Richtlinien für die Verwaltung von Sicherheitslücken und Patches

Vorlage

# Verwendung dieses Dokuments

* Diese Richtlinie wurde so verfasst, dass das Dokument für die 3 verschiedenen CyFun Sicherungsstufen verwendet werden kann (**Grundlegend**, **Wichtig**, **Wesentlich**).
* Die Erfordernisse, die zur Erreichung einer bestimmten Sicherheitsstufe erforderlich sind, werden durch die Angabe des vorgeschlagenen Textes in der oben genannten Farbe deutlich gemacht.

Inhalt

[Verwendung dieses Dokuments 2](#_Toc157679160)

[Behörde und Überprüfung 3](#_Toc157679161)

[Dokumentenkontrolle und -prüfung 3](#_Toc157679162)

[Versionsverwaltung 3](#_Toc157679163)

[Intro 4](#_Toc157679164)

[Verwaltung von Schwachstellen 4](#_Toc157679165)

[Risikobewertung 4](#_Toc157679166)

[Scannen nach internen Schwachstellen 4](#_Toc157679167)

[Scannen nach externen Sicherheitslücken 4](#_Toc157679168)

[IDS/IPS 5](#_Toc157679169)

[Richtlinie für die koordinierte Offenlegung von Schwachstellen (CVDP) (wichtig, wesentlich) 5](#_Toc157679170)

[Patch-Verwaltung 5](#_Toc157679171)

# Autorität und Überprüfung

## Dokumentenkontrolle und -prüfung

|  |  |
| --- | --- |
| **Dokumentenprüfung** |  |
| Autor |  |
| Eigentümer |  |
| Datum der Erstellung |  |
| Zuletzt überarbeitet von |  |
| Datum der letzten Überarbeitung |  |

## Versionsverwaltung

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Datum der Genehmigung** | **Genehmigt durch** | **Beschreibung der Änderung** |
| 1.0 |  |  |  |

# Intro

Eine Schwachstelle ist ein Fehler oder eine Schwäche, ein Entwurfs- oder Implementierungsfehler, oder auch ein Mangel an Aktualisierungen in Anbetracht des aktuellen technischen Wissens, der die Sicherheit von Informationstechnologien beeinträchtigen kann. Eine Schwachstelle kann zu einem unerwarteten oder unerwünschten Ereignis führen und von böswilligen Dritten ausgenutzt werden, um die Integrität, Authentizität, Vertraulichkeit oder Verfügbarkeit eines Systems zu verletzen oder ein System zu schädigen. Mehr als 90 % der Malware-Infektionen oder Cyberkriminalität beginnen mit der Ausnutzung einer bekannten Schwachstelle. Insbesondere Systeme, die eingehende Verbindungen zum Internet zulassen, wie Webserver und E-Mail-Server, sind täglich zahlreichen Angriffen ausgesetzt.

Daher ist es von entscheidender Bedeutung, dass wir so viele bekannte Schwachstellen wie möglich beseitigen. Dazu brauchen wir ein gutes Patch-Management-System und eine Überwachung der Schwachstellen.

Dieses Strategiedokument ist Teil einer Reihe von Strategiedokumenten, die **[Organisation]** bei der Entwicklung einer soliden Cybersicherheitsstrategie **unterstützen**.

# Verwaltung von Schwachstellen

## Risikobewertung

**[Organisation]** führt jährlich eine Risikobewertung durch, bei der das Risiko auf Grundlage von Bedrohungen, Schwachstellen und Auswirkungen auf Geschäftsprozesse und Vermögenswerte ermittelt wird. Diese Schwachstellen beziehen sich auf eine Schwachstelle in der Hardware, Software oder den Verfahren von **[Organisation]**.

## Scannen nach internen Schwachstellen

Kritische und vertrauliche Systeme sollten mindestens **jährlich**, **vierteljährlich** oder **kontinuierlich** auf Schwachstellen gescannt werden. Sehr kritische und sehr vertrauliche Systeme sollten mindestens monatlich gescannt werden.

Zur Untersuchung der Schwachstellen von Systemen können Schwachstellen-Scan-Tools oder Pen-tests eingesetzt werden. Diese Tools enthalten eine Datenbank mit bekannten Schwachstellen und können ein einzelnes System oder sogar ein ganzes Netzwerk auf Schwachstellen untersuchen. Scanning-Tools scannen nur die Schwachstellen, auf die sie Zugriff haben. Wenn beispielsweise Dienste durch Firewalls blockiert sind, können sie nicht dort keine Schwachstellen erkennen.

