Verbeter je kwetsbaarhedenbeheer

Aan de slag met een cyclisch proces voor jouw organisatie

Inleiding

Deze publicatie biedt praktische handvatten om cyclisch kwetsbaarhedenbeheer (vulnerability management) binnen jouw organsatie uit te voeren. Kwetsbaarheden bieden een ingang voor cyberaanvallen die jouw organisatie financiële schade en reputatieverlies kunnen bezorgen. Deze publicatie biedt praktische handvatten hoe je met kwetsbaarhedenbeheer ervoor zorgt dat je aanvallers buiten de deur houdt.

Doelgroep

Kwetsbaarhedenbeheer is relevant voor IT-professionals en besluitvormers die hun digitale weerbaarheid willen vergroten door middel van het opstarten van cyclisch kwetsbaarhedenbeheer. Deze publicatie richt zich onder andere op organisaties die onder de NIS2-richtlijn vallen.

Leeswijzer

Deze publicatie is opgedeeld in 7 delen. Bij de 5 inhoudelijke fasen van kwetsbaarhedenbeheer zijn praktische voorbeelden opgenomen in het ‘casus’ kader. Hierin wordt een voorbeeld gegeven van de methode of het geeft inzicht in het nut. In het laatste hoofdstuk zijn een enkele praktische tips opgenomen. Daarnaast wordt bij elke stap aandacht geschonken aan het zelf uitvoeren van de fase of het uitbesteden van het werk aan een externe derde partij.

Inhoud

Achtergrond

Kwetsbaarhedenbeheer is een cyclisch proces waarin kwetsbaarheden en de weerbaarheids bevorderende maatregelen worden geanalyseerd en beoordeeld.[1] In deze publicatie wordt dit proces opgedeeld in vijf fases: beoordelen, prioriteren, behandelen, evalueren, verbeteren. Het doel van kwetsbaarhedenbeheer is om de blootstelling aan risico's van de organisatie te verkleinen. Beveiligingsprocessen zoals kwetsbaarhedenbeheer dienen door organisaties zelf opgestart te worden. Het is wel mogelijk om tools en technieken aan te schaffen of partijen in te huren waarmee je het opzetten van kwetsbaarhedenbeheer gemakkelijker, effectiever en efficiënter maakt.

Het beoordelen van kwetsbaarhedenbeheerbeleid is een van de belangrijkste onderdelen van het hele kwetsbaarhedenbeheer. Beleid op dit thema, zoals het vaststellen van processen en bijvoorbeeld risico bereidheid (*risk appetite*) is van groot belang om effectief kwetsbaarhedenbeheer te faciliteren.

Wat is een kwetsbaarheid?

Een eigenschap die een aanvaller de mogelijkheid biedt een cyberaanval uit te voeren of een eigenschap die kan leiden tot uitval. Dit kan zich voordoen in een digitale dienst, proces of systeem, maar ook in de samenleving als geheel of in een specifieke organisatie.[2]

Methodologie

De in deze publicatie genoemde methode is gebaseerd op Gartner's vijf fases van kwetsbaarhedenbeheer. We gebruiken dit als leidraad om de weerbaarheid verhogende maatregelen van je organisatie uit te voeren en zo het aanvalsoppervlak te verkleinen. Kwetsbaarhedenbeheer wordt doorgaans als onderdeel gezien van aanvalsoppervlaktemanagement (*attack surface management*[3]). Hierbij wordt gekeken op welke wijze een organisatie kwetsbaar is voor aanvallen van buitenaf. Systemen die toegankelijk zijn vanaf het internet en daarnaast ook nog kwetsbaar blijken voor misbruik vormen samen het blootgestelde oppervlak van de organisatie. Kwetsbaarheden beheer is een middel om de risico's van dit blootgestelde (*exposed surface*) te mitigeren onder de bredere noemer *exposure management*. Bekijk hieronder de visualisatie en de vijf fases voor meer overzicht:

- *Beoordelen*
  - Asset inventarisatie
  - Kwetsbaarheden scannen
- *Prioriteren*
  - Blootstelling
  - Essentie
  - Het dreigingslandschap
  - Impact
- *Behandelen*
  - Updaten
  - Mitigeren
  - Accepteren
- *Evalueren*
  - Scan opnieuw
  - Evalueer effectiviteit
- *Verbeteren*
  - Pak onderliggende problemen aan
  - Ontwikkel processen en leveranciersafspraken
  - Evaluaeer meet-methode

Cyclisch proces

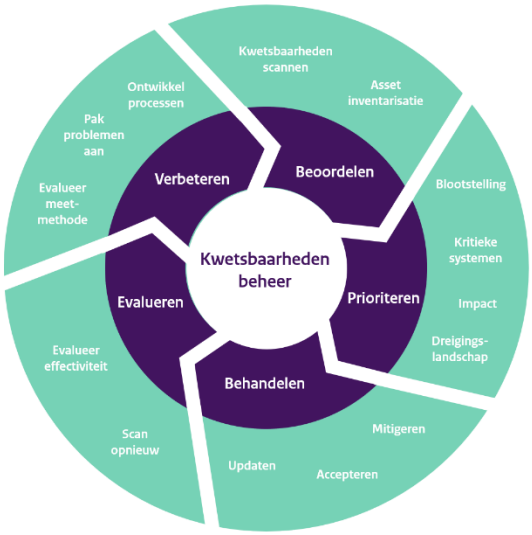
Kwetsbaarhedenbeheer is een cyclisch proces dat niet stopt bij het oplossen van kwetsbaarheden (zie afbeelding 1). Het proces begint weer opnieuw begint met het evalueren van de effectiviteit van de genomen maatregelen en het beoordelen van de huidige situatie. Door deze cyclische aanpak – beoordelen, prioriteren, behandelen, evalueren en verbeteren – te volgen, versterken organisaties hun systemen voortdurend en nemen een proactieve houding aan tegen de steeds veranderende cyberdreigingen. Dit benadrukt het belang van een cyclisch en gestructureerd beheerproces.

