

# Vulnerability-Management

## Wozu IT-Sicherheit?

Täglich werden neue Schwachstellen in Softwareprodukten und Diensten entdeckt, welche dann unter Umständen auch von Angreifern verwendet werden, um Zugriff auf sensible Daten zu erhalten oder durch den Ausfall von Dienstleistungen eine Organisation zu schädigen. Durch solche Sicherheitsvorfälle können hohe Kosten entstehen, wenn dadurch Maschinenstillstände oder Datenverluste den Geschäftsbetrieb stören. Es zeigt sich dabei, dass neu entdeckte Schwachstellen in immer kürzerer Zeit für Angriffe mittels Malware wie Viren, Würmer etc. verwendet werden. Dabei gilt zu bedenken, dass der grösste Anteil von erfolgreichen Angriffen auf bekannte Schwachstellen, für welche meist schon Lösungen zur Behebung bereitstehen, durchgeführt werden.

Zudem fordern auch immer öfter Gesetze und Richtlinien, wie die IT-Infrastruktur zu schützen sei und welche Folgen bei deren Nichterfüllung z. B. betreffend Haftungsfragen entstehen können. Es liegt also im Interesse der Geschäftsführung, die IT-Sicherheit und deren Risiken auf ein dem Geschäftsfeld angepassten Niveau zu bringen und zu halten. Ein Risiko ist dabei aus betriebswirtschaftlicher Sicht eine nach Häufigkeit und Auswirkung bewertete Bedrohung, welche ein zielorientiertes System negativ beeinflussen kann. In der IT-Sicherheit gelten dabei die Störung der Prinzipien der Integrität, Vertraulichkeit und Verfügbarkeit der Informationen und Systeme als Risiken. Der folgende Artikel soll aufzeigen, wie mittels Vulnerability bzw. Schwachstellen-Management die IT-Sicherheit gezielt erhöht und gemessen werden kann.

## Definition Vulnerability-Management

Vulnerability-Management gehört zu den präventiven Sicherheitsmassnahmen, welches grundsätzlich die Identifizierung, Priorisierung und Behebung von Schwachstellen beinhaltet. Eine Priorisierung und Einordnung der IT-Infrastrukturen nach Relevanz ist für die Unternehmung angesichts der grossen Anzahl von Sicherheitsproblemen notwendig, um gezielt die grössten Sicherheitsrisiken effizient eliminieren zu können. Dabei genügt das reine Patchen der betroffenen IT-Infrastruktur nicht, da zusätzlich auch Schwachstellen durch Konfigurationsfehler, mangelndes Sicherheitsbewusstsein der Mitarbeiter oder falscher oder nicht vorhandener Sicherheitsrichtlinien entstehen. Um allen diesen Bedrohungen vorbeugend entgegenwirken zu können, muss eine Organisation einen Gesamtüberblick über die Verwundbarkeiten der IT-Infrastruktur haben. Nur durch den Aufbau eines Vulnerability-Management-Prozesses zur Gewährleistung der IT-Sicherheit können Schwachstellen effizienter und gezielter behandelt werden und ein Überblick über den effektiven Sicherheitsstatus der Organisation erstellt werden. Detektive Sicherheitsmassnahmen (z. B. Virens Scanner, IDS-Systeme etc.) und korrektive Sicherheitsmassnahmen (z. B. Recovery und Wiederanlauf) werden dabei nicht behandelt.

Als die wesentlichsten Punkte des Vulnerability-Management-Prozesses gelten dabei folgende Phasen:

- Inventarisierung der vorhandenen IT-Ressourcen
- Identifizieren von Schwachstellen in den vorhandenen IT-Ressourcen
- Priorisierung der Schwachstellenbehebung
- Behebung der Schwachstellen nach Relevanz
- Prüfung der durchgeführten Massnahmen

Dabei darf es sich nicht um eine einmalig durchgeführte Aufgabe handeln, da diese lediglich eine Momentaufnahme zeigen würde. Der Vulnerability-Management-Prozess kann z. B. quartalsweise vorgenommen werden, je nach Schutzbedarf der Organisation kann der Zyklus durchaus sogar wöchentlich durchgeführt werden.

Die einzelnen Schritte von der Vorbereitung bis zur Implementation und Kontrolle eines Vulnerability-Management-Prozesses werden anschliessend kurz erläutert.

