TLP:GREEN

KWETSBAARHEDENBEHEER

Vulnerability Management – Toolbox

Best Practice versie 1.1

Complexiteit document
Gemiddeld

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit voor cybercriminelen en statelijke actoren. Deze zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot netwerken, systemen en (gevoelige) informatie.

Een prominente wijze waarop deze partijen zich toegang te kunnen verschaffen tot IT-componenten is via kwetsbaarheden in software. Kwetsbaarheden zijn fouten in een digitaal systeem waardoor een aanvaller in het systeem kan komen. Nieuwe kwetsbaarheden worden volcontinu ontdekt en leveranciers brengen regelmatig software updates uit om deze kwetsbaarheden te verhelpen.

Kwetsbaarhedenbeheer is een dienst binnen de organisatie die zich richt op het continu in kaart brengen van de aanwezigheid van bekende kwetsbaarheden in software en het zorgen dat deze worden gerapporteerd en verholpen. Dit is een essentieel onderdeel van het beveiligingsbeleid binnen de organisatie om het aanvalsoppervlak voor malafide partijen zoveel mogelijk in te perken. Kwetsbaarhedenbeheer wordt binnen organisaties veelal als dienst geleverd vanuit het Security Operations Center (SOC), maar dit kan per organisatie anders zijn ingericht.

Dit document is een best practice voor kwetsbaarhedenbeheer binnen de organisatie en is gericht op intern kwetsbaarhedenbeheer. Dit is een aanvulling op de eerder uitgegeven "Handreiking kwetsbaarhedenscans Rijksoverheid (2021, CIO Rijk)", wat zich vooral richt op External Attack Surface Management (EASM).

Achtergrond

Cyberaanvallen zijn een steeds belangrijkere oorzaak van deze incidenten en crises. Door actief op zoek te gaan naar kwetsbaarheden en de bevindingen op te lossen, ben je aanvallers voor. Deze kunnen dan niet van bekende kwetsbaarheden misbruik maken. Deze aanpak is inmiddels een onderdeel van de basis IB-hygiëne en wordt door de Baseline Informatiebeveiliging Overheid voorgeschreven.

Doelgroep

Personen en teams die zich op tactisch of operationeel niveau bezighouden met informatiebeveiliging in het algemeen, en kwetsbaarhedenscans (en het oplossen van bevindingen) in het bijzonder. Dit betreft onder meer Directeuren, Chief Information Security Officers (CISO's), Information Security Officers (ISO's), Security Operations Center (SOC's), projectmanagement, applicatiebeheer en ICT-beheer.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	15-3-2024	Initiële versie
V1.1	11-9-2024	TLP markering opgenomen

1.2 Referenties

Document	Link
Dienstbeschrijving Centrale SOC-voorziening (Project VSSR)	
Handreiking kwetsbaarheidsscans Rijksoverheid (2021, CIO Rijk)	https://www.cip-overheid.nl/media/djabtmgr/handreiking-kwetsbaarheidsscans-2021-05-03-versie-10.pdf
Centrale SOC-voorziening – Strategische aanbevelingen (2023, VSSR)	https://vssr.rijksapplicaties.nl/link?l=DOC-VSSR-MD-RA-SOC_Strategische_Aanbevelingen
VSSR-kennisdocumenten	VSSR (rijksapplicaties.nl)
Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013)	https://wetten.overheid.nl/BWBR0033507/2013-06-01

2 Management Samenvatting

Proactief op zoek naar kwetsbaarheden

Overal gaat er weleens iets mis. Dat geldt ook voor organisaties die informatiebeveiliging gedegen en volwassen hebben ingericht. Door allerlei oorzaken kunnen kwetsbaarheden ontstaan: een patch die mislukt, een server die niet meer gebruikt wordt maar niet is uitgezet, een verkeerd vinkje in de configuratie etc. Met kwetsbaarheidsscans ga je actief op zoek naar dergelijke kwetsbaarheden. Door de kwetsbaarheden te verhelpen, verhoog je direct de feitelijke digitale veiligheid. Ook geeft dit document informatie om de achterliggende processen structureel te verbeteren.

Een eerdere handreiking was vooral gericht op externe kwetsbaarhedenscans om zo extern zichtbare kwetsbaarheden te reduceren. Daarnaast geeft de eerdere handreiking handvaten om de projectinrichting op te zetten. Dit document is een uitbreiding op de eerdere handreiking en richt zich meer op interne scans en geeft daarnaast een verdieping in de operationele kant van kwetsbaarhedenbeheer.

Operationeel proces

Het operationele proces voor kwetsbaarhedenbeheer is in hoofdlijnen uiteengezet in "Handreiking kwetsbaarhedenscans Rijksoverheid (2021, CIO Rijk)". Binnen dit document is het proces uitgebreid met de "Discovery" stap en zal dieper worden ingegaan op de individuele procesonderdelen. De hoofdlijnen van het proces zien er als volgt uit.

