



Cyber-Sicherheitsrat
Deutschland e.V.

Werkzeugkasten Cybersicherheit



Schwachstellenmanagement

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.

Schwachstellenmanagement – Was ist das?

Schwachstellenmanagement (engl. Vulnerability Management) beschreibt den **Prozess** der Identifizierung, Bewertung, Priorisierung, Überwachung und Behebung von Schwachstellen in Informationssystemen, Netzwerken, Anwendungen und Infrastrukturen.

Das Ziel des Schwachstellenmanagements ist es, die **Verfügbarkeit, Vertraulichkeit und Integrität von IT-Systemen** zu gewährleisten, Risiken zu minimieren und Unternehmen vor potenziellen Bedrohungen durch Cyberangriffe und Datenverluste zu schützen.



Wem nutzt ein Schwachstellenmanagement?



Der Adressatenkreis für Maßnahmen zum Schwachstellenmanagement umfasst verschiedene Beteiligte, die unterschiedliche Rollen und Verantwortlichkeiten in diesem Prozess innehaben.

Die **IT-Abteilungen** sind für die Umsetzung und Überwachung von Schwachstellenmanagement-Systemen verantwortlich. Die **Geschäftsleitung** hat die Aufgabe, strategische Entscheidungen zu treffen und das Budget für Sicherheitsmaßnahmen zuzuweisen. **Mitarbeiter** tragen ebenfalls Verantwortung, indem sie Sicherheitsrichtlinien einhalten und an Schulungen im Bereich IT-Sicherheit teilnehmen. **Externe Partner und Dienstleister** spielen ebenfalls eine wichtige Rolle, indem sie bei der Identifizierung und Behebung von Schwachstellen helfen und ihre Expertise einbringen.

Welche Maßnahmen sind erforderlich?

Bei der Einführung eines Schwachstellenmanagements sollten Unternehmen und Institutionen verschiedene Schritte unternehmen, um eine effektive Sicherheitsstrategie zu entwickeln. Zunächst ist eine **Analyse der aktuellen IT-Sicherheitslage** erforderlich, um bestehende Schwachstellen und Sicherheitslücken im System zu ermitteln. Anschließend sollte eine **Schwachstellenmanagement-Strategie** entwickelt werden, die Ziele, Prioritäten und verantwortliche Personen für die Umsetzung der Maßnahmen festlegt.

Weltweit werden öffentlich bekannte Schwachstellen nach dem **Common Vulnerabilities and Exposures (CVE) Modell** gemeldet und können von IT-Verantwortlichen täglich abgerufen werden. Ziel sollte es sein, alle täglich neuen bekannten Schwachstellen zu betrachten, auf Relevanz hin zu prüfen und nach Bedarf zu behandeln. Schwachstellen werden im CVE einer **Risikobewertung** nach Kritikalität unterzogen. Ferner sollten für komplexe Schwachstellen dedizierte **Risikoanalysen** bzgl. deren Auswirkung auf die Informationssicherheit durchgeführt werden.

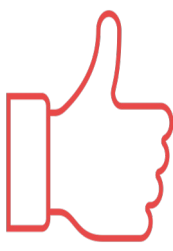
Der übliche Weg zu Behandlung einer Schwachstelle ist die **Installation von Sicherheitspatches** und -updates, um IT-Systeme auf dem neuesten Stand zu halten. Die Verantwortlichkeit für den **Patchmanagementprozess** sollte in Unternehmen formal geregelt sein. Ferner sollten **automatisierte Systeme** zum Einspielen von Patches und Updates genutzt werden.

Um ein effektives Schwachstellenmanagement zu gewährleisten, ist daher die **Auswahl geeigneter Tools und Technologien** entscheidend. Diese sollten Systeme zur Überwachung, Identifizierung und Behebung von Schwachstellen beinhalten. Des Weiteren ist es wichtig, **Mitarbeiter zu schulen** und für IT-Sicherheitsrisiken zu sensibilisieren. Hierbei sollten Wissen und Fähigkeiten im Umgang mit diesen Risiken vermittelt werden.



ACTION

Welche Chancen gibt es?



Ein effektives Schwachstellenmanagement bringt Unternehmen und Institutionen zahlreiche Vorteile. Dazu gehört die **erhöhte IT-Sicherheit**, die durch die Reduzierung von Sicherheitsrisiken erreicht wird. Dies geschieht durch die frühzeitige Identifizierung und Behebung von Schwachstellen.


Die Einhaltung branchenspezifischer und gesetzlicher Anforderungen trägt dazu bei, **Haftungsrisiken zu minimieren** und hilft somit zur Compliance des Unternehmens beizutragen. Darüber hinaus schützt ein effektives Schwachstellenmanagement **sensible Daten**, indem es unbefugten Zugriff auf vertrauliche Informationen verhindert und vor Datenverlusten bewahrt.

Unternehmen profitieren auch von **Kosteneinsparungen**, indem teure Sicherheitsvorfälle und Datenverluste durch proaktive Maßnahmen und kontinuierliche Überwachung vermieden werden. Zudem ermöglicht das Schwachstellenmanagement eine **effizientere Ressourcennutzung**, indem Schwachstellen priorisiert und Ressourcen gezielt zur Behebung kritischer Sicherheitslücken eingesetzt werden.

Welche Risiken gibt es?

Obwohl das Schwachstellenmanagement viele Vorteile bietet, gibt es auch einige Risiken und Nachteile, die beachtet werden müssen. Ein wichtiger Aspekt ist die **fehlende Garantie**, dass alle Schwachstellen bekannt sind. Sogenannte **Zero-Day-Exploits** sind Angriffe, die auf solche nicht öffentlich bekannten Schwachstellen abzielen. Daher ist es trotz umfassender Maßnahmen nicht möglich, alle Schwachstellen zu identifizieren.

Darüber hinaus erfordert ein effektives Schwachstellenmanagement erhebliche **finanzielle und personelle Ressourcen**, was für kleinere Unternehmen und Institutionen möglicherweise schwer erreichbar ist. Ein weiteres Problem stellt die **subjektive Bewertung und Priorisierung** von Schwachstellen dar. Dies kann dazu führen, dass Sicherheitslücken übersehen werden, während andere möglicherweise zu viel Aufmerksamkeit erhalten.



Fazit

Schwachstellenmanagement ist ein entscheidender Aspekt der IT-Sicherheit für Unternehmen und Institutionen, der hilft, potenzielle Bedrohungen **frühzeitig zu erkennen** und zu beheben.

Die erfolgreiche Einführung eines Schwachstellenmanagements erfordert jedoch eine **sorgfältige Planung**, die Bereitstellung von **Ressourcen** und eine **kontinuierliche Anpassung** an die sich ständig ändernde Bedrohungslandschaft. Unternehmen und Institutionen müssen sich dieser Herausforderungen bewusst sein und einen ganzheitlichen Ansatz verfolgen, um ihre IT-Sicherheit langfristig zu gewährleisten.