## Standardisieren der IT-Konfigurationen

Damit ein Vulnerability-Management-Prozess effektiv implementiert werden kann, sollte der Einsatz von standardisierten IT-Konfigurationen in Betracht gezogen werden. Eine typische Standardkonfiguration beinhaltet meist folgende Komponenten:

- Hardware (Typ und Model)
- Betriebssystem (Version und Patch-Level)
- Installierte (Haupt-)Anwendungen mit Version und Patch-Level
- Spezielle (sicherheitsrelevante) Einstellungen betreffend Betriebssystem und Anwendungen

Dadurch können notwendige Tests betreffend den Auswirkungen von Patches oder Konfigurationsänderungen auf wenigen Referenzsystemen durchgeführt werden.

## Erstellen einer Patch- und Vulnerability-Gruppe

Die Hauptaufgaben dieser Gruppe beinhalten die Inventarisierung der IT-Ressourcen, das Identifizieren, Priorisieren und Beheben der Schwachstellen und deren Überprüfung. Als Mitglieder kommen Personen mit Kenntnissen von unterschiedlichen Sicherheits- oder Administrationsbereichen in Frage. Die Anzahl der Gruppenmitglieder ist Abhängig von der Organisationsgrösse, deren Budget und der Komplexität des Netzwerkes. Die Kernpunkte der Gruppe für die Umsetzung des Vulnerability-Management-Prozesses werden in den folgenden Schritten detailliert erläutert.

### Schritt 1: Inventarisierung der vorhandenen IT-Ressourcen

Die Inventarisierung sämtlicher IT-Ressourcen (Hardware, OS, Applikationen) kann grösstenteils automatisch mit entsprechender Software durchgeführt werden, wobei einzelne Daten (z. B. Standort) dennoch manuell erfasst werden müssen. Welche Details erfasst werden müssen, ist von der jeweiligen Organisation und der Verwendung dieser Informationen betreffend Vulnerability-Management abhängig. Generell sind folgende Eigenschaften möglich, aber nicht immer notwendig:

- System Name
- System Administrator
- Standort
- Verwendeter Netzwerkport
- Software-Konfiguration (OS, Version, Applikationen, Netzwerkdienste, IP-Adresse (falls statisch))
- Hardware-Konfiguration (CPU, Speicher, Harddisk, Netzwerk-Karten, WLAN, IO-Devices (z. B. USB), Firmware-Versionen)

Anschliessend sollte eine erste Priorisierung der IT-Ressourcen durchgeführt werden. Dadurch können den Systemen gezielter Risiken zugewiesen werden und müssen dann priorisiert beobachtet werden. Eine Gruppierung kann mittels folgender System-Eigenschaften durchgeführt werden:

- Notwendigkeit der Ressource für den regulären Geschäftsbetrieb (z. B. Server)
- Relevanz für Sicherheits-Management
- Verwendung an Netzwerkgrenze/Netzwerkübergang
- Relevanz der enthaltenen Informationen
- Erreichbarkeit von externen Benutzern relevant

Zudem muss definiert werden, für welche IT-Systeme die Gruppe zuständig ist und welche von den jeweiligen lokalen Administratoren selber verwaltet und überprüft werden müssen.

## **Schritt 2. Identifizieren von Schwachstellen**

Für die zugeteilten IT-Ressourcen müssen nun mögliche Schwachstellen identifiziert werden. Für diese Aufgaben eignen sich besonders Vulnerability-Scanner, welche ein Automatisieren dieser Aufgabe ermöglichen. Zudem sollten weitere Ressourcen mit sicherheitsrelevanten Informationen regelmässig beobachtet werden, z. B. Webseiten von Herstellern, Schwachstellen-Datenbanken und sicherheitsrelevante Mailing-Listen etc.

## **Schritt 3. Priorisierung der Schwachstellenbehebung**

Mittels Risikoanalyse sollte die Priorisierung der Schwachstellenbehebung durchgeführt werden. Dabei muss die Wichtigkeit der Ressource für den Betrieb der Organisation berücksichtigt werden. Zudem sollte bei der Priorisierung ein möglicher Image-Verlust oder Produktionsausfall durch Datendiebstahl oder Systemausfall integriert werden.

