Beleid rond vulnerabiliy- en Patchmanagement

 Sjabloon

# Dit document gebruiken

* Dit beleid werd zo opgesteld dat het document kan gebruikt worden voor de 3 verschillende **CyFun** zekerheidsniveaus. (**Basis**, **Belangrijk**, **Essentieel**)
* De noden die nodig zijn om te voldoen aan een bepaald zekerheidsniveau zal duidelijk gemaakt worden door de voorgestelde tekst aan te duiden in de kleur zoals hierboven vermeld..

Inhoud

[Dit document gebruiken 2](#_Toc157679160)

[Autoriteit en herziening 3](#_Toc157679161)

[Documentcontrole en beoordeling 3](#_Toc157679162)

[Versiebeheer 3](#_Toc157679163)

[Intro 4](#_Toc157679164)

[Beheer van kwetsbaarheden 4](#_Toc157679165)

[Risicobeoordeling 4](#_Toc157679166)

[Scannen op interne kwetsbaarheden 4](#_Toc157679167)

[Scannen op externe kwetsbaarheden 4](#_Toc157679168)

[IDS/IPS 5](#_Toc157679169)

[Beleid voor de Gecoördineerde bekenmaking van kwetsbaarheden CVDP (Belangrijk, Essentieel) 5](#_Toc157679170)

[Patchbeheer 5](#_Toc157679171)

# Autoriteit en herziening

## Documentcontrole en beoordeling

|  |  |
| --- | --- |
| **Documentcontrole**  |  |
| Auteur  |  |
| Eigenaar |  |
| Datum aangemaakt |  |
| Laatst herzien door  |  |
| Laatste herzieningsdatum |  |

.

## Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie**  | **Datum van goedkeuring** | **Goedgekeurd door**  | **Beschrijving van verandering** |
|  |  |  |  |

# Intro

Een kwetsbaarheid is een gebrek of een zwakke plek, een ontwerp- of uitvoeringsfout, het ontbreken van updates in het licht van de bestaande technische kennis, die de veiligheid van informatietechnologieën in het gedrang kan brengen. Een kwetsbaarheid kan leiden tot een onverwacht of ongewenst voorval en uitgebuit worden door kwaadwillige derden om de integriteit, authenticiteit, vertrouwelijkheid of beschikbaarheid van een systeem te schenden of om een systeem schade toe te brengen. Meer dan 90% van de malware-infecties of cybercriminaliteit begint met het uitbuiten van een bekend lek. Vooral systemen die inkomende verbindingen met het internet toestaan, zoals webservers en e-mailservers, worden dagelijks geconfronteerd met talloze aanvallen.

Daarom is het van groot belang dat we zoveel mogelijk bekende kwetsbaarheden elimineren. Hiervoor hebben we een goed patchbeheersysteem en kwetsbaarhedenbewaking nodig.

Dit beleidsdocument maakt deel uit van een set van beleidsdocumenten die **[Organisatie]** ondersteunen bij het opstellen van een gedegen strategie rond cyberbeveiliging.

# Beheer van kwetsbaarheden

## Risicobeoordeling

**[Organisatie]** voert een jaarlijkse risicobeoordelingen uit waarbij het risico wordt bepaald aan de hand van bedreigingen, kwetsbaarheden en gevolgen voor bedrijfsprocessen en activa. Deze kwetsbaarheden verwijzen naar een zwakke plek in de hardware, software of procedures van **[Organisatie].**

## Scannen op interne kwetsbaarheden

Kritieke en vertrouwelijke systemen moeten minstens **jaarlijks** ,**per kwartaal**, **continue scanning** worden gescand op kwetsbaarheden. Zeer kritieke en zeer vertrouwelijke systemen moeten minstens elke maand worden gescand.
Tools voor het scannen op kwetsbaarheden of \*penetratietesten kunnen worden gebruikt om de zwakke plekken van systemen te onderzoeken. Deze tools bevatten een database met bekende kwetsbaarheden en kunnen een enkel systeem of zelfs een heel netwerk scannen op kwetsbare systemen. Scanning tools scannen alleen kwetsbaarheden waartoe ze toegang hebben. Als services bijvoorbeeld worden geblokkeerd door firewalls, kan het daar geen verslag over uitbrengen.