In de volgende hoofdstukken bespreken we iedere fase inhoudelijk. We geven vervolgens per fase algemeen advies en praktische tips met betrekking tot het uitbesteden of intern oplossen van je kwetsbaarhedenbeheer.

[1] Proactief op zoek naar kwetsbaarheden | Publicatie | Nationaal Cyber Security Centrum

[2] Woordenboek - Cyberveilig Nederland

[3] Handreiking Kwetsbaarheidsscans Rijksoverheid



Afbeelding 1. Zie ook bijlage 1

1. Beoordelen

In de fase *beoordelen* inventariseer je je assets en scan je deze op kwetsbaarheden, waardoor je een solide basis legt voor de volgende stappen in het beheerproces. Zonder deze eerste stap blijft onduidelijk waar prioriteiten liggen. Dit leidt tot inefficiënte beveiligingsmaatregelen of gemiste kritieke dreigingen.

Beoordelen is dus het vertrekpunt voor een effectief, gestructureerd en cyclisch beheerproces. Tijdens deze fase worden potentiële zwakke plekken in systemen en applicaties in kaart gebracht, waardoor je inzicht krijgt in je aanvalsoppervlak.

Asset inventarisatie

De inventarisatie van assets is een noodzakelijk onderdeel van het kwetsbaarhedenbeheer proces,omdat het inzicht geeft in welke systemen, applicaties en apparaten beschermd moeten worden Zo kun je gerichte beveiligingsmaatregelen nemen.

Wat is een asset?

Assets zijn alle middelen die essentieel zijn voor het functioneren van de organisatie. Dit omvat fysieke middelen (zoals hardware), digitale middelen (zoals data, software en systemen) en immateriële middelen (zoals intellectueel eigendom en reputatie).

Een nauwkeurig en zorgvuldig bijgewerkte CMDB (Configuration Management Database) is het ideaal, maar op z'n minst wil je een overzicht van de volgende zaken[4]:

Wat heb je precies als assets en welke kernprocessen raken die binnen de organisatie?[5] Denk hierbij aan digitale diensten, servers, applicaties, printers etc.

Waar is het? Hoe heeft het verbinding met de organisatie? Hoe is de organisatie blootgesteld tot het publieke internet?

Wat voor software is erop geïnstalleerd, welke versie is het en zijn er nu al kwetsbaarheden bekend met betrekking tot de versie?[6]

Wie is verantwoordelijk voor beheer en onderhoud en wie heeft er toegang toe?

Er zijn VA (Vulnerability Assessment)-tools om assets te ontdekken (kwetsbaarheden scans). Het is mogelijk om de data (in de CMDB) aan te vullen door de functionaliteiten van verschillende VA-tools te combineren. Heb je geen toegang tot VA-tools? Dan is handmatig onderzoek doen naar je assets een tijdsrovende en foutgevoelige optie.[7] Bijvoorbeeld door gesprekken te voeren met proceseigenaren en leveranciers en dit handmatig te registreren.

Daarbij is het belangrijk dat alle assets op verschillende niveaus goed in kaart zijn gebracht en er geen assets worden gemist. Denk aan een printer die verbonden is met het netwerk of aan werk- en privételefoons.

Configuratiemanagement

Configuratiemanagement is een belangrijk onderdeel van je asset inventarisatie. Door nauwkeurig bij te houden welke hardware, software, en netwerkinstellingen aanwezig zijn, identificeer en prioriteer je kwetsbaarheden effectiever. Bovendien maakt configuratiemanagement het mogelijk om afwijkingen van veilige standaardconfiguraties snel te detecteren. Dat helpt je bij het minimaliseren van risico's en het bevorderen van consistente beveiligingspraktijken. Met goed beheerde configuraties

[4] Hoe breng ik mijn technische te beschermen belangen in kaart? | Wat kun je zelf doen? | Nationaal Cyber Security Centrum

[5] Hoe breng ik mijn te beschermen belangen in kaart? | Wat kun je zelf doen? | Nationaal Cyber Security Centrum

[6] SBOM-startersgids | Publicatie | Nationaal Cyber Security Centrum

[7] Hoe breng ik mijn technische te beschermen belangen in kaart? | Wat kun je zelf doen? | Nationaal Cyber Security Centrum

leg je de basis voor solide en proactief kwetsbaarhedenbeheer.

Kwetsbaarheden scannen

Zet scans in voor het voorbereiden op een effectieve aanpak en mitigatie van geïdentificeerde kwetsbaarheden.

Maar hoe vaak moet je eigenlijk scannen? Jouw uiteindelijke doel moet overeenkomen met de waarde van het leveren van vernieuwde kwetsbaarheidsgegevens. Denk aan patchbeheer en beveiligingsmonitoring. Het heeft geen zin om vaker te scannen als deze processen niet profiteren van frequenter scannen. Het moet passen binnen de processen van de organisatie, maar wel met de voorwaarde dat de waarde van scans goed zijn ingeschat.

Heeft je organisatie niet de capaciteiten om een VA scan uit te voeren of uit te besteden? Dan is het extra belangrijk om aandacht te besteden aan je asset inventarisatie. Want in dat geval moet je per asset handmatig onderzoek doen naar kwetsbaarheden. Besteed vervolgens aandacht aan het goed integereren van je kwetsbaarheden beoordeling in bestaande processen. Zie het kopje 'Intern' voor meer informatie.

Algemeen advies:

VA-scans werken niet in een keer, vooral in complexe bedrijfsomgevingen. Hou rekening met problemen of situaties, zoals authenticatieproblemen of een servercrash. Houd hier rekening mee.

Informeer je afdeling IT wanneer een scan plaatsvindt. Zo verras je ze niet wanneer een scan problemen oplevert in een IT-omgeving.

Het is een goed idee om een VA-scan buiten kantooruren uit te voeren, maar houd er rekening mee dat de scans niet tegelijkertijd met andere activiteiten zoals back-ups en bestandsoverdrachten plaatsvinden. Denk ook aan beschikbaarheid van ondersteuning en mogelijke probleemoplossing tijdens een scan.