Eine einfache Bestimmung des Risikos pro IT-Ressource kann z.B. mittels folgender Formel durchgeführt werden:

$$\text{Gesamtrisiko} = \text{Bedrohung} \times \text{Schwachstelle} \times \text{Wert}$$

Dabei wird für jeden Faktor der Wert 1-5 (sehr klein bis sehr hoch) gemäss Einschätzung eingesetzt. Betreffend Bedrohung bezieht sich der Faktor auf die Auswirkungen von Integrität, Verfügbarkeit oder Vertraulichkeit der IT-Ressource. Je höher das Produkt ist (max. 125), desto höher muss die Priorität in der Schwachstellenbehebung gesetzt werden. Ebenfalls ist aus der Formel zu sehen, dass Bedrohungen erst zu Risiken werden, wenn sie auf Schwachstellen treffen. Diese müssen deshalb unternehmensintern bekämpft werden, um das Risiko zu vermindern, da Bedrohungen fast nicht verhindert werden können. Mittels erweiterter qualitativer- oder (semi-) quantitativer Ansätze zur Risikoanalyse können noch exaktere Ergebnisse erzielt werden.

## **Schritt 4. Testen der Schwachstellenbehebung**

Durch den Einsatz von standardisierten IT-Konfigurationen können die Auswirkungen der Behebung der Schwachstelle z. B. mittels Patch bzw. dessen unterlassen sowie Änderungen an der Konfiguration getestet werden. Dies gilt nur für die von der Gruppe unterstützten IT-Systeme, die weiteren müssen von den lokalen Administratoren selber vorher auf mögliche Systemänderungen geprüft werden.

Damit die Integrität und Sicherheit der Patches gewährleistet ist, sollten gewisse Massnahmen vor der Installation durchgeführt werden:

- Prüfung der Integrität mittels Checksumme (z. B. MD5, SHA-1)
- Prüfung mittels Virens Scanner
- Anwenden der Patches bzw. Konfigurationsänderungen auf Testsystem
- Prüfung auf Abhängigkeiten mit bestehenden Patches / Konfigurationen
- Das Testsystem sollte die exakte Konfiguration wie das produktive System aufweisen
- Eventuell auf Erfahrungen anderer Anwender zurückgreifen
- Testen der Deinstallation des Patches

Bei grösseren Organisationen empfiehlt es sich, eine Datenbank mit Information sowie den entsprechenden Patches zur Schwachstellenbehebung zu betreiben, welche weitere Details zur Schwachstellenbehebung enthalten können. Durch das zusätzliche Verwalten der Patches kann beim Ausfall des Internetzuganges oder Problemen beim Patch-Anbieter dennoch die Behebung der Schwachstellen durchgeführt werden. Einige Vulnerability-Management-Lösungen bieten solche Datenbanken im Funktionsumfang an.

### **Schritt 5. Durchführung der Schwachstellen-Behebung**

Nach erfolgreichem Testen sollte die Schwachstellen-Behebung durchgeführt werden. Anhand der durchgeführten Tests können nun folgende Varianten für die Behebung der Schwachstelle umgesetzt werden:

- Installation des Patches
- Durchführung von Konfigurationsänderungen
- Entfernen der betroffenen Software

Primär kann die automatische Installation der Patches mittels Patch-Management Software durchgeführt werden. Falls dies nicht möglich sein sollte, ist der Kontakt mit lokalen Administratoren notwendig, um diesen Informationen zur Behebung der Schwachstelle zu unterbreiten. Es gilt auch zu berücksichtigen, dass viele Anwendungen die Möglichkeit bieten, selbstständig Prüfungen auf Upgrades bzw. Patches durchzuführen. Durch nutzen dieser Mechanismen kann der Aufwand zur Identifizierung, Verteilen und installieren der Patches reduziert werden.

Anschliessend sollte die Schwachstellen-Behebung auch bei denjenigen Systemen, welche aktuell nicht zur höchsten Risikogruppe gehören, durchgeführt werden. Dies ist notwendig, da das spätere Aktivieren eines eventuellen betroffenen Dienstes plötzlich zu einem Risiko werden kann.

Falls die Durchführung der Schwachstellen-Behebung nicht sofort durchgeführt werden soll oder kann, gilt folgendes zu Bedenken:

- Welchem Risiko ist die Ressource ausgesetzt (z. B. öffentlich erreichbar wie Webserver)
- Wahrscheinlichkeit einer Ausnutzung der Schwachstelle
- Konsequenzen einer möglichen Schwachstellen-Ausnutzung (Einfluss auf Verfügbarkeit / Vertraulichkeit)

Welches die richtige Entscheidung ist, muss im Kontext der Organisation und mittels Absprache mit dem Management bzw. Administratoren erörtert werden.