Die Werkzeuge teilen die Schwachstellen in verschiedene Risikostufen ein. Beachten Sie jedoch, dass das höchste Risiko besteht, wenn die Schwachstelle über das Internet ausgenutzt werden kann. Ist dies nicht der Fall, stellt sie dennoch ein Risiko dar, da sie von einem infizierten System zur Verbreitung von Malware auf andere Rechner im Netzwerk genutzt werden kann, allerdings ist die Wahrscheinlichkeit geringer.

## Scannen nach externen Sicherheitslücken

Zusätzlich zum internen Scan sollte ein externer Schwachstellen-Scan (Pen-Test) **jährlich, vierteljährlich**, oder **kontinuierlich durchgeführt werden**. Die Ergebnisse dieses externen Pen-Tests sollten die Grundlage für einen jährlichen, halbjährlichen oder monatlichen Plan zur Verbesserung der Schwachstellen bilden und auch als unabhängiges Maß für die Systemsicherheit dienen.

## IDS/IPS

Während Schwachstellen-Scanner zur Erkennung potenzieller Risiken eingesetzt werden, bieten Systeme zur Erkennung von Eindringlingen (*Intrusion Detection System* - IDS) und zur Verhinderung von Eindringlingen (*Intrusion Detection System* - IPS) eine Echtzeit-Überwachung des Netzes, um festzustellen, ob böswillige Aktionen stattfinden. IDS-Systeme können eine Warnung senden, sobald ein verdächtiges Verhalten festgestellt wird. IPS können sogar Maßnahmen ergreifen, indem sie zum Beispiel den Datenverkehr in der Firewall blockieren.

IDS/IPS sollten für kritische und vertrauliche Systeme in Betracht gezogen werden, wenn das Risiko die Kosten überwiegt.

## Richtlinie für die koordinierte Offenlegung von Schwachstellen (CVDP) (wichtig, wesentlich)

Organisationen, die die CyFun-Sicherheitsstufe **Wichtig** oder **Wesentlich** anstreben, sollten eine koordinierte Politik zur Offenlegung von Schwachstellen einführen.

Dabei handelt es sich um eine Reihe von Regeln, die von der **[Organisation]**, die für die Informationssysteme verantwortlich ist, festgelegt wurden und die es Teilnehmern (oder "ethischen Hackern") mit guten Absichten ermöglichen, potentielle Schwachstellen in ihren Systemen aufzuspüren oder ihr alle relevanten Informationen darüber zu liefern. Diese Regeln, die normalerweise auf einer Website veröffentlicht werden, ermöglichen die Schaffung eines rechtlichen Rahmens für die Zusammenarbeit zwischen der verantwortlichen Organisation und den Teilnehmern der Politik. Diese Regeln sollten unter anderem die Vertraulichkeit der ausgetauschten Informationen gewährleisten und die Offenlegung von entdeckten Schwachstellen auf verantwortungsvolle und koordinierte Weise regeln.

Bitte beziehen Sie sich bei der Erstellung dieses CVDP auf den vom Zentrum für Cybersicherheit Belgien erstellten Leitfaden über die koordinierte Politik zur Offenlegung von Schwachstellen.

[\*https://nl.wikipedia.org/wiki/Penetratietest](https://nl.wikipedia.org/wiki/Penetratietest)

# Patch-Verwaltung

Alle verwalteten Server, Firewalls, Switches und Clients sollten mindestens alle zwei Monate mit den neuesten relevanten Patches aktualisiert werden, sofern nicht ausdrücklich etwas anderes beschlossen wurde.

Sicherheits-Patches sollten so bald wie möglich installiert werden. Dies kann nur nach einer gründlichen Analyse der Auswirkungen des zu installierenden Patches auf die Umgebung geschehen.

Es muss ein System oder ein Prozess vorhanden sein, um zu wissen, welche Sicherheits-Patches verfügbar und anwendbar sind.

Zu den Sicherheitspatches gehören solche für Betriebssysteme, Serversoftware wie Datenbanken und Dienste sowie Anwendungen.

**HINWEIS:** Wenn ein System nicht in der Lage ist, Sicherheits-Patches anzuwenden, obwohl die Schwachstellen bekannt sind, sollte das System vom Internet und anderen mit dem Internet verbundenen Systemen isoliert und physisch gesichert werden.