Uitbesteden of intern

Hieronder staan een aantal verschillen om rekening mee te houden.

Uitbesteden

Stel duidelijke verwachtingen en SLA's op

Definieer de deliverables, tijdlijnen en verwachtingen via Service Level Agreements (SLA's). Blijf de afspraken ook updaten.

Zorg voor transparantie en communicatie

Stem communicatielijnen af en hanteer open communicatie, zodat onder andere kritieke kwetsbaarheden snel worden gerapporteerd.

Intern

Investeer in de juiste tools en training

Zorg ervoor dat je team toegang heeft tot scan-tools en training van de laatste kwetsbaarheden en beoordelingsmethoden. Dit is cruciaal voor een effectieve kwetsbaarheidsidentificatie.

Integreer beoordelingen in bestaande processen

Maak van kwetsbaarhedenbeoordeling een terugkerend geïntegreerd proces dat is afgestemd op patchbeheer, incidentrespons en overige relevante processen.

Prioriteer uitgebreide asset-inventarisatie

Het is eerder genoemd, maar de kracht zit in de herhaling; richt je op het nauwkeurig inventariseren van alle assets, waaronder ook cloud en remote devices. Automatiseer de identificatie en controleer steeksproefgewijs handmatig.

Casus

Een marketingbureau heeft verschillende netwerkprinters verspreid in hun kantoor.

Tijdens door een extern uitgevoerde kwetsbaarheidsanalyse kwam gelukkig op tijd naar voren dat de printers nooit waren meegenomen in het kwetsbaarheidenbeheer. De printers hadden volgens de leverancier verouderde firmware, zwakke wachtwoorden en waren toegankelijk via open poorten op het interne netwerk. De printers waren ook niet meegenomen in de configuratie management. De combinatie van factoren maakte de printers kwetsbaar voor toegang en exploitatie door cybercriminelen.

2. Prioriteren

In de fase *prioriteren* stel je prioriteiten op van de bekende kwetsbaarheden en je eigen systemen. Dit doe je aan de hand van het risicoprofiel van je organisatie. Gebruik de publicatie *Hoe bepaal ik de meest relevante risico's voor mijn organisatie?* wanneer je meer wilt weten hoe je een profiel kunt opstellen.

Het toekennen van scores aan zowel de kwetsbaarheid als de apparatuur waar deze kwetsbaarheid in zit, helpt je in het prioriteren. Voor het toekennen van scores zijn er meerdere componenten waar je rekening mee moet houden. Deze componenten zijn het dreigingslandschap, de blootstelling, essentie, het dreigingslandschap en impact. Deze componenten zorgen voor een score per kwetsbaarheid (zie casus). Vervolgens neem je het gemiddelde van deze scores en het uiteindelijke cijfer. Het uiteindelijke cijfer weeg je af met de andere kwetsbaarheden om te kijken welke kwetsbaarheid prioriteit heeft over anderen. We zullen nu iedere component verder uitdiepen.

Blootstelling

De mate van blootstelling (*exposure*) van het systeem helpt erg in het priorteren van kwetsbaarheden. Op het moment dat een systeem met een kwetsbaarheid niet toegankelijk is vanaf het publieke internet dan heeft deze kwetsbaarheid qua blootstelling een lagere prioriteit ten opzichte van een kwetsbaarheid in een systeem wat wel publiekelijk toegankelijk is en dus een grotere blootstelling heeft.

Kritieke systemen

Hoe kritiek een systeem is voor de organisatie heeft invloed op de prioritering. Een vitaal systeem voor het kernproces van een organisatie heeft een hogere prioriteit heeft dan een randsysteem. Naast het kijken hoe kritiek het systeem is voor de organisatie moet je ook kijken naar hoe kritiek het is binnen processen. Ook niet vitale systemen met grote invloed op processen kunnen prioriteit krijgen. Hoe kritiek een systeem is voor de organisatie bestaat dus zowel uit hoe kritiek het systeem is in een proces als hoe kritiek het proces is voor de organisatie.

Het dreigingslandschap

Het dreigingslandschap is belangrijk om rekening mee te houden en kan snel veranderen. Onderdelen van het dreigingslandschap zijn bijvoorbeeld de aanwezigheid van exploitcode voor de kwetsbaarheid, of de kwetsbaarheid al misbruikt wordt, of de kwetsbaarheid al breed bekend is en of er binnen jouw of soortgelijke organisaties al pogingen zijn gedaan om de kwetsbaarheid te misbruiken. Het is van belang een up-to-date beeld van het dreigingslandschap te behouden omdat deze continu aan ontwikkeling onderhevig is. Het NCSC heeft hier al een publicatie over geschreven, zie *Hoe breng ik mijn dreigingen in kaart?* voor meer informatie.

Impact

De potentiële impact van de compromittatie van een systeem heeft invloed op de prioriteit. Wanneer compromittatie zorgt voor het lekken van gevoelige gegevens zoals financiële of persoonsgegevens dan heeft deze kwetsbaarheid qua impact een hoge prioriteit. Wanneer compromittatie enkel leidt tot het tijdelijk uitschakelen van een systeem dan zal de prioriteit van deze kwetsbaarheid op dit vlak lager liggen.

Algemeen advies

Het is belangrijk dat de juiste mensen bij het prioriteren te betrekken. Zorg ervoor dat de risico eigenaar erbij betrokken is, deze persoon zal beter weten hoeveel prioriteit het systeem verdiend.

Wanneer je voor de eerste keer gaat prioriteren zal dit proces veel langer duren dan wanneer het proces vaker is doorlopen, het is daarom een goed idee om het te oefenen.

Ook een kwetsbaarheid met een lage score moet uiteindelijk opgepakt worden.
Wanneer een kwetsbaarheid een lage score krijgt betekent dit niet dat deze niet opgepakt moet worden, het betekent dat er nu kwetsbaarheden zijn die belangrijker zijn.