De tools delen zwakke punten in verschillende risiconiveaus in. Wees je er echter van bewust dat het hoogste risico is wanneer de zwakke plek kan worden uitgebuit vanaf het internet. Als dit niet het geval is, is het nog steeds een risico, omdat het door een geïnfecteerd systeem kan worden gebruikt om malware te verspreiden naar andere machines in het netwerk, maar de kans is kleiner.

## Scannen op externe kwetsbaarheden

Naast de interne scan moet er **jaarlijks** **,per kwartaal**, **continue scanning** een externe kwetsbaarheidsscan worden uitgevoerd (pentest). De resultaten van deze externe pentest moeten de basis vormen voor een jaarlijks, 6-maandelijks, maandelijks plan om de kwetsbaarheden te verbeteren en dienen tevens als onafhankelijke maatstaf voor de beveiliging van het systeem.

## IDS/IPS

Terwijl kwetsbaarhedenscanners worden gebruikt om potentiële risico's op te sporen, zorgen IDS (intrusion detection) en IPS (intrusion prevention) systemen voor realtime netwerkbewaking om te zien of er kwaadaardige acties plaatsvinden. IDS-systemen kunnen een waarschuwing versturen op het moment dat verdacht gedrag wordt opgemerkt. IPS kan zelfs actie ondernemen, bijvoorbeeld door verkeer in de firewall te blokkeren.

 IDS/IPS moet worden overwogen voor kritieke en vertrouwelijke systemen, als het risico opweegt tegen de kosten.

## Beleid voor de Gecoördineerde bekenmaking van kwetsbaarheden CVDP (Belangrijk, Essentieel)

Organisaties die het CyFun zekerheidsniveau **Belangrijk** of **Essentieel** nastreven dienen een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden op te stellen.

Dit is een geheel van regels die vooraf zijn bepaald door [Organisatie] die verantwoordelijk is voor informatiesystemen waardoor deelnemers (of “ethische hackers”), met goede bedoelingen, mogelijke kwetsbaarheden in haar systemen kunnen opsporen, of haar alle relevante informatie hierover kunnen bezorgen. Deze regels, doorgaans openbaar gemaakt op een website, maken het mogelijk een juridisch kader te bepalen voor de samenwerking tussen de verantwoordelijke organisatie en de beleidsdeelnemers. Deze regels moeten onder meer de vertrouwelijkheid van de uitgewisselde informatie garanderen en een eventuele bekendmaking van de ontdekte kwetsbaarheden op een verantwoorde en gecoördineerde manier omkaderen.

Raadpleeg de Gids over het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden, opgesteld door het Centrum voor Cybersecurity België bij het opstellen van deze CVDP.

\*<https://nl.wikipedia.org/wiki/Penetratietest>

# Patchbeheer

Alle beheerde servers, firewalls, switchen en clients moeten ten minste elke 2 maanden worden voorzien van de nieuwste relevante patches, tenzij expliciet anders is besloten.

Beveiligingspatches moeten zo snel mogelijk geïnstalleerd worden. Dit kan enkel na een grondige impact analyse op de omgeving van de te installeren patch.

Er moet een systeem of proces zijn om te weten welke beveiligingspatches beschikbaar en toepasbaar zijn.

Beveiligingspatches omvatten die van besturingssystemen, serversoftware zoals databases en services en toepassingen.

**OPMERKING:** Als een systeem niet in staat is om beveiligingspatches toe te passen, ook al zijn kwetsbaarheden bekend, moet het systeem worden geïsoleerd van het internet en andere systemen die met het internet verbonden zijn en moet het fysiek worden beveiligd.