarkeiten geheilt werden. In der Regel ist der Schwachstellenscan Teil einer umfassenden **Schwachstellenanalyse**, die die gefundenen Verwundbarkeiten adressatengerecht beurteilt.



Wie sind die Scans gestaltet?

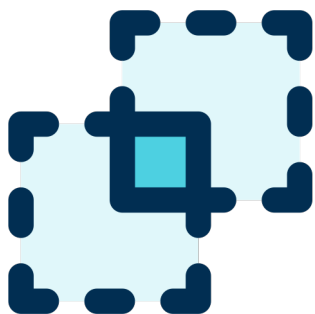
Grundsätzlich läuft ein Schwachstellenscan **automatisiert** ab, teilweise mit durch **Künstliche Intelligenz oder Machine Learning gestützte Methoden**. Bei Schwachstellenscans werden alle (wichtigen) Geräte, Schnittstellen, Interfaces, Ports und Verschlüsselungen im Netzwerk getestet und analysiert.

Im ersten Schritt werden **Informationen über das Zielobjekt** gesammelt, um daran anknüpfend mit der **Scanningsoftware** die vorhandenen Sicherheitslücken in der IT-Infrastruktur zu identifizieren. Anschließend werden die gefundenen Schwachstellen anhand Ihres Schweregrads für die Sicherheitsarchitektur eingeordnet und ihre **Relevanz bewertet**.

Im Schwachstellenbericht werden schließlich die Verwundbarkeiten aufgeführt und entsprechende **Handlungsempfehlungen** zur Schließung entwickelt. Nachdem die Schwachstellen gepatcht wurden, kann ein **erneuter Scan** die Wirksamkeit der Änderungen prüfen.



Was ist der Unterschied zu Pentests?



Auch mit KI gestützten Tools und ihrer breiten Abdeckung haben Schwachstellenscans einen **anderen Ansatz** als Pentests.

Pentests enthalten eine **menschliche Komponente**, umfassen einen begrenzten **Testzweck** und versuchen Schwachstellen im **Gesamtprozess** offenzulegen.

Bei Schwachstellenscans werden üblicherweise alle (wichtigen) technischen Komponenten im Netzwerk getestet, um eine **möglichst vollständige technische Sicherheit** zu erreichen.

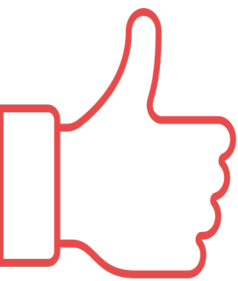
Neue Systeme mit **KI-Unterstützung kombinieren** mehrere Methoden der Absicherung und erlauben voraussichtlich bald eine ähnliche Tiefe der Prüfung wie technische Pentests, jedoch hängt die Qualität der Tools von den genutzten Datenbanken ab. Es ist zu erwarten, dass die großen Cloudanbieter aufgrund der immensen Datenmengen, die diese analysieren, eine Führungsrolle einnehmen werden. Da Pentests jedoch auch menschliche Aspekte sowie Unternehmensabläufe einbeziehen, wird es langfristig **beide Methoden gleichberechtigt** geben müssen.

Wem nutzen Schwachstellenscans?

Schwachstellenscans sind ein **niedrigschwelliges** Tool, um **präventiv** auf Cyberbedrohungen einzugehen. Aufgrund der **leichten Verfügbarkeit** sind sie für jede Organisation nützlich und angeraten.



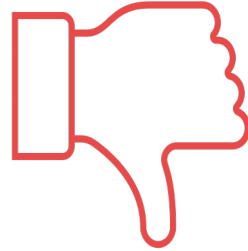
Welche Chancen gibt es?




Ein Schwachstellenscan ist aufgrund der vollautomatisierten Durchführung **sehr schnell** und **verhältnismäßig kostengünstig**, beispielsweise im Vergleich zu einem Pentest. Das **Kosten-Nutzen-Verhältnis** ist bei dieser Methode besonders hoch. Zudem können die meisten Sicherheitslücken sehr schnell gepatcht werden. Er dient vorrangig dazu, die **bekanntesten und relevantesten Bedrohungen** eines Systems zu identifizieren, um diese für kriminelle Hacker leicht nutzbaren Ziele zu schließen.

Welche Risiken gibt es?

Beim Überprüfen der Systeme kann es gelegentlich zu **Ausfällen** kommen, wenn die Scans nicht fachgerecht durchgeführt werden. Die Qualifikation und **Expertise des Anbieters** sind daher zu prüfen. Zudem erhöhen sie den **Netzwerktraffic** und können so die Verfügbarkeit von Systemen beeinträchtigen. Ein Schwachstellenscan ist nur so gut, wie die **Datenbank**, auf die er zurückgreift. Die dort enthaltenen Schwachstellen bilden die Grundlage für die Erkennung in den Zielsystemen. Sie können nur die Schwachstellen abbilden, die bereits bekannt sind – **neuartige oder wenig bekannte Verwundbarkeiten** werden möglicherweise nicht berücksichtigt. Das alleinige Vertrauen auf einen Schwachstellenscan kann zu einem **trügerischen Sicherheitsgefühl** führen, weshalb dieses Werkzeug in ein **ganzheitliches Sicherheitssystem** integriert werden sollte, das auch andere Methoden einbezieht.



Fazit



Schwachstellenscans geben einen **breit angelegten Überblick** über Verwundbarkeiten der eigenen Systeme, bilden jedoch lediglich eine **Momentaufnahme** ab und sollten durch **weitere Methoden** wie Pentests unterstützt werden. Um eine größere Sicherheit zu erhalten, sollte ein Schwachstellenmanagement etabliert werden, das **fortlaufend** und **holistisch** in regelmäßigen Abständen Scans durchführt und entsprechende Handlungsmaßnahmen ableitet.