### **Schritt 6. Überprüfung der Schwachstellen-Behebung**

Die Überprüfung der Umgesetzten Massnahmen ist der nächste Schritt der Schwachstellen-Management-Gruppe. Dazu stehen mehrere Möglichkeiten zur Verfügung:

- Prüfung der betroffenen Systeme mittels Vulnerability-Scanner
- Durchsicht der Patch-Logdateien auf korrekte Installation
- Durchführung eines Penetrationstest (durch interne- oder externe Spezialisten)

Die erhaltenen Informationen können nun einen aktuellen Zustand der Sicherheit der IT-Infrastrukturen aufzeigen und belegen.

### **Prüfung des Vulnerability-Management-Prozesses**

Um die Effektivität des Vulnerability-Management-Prozesses zu messen, stehen generell folgende drei Ansätze zur Verfügung:

- Anfälligkeit für Attacken
- Reaktionszeit
- Kosten

Dabei weist jede Messmethode mehrere Messansätze mit unterschiedlichen Stärken und Schwächen auf. Eine Gegenüberstellung der Methoden zeigt die wesentlichen Merkmale und Ansätze zur Messung und Prüfung der Effektivität des Vulnerability-Managements auf.

Messmethode	Ansätze zur Messung
Anfälligkeit für Attacken	<p>Um die Anfälligkeit für Attacken messen zu können, stehen drei unterschiedliche Ansätze zur Verfügung:</p> <ul style="list-style-type: none"> <li>• Anzahl installierter Patches (z. B. mittels Patch-Management-Software)</li> <li>• Anzahl vorhandener Schwachstellen (z. B. mittels Vulnerability-Scanner)</li> <li>• Anzahl vorhandener Netzwerk-Dienste (z. B. Anzahl Webserver als potentielles Risiko)</li> </ul>
Reaktionszeit	<p>Gemessen wird die Zeit von der Identifizierung, Klassifizierung und Reaktion auf die Schwachstelle. Diese Messung ist besonders interessant, da die Zeit zwischen der Entdeckung einer Schwachstelle bis zu deren Ausnutzung immer kürzer wird.</p> <p>Zur Messung der Reaktionszeit stehen drei Varianten zur Verfügung:</p> <ul style="list-style-type: none"> <li>• Reaktionszeit für die Schwachstellen- oder Patch-Identifikation</li> <li>• Reaktionszeit für das Patchen aller relevanten IT-Systeme (enthält Analyse, Testen, Behebung der Schwachstellen mittels Patch)</li> <li>• Reaktionszeit für Konfigurationsänderung (Schwachstellenbehebung ohne Patch, z. B. durch Änderung der Firewall- /Router- oder Dienstkonfiguration)</li> </ul>
Kosten	<p>Die Messung des Vulnerability-Managements mittels verursachter Kosten stellt vier Hauptgruppen zur Verfügung:</p> <ul style="list-style-type: none"> <li>• Kosten der Patch- und Schwachstellen-Gruppe (Kosten der Personen der Gruppe, inkl. Kosten für ev. ausgelagerte Dienste. Berücksichtigen der Einsparungen durch Zentralisierung)</li> <li>• Kosten des/der verwendeten Enterprise-Patch- und Schwachstellen-Management-Tools (beinhaltet Patch-Programme, Vulnerability-Scanner und Datenbanken, IDS und LOG-Analyse etc.)</li> <li>• Höhe der trotzdem entstandenen Kosten (d. h. Kosten welche bei besserer Effizienz der Vulnerability-Managements gespart werden könnten. Beinhaltet z. B. verlorene Arbeitszeit durch den Angriff, Datenverlust, Wert an Imageverlust etc.)</li> </ul>

## Fazit

Die Umsetzung eines Vulnerability-Management-Prozesses besteht aus unterschiedlichen Teilschritten, welche sich nicht nur auf die technische Behebung einer Schwachstelle mittels Patch beziehen, sondern einen umfassenden Prozess darstellt, der auch die Risikoanalyse sowie das Management beinhaltet. Dabei müssen Schwachstellen im jeweiligen Kontext betrachtet und priorisiert werden, um gezielt die relevanten IT-Systeme schützen zu können. Mittels Vulnerability-Management ist ein wirksamer Schutz gegen bekannte Schwachstellen möglich, da jedoch auf eventuelle Zero-Day-Exploits oder andere unvorhergesehene Ereignisse keine Vorbereitung möglich ist, muss zusätzlich ein funktionierender Notfall-Plan vorhanden sein.