Uitbesteden of Intern

Wanneer je kwetsbaarhedenbeheer wordt uitgevoerd door een derde partij is het belangrijk dat het proces goed wordt doorlopen. Het is hiervoor belangrijk dat de derde partij antwoord kan geven op alle punten die in dit hoofdstuk besproken worden.

Uitbesteden

Weet wat je van je leverancier afneemt.
Veel organisaties zullen delen van hun IT-behoeften afnemen bij een leverancier, zorg dat je zwart op wit hebt van deze leverancier wat hier wel en niet onder valt

(SLA's). Valt het updaten van de devices en software pakketten onder jouw taak of doen zij dit voor jullie?

Overleg periodiek met de leverancier over de context.
Zorg er voor dat de leverancier alle context (welke systemen zijn er belangrijk, hoe staat het met het dreigingslandschap) heeft, dit betekend dat het een goed idee is om periodiek met de leverancier te zitten om de recente context up-to-date te houden.

Maak duidelijke afspraken over een verwachte tijdlijn
Zorg ervoor dat bij het uitbesteden er duidelijke afspraken zijn over het prioriteringsproces. Verwacht de leverancier input of gaan ze volledig zelf te werk?

Intern

Betrek ook de supervisor van de gebruikers van het systeem.
Door ook de supervisor van de gebruikers te betrekken zorg je ervoor dat deze direct geïnformeerd is, mocht het nodig zijn om het systeem offline te nemen. Daarnaast weten zij heel goed hoe essentieel een systeem is voor hun processen.

Wanneer een organisatie ervoor kiest zelf te prioriteren, hoeft niet alles vanaf de grond opgebouwd te worden.
Voor het effectief registreren, scannen en inwinnen van dreigingsinformatie zijn al tal van tools beschikbaar.

Casus

Het marketingbureau heeft een externe partij ingehuurd voor alle vrijwel IT-zaken, maar kwetsbaarhedenbeheer zit niet in hun pakket. Tijdens de fase prioriteren wordt er gekeken welke kwetsbare systemen de hoogste pioriteit hebben. Hieronder is voor de netwerkprinters een proriteitsbeoordeling weergegeven:

Blootstelling: (8/10)

Het systeem is direct bereikbaar over het internet en is dus volledig openbaar en makkelijk te misbruiken.

Essentie: (3/10)

De printer word eigenlijk voornamelijk gebruikt om labels voor post te printen.

Dreigingslandschap: (7/10)

Er wordt misbruik gemaakt van enkele van de kwetsbaarheden die de printers hebben, dit komt slechts in enkele gevallen voor en het is onduidelijk of dit gebeurt binnen soortgelijke organisaties.

Impact: (4/10)

De printer is voornamelijk een makkelijke manier om het netwerk binnen te dringen. Misbruik zorgt voor beschikbaarheids problemen.

Gemiddelde score: (5.5/10)

Deze informatie wordt opgeslagen en verwerkt en op basis van de gemiddelde scores wordt er gekozen welke kwetsbaarheden eerst worden aangepakt.

3. Behandelen

De behandelfase is de fase waar veel ad-hoc handelende organisaties direct toe overgaan als het gaat om kwetsbaarhedenmanagement. Het is belangrijk om eerst de fasen 'Beoordelen' en 'Prioriteren' te doorlopen.

De behandelfase bestaat uit drie opties: updaten, mitigeren en accepteren. Veel organisaties zullen alleen updaten als een optie zien, maar zullen soms zonder het te realiseren zich ook al bezighouden met de andere twee opties. Updaten is ook niet altijd een optie. Als er bijvoorbeeld nog geen update is vanuit de leverancier maar er moet wel actie worden ondernomen, dan zijn mitigeren of accepteren de enige die overblijven.

Behandelen is vergelijkbaar met risicobehandeling van de Routekaart Risicomanagement van het NCSC. Het verschil is dat updaten niet een van de opties is in de Routekaart Risicomanagement, want ook een volledig geüpdatet systeem heeft risico's.

Updaten

Updaten is de makkelijkste optie en moet de standaard instelling zijn. Voordat een kwetsbaarheid behandeld kan worden door te updaten, moet er met een aantal dingen rekening worden gehouden. Eerst moet de systeemeigenaar benaderd worden om te bepalen wat voor een impact de update heeft. Een voorbeeld hiervan is dat het updaten van een databaseversie ervoor kan zorgen dat er mogelijk informatie verloren gaat, of bepaalde structuren niet meer goed werken. In dat soort gevallen is het belangrijk dat er met de stakeholders en gebruikers een beslissing wordt gemaakt over het updaten.

Mitigeren

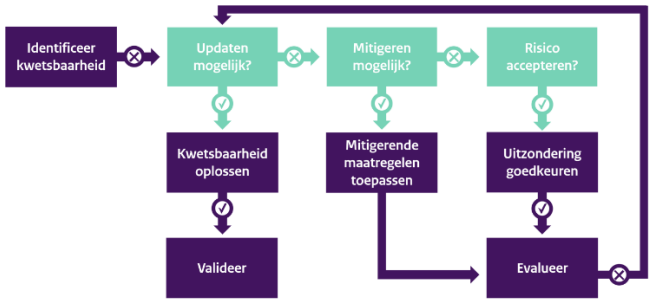
Wanneer updaten geen optie is, omdat een kwetsbaarheid zich bijvoorbeeld in een proces bevindt dat tijdssensitief is, dan is mitigeren de volgende optie. Mitigeren betekent het limiteren van het kwaad dat er gedaan kan worden door misbruik. De maatregelen zijn: het isoleren van het systeem met de kwetsbaarheid, ervoor zorgen dat succesvolle aanval vanaf bepaalde netwerken niet mogelijk is en het veranderen van de configuratie. Bij het veranderen van de configuratie moet je bijvoorbeeld denken aan het tijdelijk uitschakelen van sommige features of tijdelijk extra focus op het systeem door middel van extra logging.