1. Discovery: Uitvoeren van een discovery-scan om de componenten in het netwerk in kaart te brengen.
2. Identificeren: Systematisch en geautomatiseerd in kaart brengen van alle kwetsbaarheden in het netwerk.
3. Beoordelen: Analyseren van de uitkomst van het identificeren waarbij aandacht uitgaat naar het duiden, prioriteren en toewijzen van de kwetsbaarheden.
4. Oplossen: Verhelpen van de gevonden kwetsbaarheden door systeem- en/of proceseigenaren.
5. Verifiëren: Ophalen van terugkoppeling betreft het oplossen en met automatische scans technisch verifiëren van de oplos-fase.
6. Rapporteren: Voorzien in de informatiebehoefte van verschillende belanghebbenden betreft de uitvoering van het proces en het risicoprofiel van de organisatie.

Met de "Handreiking kwetsbaarhedenscans Rijksoverheid (2021, CIO Rijk)" en deze best practice beschikt een organisatie over alle middelen om de initiële investering in projectvorm te realiseren en de operationele processen in te richten. Beide documenten tezamen dekken de hele scope van extern en intern kwetsbaarhedenscanning en -beheer af.

3 Inleiding, positionering en scope

3.1 Inleiding

De wereld om ons heen verandert snel. We werken steeds meer digitaal. Ook op technologisch gebied volgen ontwikkelingen elkaar snel op. Zonder (digitale) informatie kunnen we ons werk niet doen. Informatie is daarmee een onmisbaar onderdeel van ons werk. De overheid is voor het uitvoeren van haar bedrijfsprocessen steeds afhankelijker van IT-systemen. Vanzelfsprekend moet er gegarandeerd kunnen worden dat deze (online) systemen veilig zijn. Daarbij komt dat de cybercriminaliteit groeit en professionaliseert en dreigingen toenemen.

We nemen tal van maatregelen om de systemen en de techniek te beschermen. Daarbij is het van belang om systemen en techniek structureel te bekijken op kwetsbaarheden. Dit zorgt ervoor dat als er op de één of andere manier toch iets vergeten wordt, je hier zelf achter komt waarna je dit kan aanpakken en/of oplossen. Behalve het voorkomen van incidenten, krijg je ook een beeld van de werking van processen rondom projecten, wijzigingen, imagebeheer, patchmanagement, en mogelijke verbeteringen.

Al met al draagt het uitvoeren van kwetsbaarheidsscans en –essentieel- het structureel opvolgen van de bevindingen bij aan de digitale weerbaarheid van de Rijksoverheid. De noodzaak wordt benadrukt door de toenemende afhankelijkheid van ICT, de beperkte terugvalmogelijkheden en de toenemende dreiging van buitenaf. Toch is het onmogelijk om op alles voorbereid te zijn en 100% veiligheid bestaat ook in het digitale domein niet. Wel kunnen we ons beter voorbereiden op een digitale ontwrichting.

3.2 Positionering

Een kwetsbaarhedenscan beoogt het versterken van de feitelijke veiligheid en digitale weerbaarheid. Het rapport van de WRR: "Voorbereiden op digitale ontwrichting", is mede aanleiding geweest voor het expliciet aandacht schenken aan kwetsbaarheidsscans. Evenals het Cybersecuritybeeld Nederland (CSBN) en de bespreking daarvan in het Secretarissen-Generaal Overleg (SGO) en de Ambtelijke en Ministeriële Commissie Economie en Veiligheid (ACEV/MCEV) evenzo.

Met het uitvoeren van kwetsbaarheidsscans geef je nadere invulling aan de normen 12.6/12.6.1 en 18.2.3.1 van de Baseline Informatiebeveiliging Overheid (BIO, https://bio-overheid.nl/) en maak je een stap in een meer volwassen uitvoering en inrichting van informatiebeveiliging. Deze best practice ondersteunt daarbij.