Mitigeren is een tijdelijke oplossing. Bespreek daarom met de stakeholders een houdbaarheidsdatum van de mitigatie af. Wanneer deze houdbaarheidsdatum is verlopen wordt er opnieuw gekeken of updaten een optie is, of dat er misschien andere mitigaties zijn of dat het risico geaccepteerd moet worden.

Accepteren

Wanneer updaten en mitigeren geen opties zijn, blijft er enkel nog accepteren over. Accepteren is alleen mogelijk als dit binnen de risicobereidheid van de organisatie past. Het kan zijn dat een systeem bijna end-of-life is en dat er al aan een vervanger wordt gewerkt. Misschien is het dan een optie dat voor de korte tijd dat dit systeem nog draait, dit gebeurt met een kwetsbaarheid. Het is ook mogelijk dat updaten niet mogelijk is omdat het systeem al oud is en buiten de ondersteuningsperiode van de maker valt. Als dit gebeurt, in combinatie met een systeem waarbij al standaard alle mitigaties zijn toegepast, dan is het accepteren van risico de enige optie. Ook bij accepteren is het een belangrijk punt om een houdbaarheidsdatum te hebben op de acceptatie. Hoe langer een systeem kwetsbaar is des te meer kans er is dat er misbruik gemaakt wordt van de kwetsbaarheid (zie afbeelding 2 voor de belangrijkste stappen).

Als zowel updaten en mitigeren geen optie zijn, maar het accepteren van het risico niet binnen de risico bereidheid valt dan moet een systeem uitgeschakeld en vervangen worden.



Afbeelding 2. Zie ook bijlage 2.

Algemene punten

Updaten is altijd de beste keus.
Als het mogelijk is om een kwetsbaarheid te behandelen door het toepassen van een update dan is dit altijd de beste oplossing.

Waar mogelijk test de updates voordat je ze uitrolt.
Als het mogelijk is om de updates te testen voordat deze worden uitgerold doe dit. Het zorgt er voor dat vervelende verassingen in compatibiliteit snel bekend worden.

Uitbesteden

Zorg dat de leverancier op de hoogte is van je risicobereidheid.
Je leverancier gaat voor jou de problemen oplossen, maar om dit juist te doen is het belangrijk dat ze op de hoogte zijn van je risicobereidheid. Neem deze overwegingen op in de SLA. Zo weet de leverancier wanneer het accepteren van risico's mogelijk is.

Vergelijk verschilende partijen op hun snelheid.
De snelheid van het oplossen van kwetsbaarheden is natuurlijk niet alles, het is echter wel een belangrijk punt. Tot het is opgelost blijf je als organisatie kwetsbaar.

Intern

Prioriteer zorgvuldigheid boven snelheid.
Het gedetailleerd en zorgvuldig uitvoeren van het behandelingsproces is erg belangrijk. Wanneer je over de maximum snelheid van het proces gaat, worden er sneller fouten gemaakt.. Het zorgt er ook voor dat er binnen de organisatie bekend is wanneer er een update verwacht kan worden.

Gebruik automatische updates.
Veel applicaties hebben automatische updates, denk aan Windows, Adobe Acrobat, Firefox etc. Wanneer de makers van deze applicaties een kwetsbaarheid vinden brengen ze vaak snel een update naar buiten om deze kwetsbaarheid op te losssen. Deze updates zorgen er maar zelden voor dat het programma niet meer werkt, wanneer dit wel het geval is kan je altijd weer een oudere versie tijdelijk installeren. Het gebruik van automatische updates kan erg veel tijd besparen.

Casus

Op basis van de prioriteitenafweging uit de vorige fase is duidelijk geworden dat de netwerkprinters aan het internet blootgesteld zijn, er een exploiteerbare kwetsbaarheid bekend en beschikbaar is waardoor het een score van 5.5/10 heeft gekregen. Er is gelukkig een update beschikbaar voor het merk en de softwareversie van de printers. Het marketingbureau laat aan alle medewerkers weten dat morgen de printer niet beschikbaar is vanwege updates en dingen die dan geprint moeten zijn dus vandaag geprint moeten worden.

De volgende dag zijn de updates allemaal succesvol geïnstalleerd, maar blijkt dat dit wel de laatste software update was voor deze printers. Het marketingbedrijf kiest er dus voor om alvast mitigerende maatregelen uit te voeren, de printers komen op hun eigen netwerk en worden niet meer vanaf het internet toegankelijk.

4. Evalueer

Het valideren van de resultaten van herstel- of risicobeperkende maatregelen zorgt ervoor dat het huidige risiconiveau is afgestemd op de oorspronkelijke verwachtingen. Het is belangrijke om te weten of de maatregelen die in de behandelingsfase zijn genomen doeltreffend waren.

Scan opnieuw

Door opnieuw te scannen op kwetsbaarheden toont een organisatie aan of het aanvalsoppervlak daadwerkelijk is verkleind. Doe dit bij voorkeur op dezelfde wijze als tijdens de beoordelingsfase.

Evalueer effectiviteit

Om te zorgen dat de gekozen beheersmaatregelen daadwerkelijk effect hebben, moet je ze periodiek evalueren. Dit doe je door het bijhouden van de implementatie, het evalueren van de prestaties en het beoordelen van de effectiviteit van de beheersmaatregelen. Vervolgens bepaal je of de effectiviteit van de maatregelen de gewenste impact heeft op het restrisico (het risico dat overblijft nadat de risicomaatregel is uitgevoerd).

Na het opnieuw uitvoeren van de scan stel je vast of de maatregelen effectief zijn geweest. Als de maatregelen effectief waren, dan is het restrisico voor de organisatie kleiner geworden. Als de risico-eigenaar van mening is, dat het restrisico een acceptabel niveau heeft bereikt, dan zijn aanvullende maatregelen niet nodig.

Inzicht in de actuele assets en de configuratie van systemen in het netwerk van een organisatie is noodzakelijk om het aanvalsoppervlak te bepalen. Maatregelen die getroffen zijn in de behandelfase dienen verwerkt te worden in de asset/configuratie database. Nieuwe assets dienen te worden toegevoegd en configuratieaanpassingen (updates) worden vastgelegd.

Uitbesteden of intern

Voor de evalueerfase kan voor dezelfde vorm (intern/extern) als in de beoordelingsfase worden gekozen. In het geval van het intern beleggen van deze processtap is het aan te raden periodiek een externe partij een objectieve test/scan uit te laten voeren om het eigen proces te verifiëren.

Advies algemeen

Betrek stakeholders bij de evaluatie

Om te kunnen bepalen of het proces of de behandeling goed verlopen is, is het belangrijk de juiste stakeholders te betrekken. De risicoeigenaar (bestuurder), de behandelaar (IT-beheerder) en de gebruikers.

Maak gebruik van frameworks

Bijvoorbeeld NIST, ISO27001 of CIS Controls

Uitbesteden

Vraag om gedetailleerde rapportages

Om goed te kunnen begrijpen of diensten goed en effectief uitgevoerd zijn is het noodzakelijk te begrijpen wat er gedaan is. Enkel terugkopeling over het resultaat is daarin onvoldoende.

Plan regelmatige evaluatie momenten in

Voorkom samenwerkingsproblemen door het uitbesteden van diensten zorgvuldiig voor te bereiden en de voortgang regelmatig te bespreken.

Intern

Gebruik meetbare KPI's

Key Performance Indicators (KPI's) moeten de organisatie een duidelijk beeld geven over de effectiviteit van de behandelingsmaatregelen. Indien een KPI met een goed of slecht resultaat niet direct leidt tot het moeten maken van keuzes of nemen van maatregelen, is het geen goede KPI om te meten.

Implementeer onafhankelijke audits

Interne processen kunnen ondanks zorgvuldigheid toch een bepaalde mate van subjectiviteit bevatten. Daartoe is het verstandig om periodiek een onafhankelijke partij objectief mee te laten kijken.

Casus

Het marketingbureau heeft de netwerkprinters in hun kantoor geüpdatet. Ze pasten de nodige firmware-updates toe, versterkten de wachtwoorden en segmenteerden de printers in een apart netwerk om hun blootstelling aan interne aanvallen te beperken.

Vervolgens werd er opnieuw een kwetsbaarheidsanalyse uitgevoerd. De beleidsaanpassing, updates, aangepaste toegangseisen en segmentatie hebben het aanvalsoppervlak effectief verkleind.

Echter, gebleken is dat de netwerkprinters na deze handelingen nog steeds niet zijn opgenomen in de asset-inventarisatielijst. Hierdoor is de kans groot dat ze in de volgende cyclys geen deel uitmaken van het kwetsbaarhedenbeheerproces en mogelijk onopgemerkt kwetbaar kunnen worden.

Als verbeterpunt neemt de organisatie het bijwerken van de asset-inventarisatielijst naar een up-to-date en volledige versie.

5. Verbeteren

In de fase *verbeteren* richten we ons op het in kaart brengen van de geleverde prestaties van het proces. Ook identificeren we manieren om de volwassenheid en het vermogen om kwetsbaarheden goed te beheren continu te verbeteren.

Pak onderliggende problemen aan

Om nieuwe kwetsbaarheden te voorkomen is het van belang vast te stellen hoe deze zijn ontstaan. Na de herbeoordeling van de genomen beheersmaatregelen is het van belang om vast te stellen hoe deze kwetsbaarheden ontstaan zijn. Afhankelijk van de soort kwetsbaarheid kan er worden vastgesteld welke soort beheersmaatregel kan worden toegepast.

Ontwikkel processen

Procesontwikkeling is het verbeteren van de volwassenheid van het kwetsbaarhedenbeheerproces. Organisaties beginnen kwetsbaarhedenbeheer vaak met een basis-set van processen en in het geval van uitbesteden met beperkte leveranciersafspraken. De procesontwikkeling loopt dan ook van ad-hoc, handmatige en niet-risico gebaseerd patching tot geïntegreerde, risicobewuste beveiligingsbeoordeling- en monitoring programma's. Deze ontwikkelingen leiden bijvoorbeeld tot nieuw beleid en procesafspraken of nieuwe leveranciersafspraken.

Evalueer meet-methode

Effectiviteit van kwetsbaarhedenbeheer moet voortdurend worden gemeten bij het beoordelen of de juiste risicovermindering wordt bereikt. Het meten van hoe alle beoordelings-, mitigatie- en herstelactiviteiten kwetsbaarheden verminderen is een essentieel onderdeel van het proces. Er zal niet één metrische waarde zijn die kan kwantificeren hoe goed een bepaald kwetsbaarhedenbeheersysteem het doet.

Uitbesteden of intern

De fase *verbeteren* kan je het best intern uitvoeren. Het implementeren van verbeteracties gaat in overleg met de uitvoerder, intern of extern.

Advies algemeen

Prioriteer

Richt je op de kwetsbaarheden met de hoogste impact op je belangrijkste assets

Betrek de relevante afdelingen

Samenwerking is cruciaal en het verbeteren van je kwtsbaarheden vereist vaak een bedrijfsbrede aanpak.

Documenteer de verbeteringen

Maak een overzicht van alle genomen maatregelen en besluiten. Hiermee voorkom je dat alle kennis bij een individu ligt en dit is belangrijk voor het implementeren van toekomstige verbeteringen.

Casus

Het marktetingbureau uit deze casus werd kwetsbaar door achterstand. Doordat de netwerkprinters niet opgenomen waren in de asset-inventarisatie, werden de configuraties niet bijgehouden en de elementen niet meegenomen in het kwetsbaarhedenbeheer.

Door het treffen van de beveiligingsmaatregelen uit de ‘Behandeling’ fase zijn deze kwetsbaarheden verholpen of kleiner gemaakt. Het onderliggende probleem was echter dat deze assets geen onderdeel uitmaakten van het kwetsbaarhedenbeheer. De probleemoorzaak was dus in de eerste plaats van organisatorische aard.

Door het opnemen van de netwerkprinters in de assetinventory en het kwetsbaarhedenbeheer, wordt dit in de toekomst voorkomen. Daarnaast zou het een goede procesontwikkeling zijn om het netwerk te onderzoeken op de aanwezigheid op andere ‘vergeten’ assets of netwerkonderdelen.

6. Aandachtspunten

Risico's en valkuilen

De aanwezigheid van niet-gemelde kwetsbaarheden (o-day) vormt een risico, omdat actoren kunnen profiteren van kwetsbaarheden.

Wanneer je organisatie **elk geïdentificeerde kwetsbaarheid probeert op te lossen** dan worden er middellen en tijd verspild aan kwetsbaarheden met minimale potentiele impact op de organisatie. De geprioriteerde kwetsbaarheden worden mogelijk niet op tijd aangepakt.

Ineffectieve communicatie verhoogt het risico dat er informatie, zoals kwetsbaarheden en prioriteiten, niet helder wordt overgebracht en dit kan leiden tot vertraging.

Je kunt er vaak weinig tegen doen, maar het hebben van **onvoldoende middelen voor herstel** vergroot de risico dat kwetsbaarheden niet optijd worden aangepakt, waardoor je assets langer kwetsbaar zijn voor aanvallen.

Door **alleen kwetsbaarheden** die in de prioriteerfase als kritiek zijn beoordeeld op te lossen heb je hetrisico dat aanvallers de steeds toenemende middel/laag kwetsbaarheden gebruiken om aan te vallen.

Governance

Een belangrijke stap die organisaties kunnen zetten voordat ze met kwetsbaarhedenbeheer aan de slag gaan is het opstellen van beleid op dit gebied. Iedere net besproken fase van het proces heeft verschillende, op elkaar afgestemde beleidskaders nodig. Voorbeelden per fase:

Beoordelen

- Stel te beschermen belangen vast, welke assets zijn van cruciaal belang voor mijn organisatie
- Leg de verantwoordelijkheid/ eigenaarschap voor assets of processen vast.
- Stel een continue registratieproces vast.

Prioriteren

- Stel de risicotolerantie (*risk appetite*) vast.
- Bepaal een wegingssytematiek voor priotisering.

Behandelen

- Stel een patch/update proces in. Eventueel met een testproces.
- Stel een logisch mitigatieproces vast.

Evalueren

- Bepaal de beoordelingsmetriek.

Verbeteren

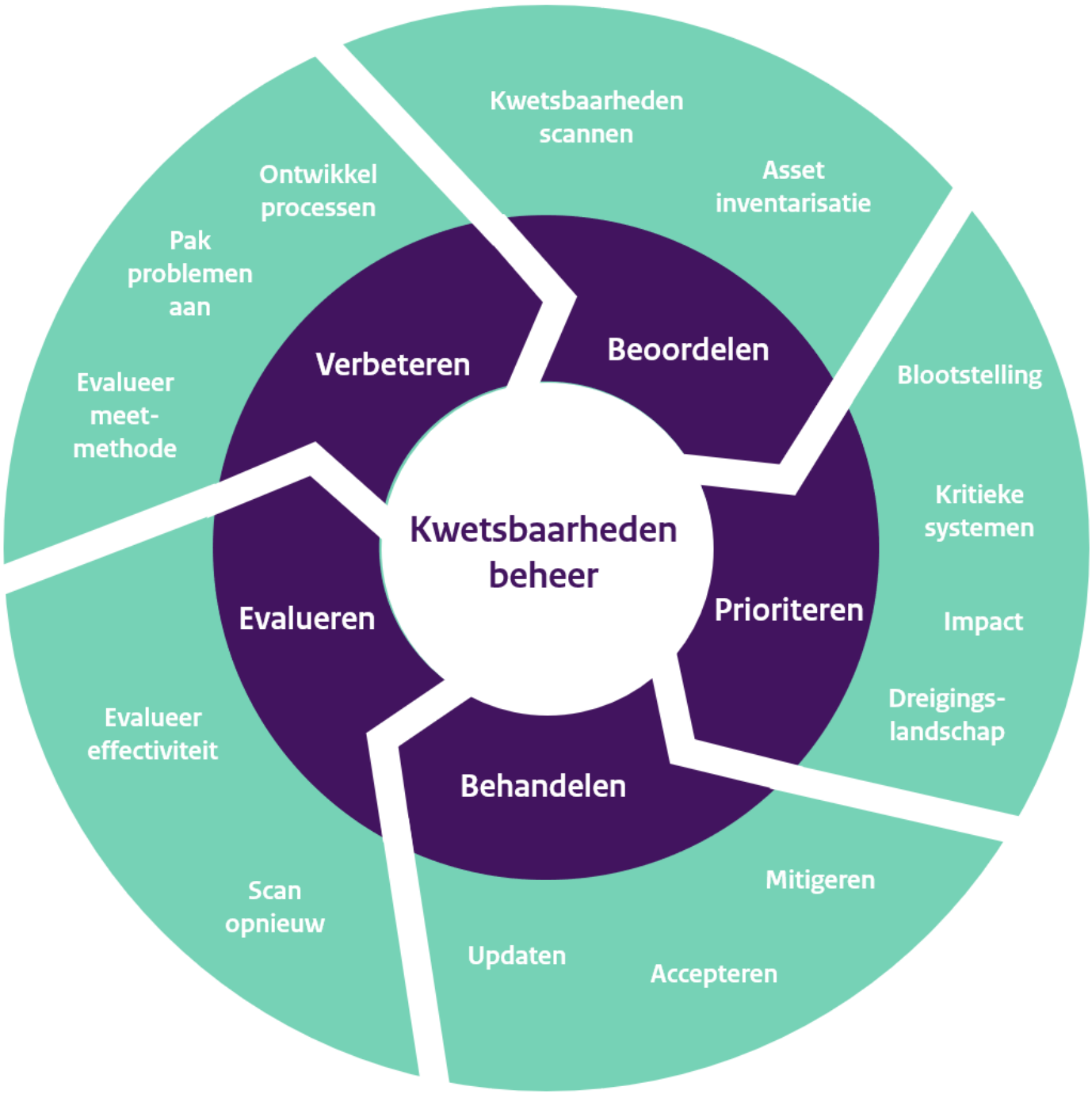
- Stel proceseigenaren vast voor verbeterpunten.

Uitbesteden of intern

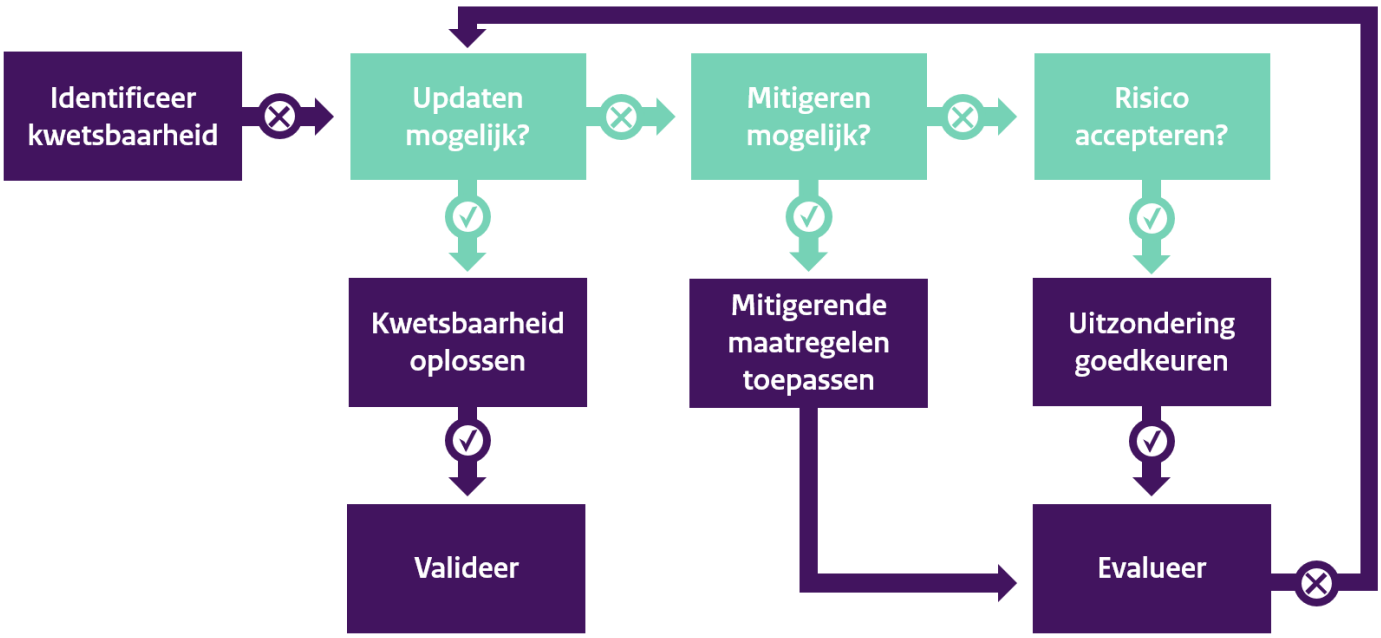
Hoeveel een organisatie uitbesteed is afhankelijk van het volwassenheidsniveau en de besteedbare capaciteit. In het geval van een onvolwassen organisatie, die kwetsbaarhedenbeheer voor het eerst gaat opstarten, zullen veel processen initieel intern uitgevoerd worden. Het is daarbij van belang dat een organisatie bedenkt welke richting het op langere termijn op wil en zich daarop voorbereiden. Daarbij kan bijvoorbeeld gekozen worden om softwarepakketten (tools) aan te schaffen die in eerste instantie complexer zijn dan strikt noodzakelijk. Dit biedt de mogelijkheid dat er ook na het zetten van enkele stappen in de volwassenheid, van dezelfde systematiek of tool gebruik gemaakt kan worden. Zowel bij het intern als extern beleggen, is het van groot belang duidelijke afspraken te maken over het terugkoppelen van resultaatgegevens en verantwoordelijkheden.

Bijlagen

Bijlage 1



Bijlage 2


Identificeer kwetsbaarheid
Updaten mogelijk?
Mitigeren mogelijk?
Risico accepteren?
Kwetsbaarheid oplossen
Mitigerende maatregelen toepassen
Uitzondering goedkeuren
Valideer
Evalueer

Gerelateerde publicaties

In deze publicatie verwijzen we naar de volgende publicaties:

Publicatie	URL
Routekaart risicomanagement	https://www.ncsc.nl/wat-kun-je-zelf-doen/routekaart-risicomanagement/risicobehandeling
Vijf fases van kwetsbaarhedenbeheer	Gartner's vijf fases van kwetsbaarhedenbeheer
Kwetsbaarheidsscan	https://www.cip-overheid.nl/media/djabtmgr/handreiking-kwetsbaarheidsscans-2021-05-03-versie-10.pdf
Asset management	https://www.ncsc.gov.uk/guidance/asset-management
Vulnernability scanning tools and services	https://www.ncsc.gov.uk/guidance/vulnerability-scanning-tools-and-services
Hoe breng ik mijn technische tbb in kaart	https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/herkennen/hoe-breng-ik-mijn-technische-tbb-in-kaart
Hoe breng ik mijn te beschermen belangen in kaart	https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/herkennen/hoe-breng-ik-mijn-te-beschermen-belangen-in-kaart
Sbom startersgids	https://www.ncsc.nl/wat-doet-het-ncsc-voor-jou/documenten/publicaties/2023/juli/5/sbom-startersgids

Bekijk ook de digitale versie van deze publicatie op www.ncsc.nl:
https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/detecteren/kwetsbaarhedenbeheer

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Januari 2025