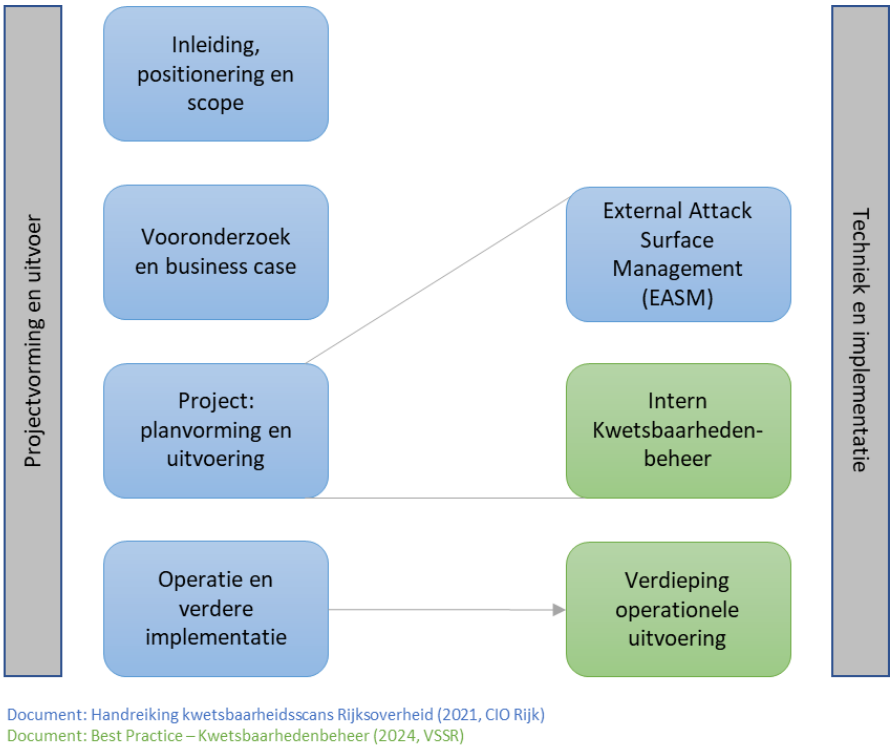
3.3 Scope van deze best practice

In het document "Handreiking kwetsbaarhedenscans Rijksoverheid (2021, CIO Rijk)" is aangegeven dat een uitbreiding betreft interne scans zou volgen. Met dit document wordt verder ingegaan op interne scanning en processen met betrekking tot het oplossen van kwetsbaarheden. Binnen dit document wordt gecontinueerd op de eerdere handreiking op de volgende wijzen:

- De eerder beschreven projectaanpak ook kan worden gebruikt voor het opzetten van intern kwetsbaarhedenbeheer;
- Hoewel voor het oplossen van een kwetsbaarheid de herkomst niet van groot belang is, is het wel goed om te benoemen dat de focus in dit document zal liggen op de meer operationele kant van intern kwetsbaarhedenbeheer (waar deze in de eerdere handreiking voornamelijk was toegespitst op extern kwetsbaarhedenbeheer);
- Dit document bevat een verdieping op het beheerproces zoals geschetst in het eerder document;

- Het operationele proces binnen dit document bevat een minimale verdiepingsslag in de eerste processtap waarmee scannen wordt opgedeeld in Discovery (dit betreft component discovery) en identificeren (kwetsbaarheden identificeren); en,
- Als laatste wordt in de eerdere handreiking "Sturing" genoemd. Dit onderdeel wordt binnen dit document specifieker opgesplitst in "Verifiëren" en "Rapporteren".

De relatie tussen de twee documenten is in Figuur 1 weergegeven. Het document dat voor u ligt, concentreert zich op de groen gemarkeerde onderdelen.



Figuur 1 Relatie tussen de best practice (VSSR) en handreiking (CIO Rijk) kwetsbaarhedenbeheer

Verder gaat dit document in op kwetsbaarhedenbeheer voor zover als kwetsbaarheden voortkomen uit het geautomatiseerd scannen van kwetsbaarheden binnen de IT-infrastructuur. Onderwerpen die hiermee buiten scope vallen zijn:

- Kwetsbaarheden die voortkomen uit andere processen, zoals applicatie (pen)testen, het responsible disclosure proces.
- Risicomanagement binnen de organisatie.
- Het in kaart brengen van kwetsbaarheden voor IT-componenten die buiten scope zijn geplaatst voor geautomatiseerde scanning.

Het is wel aan te bevelen om kwetsbaarheden voortkomend uit de buiten-scope processen (en eventuele andere processen) samen met kwetsbaarheden die voortkomen uit geautomatiseerde scanning allemaal via het zelfde proces op te laten volgen.

3.4 Definitie kwetsbaarhedenbeheer

Een kleine fout in informatiebeveiliging is snel gemaakt, maar kan grote gevolgen hebben. Regelmatig ligt gevoelige data, zoals persoonsgegevens, op straat. Terugkerende oorzaken zijn niet-doorgevoerde updates, onveilige systeeminstellingen, een technisch probleem (fouten tijdens programmeren of ontwikkelen), of menselijk handelen (onbetrouwbaar wachtwoord). Niet iedereen is zich bewust van dergelijke risico's voor hun organisatie. Met het geautomatiseerd uitvoeren van

scans, worden kwetsbaarheden in IT-systemen in kaart gebracht (geïdentificeerd). Deze kunnen vervolgens worden opgelost, zodat het risico op schade wordt geminimaliseerd.

Technisch, breed, geautomatiseerd en passief
Volgens de definitie die deze best practice gebruikt, bestaat kwetsbaarhedenbeheer uit (1) geautomatiseerde scans op (2) technische kwetsbaarheden in de (3) volledige Informatie- en Communicatie Technologie (ICT)-systemen van de desbetreffende Rijksorganisatie inclusief uitbestede diensten en websites (4) waarbij het gaat om het, oplossen en rapporteren van kwetsbaarheden. De processtappen zijn detecteren (discovery en identificeren), beoordelen (duiden en prioriteren), oplossen, verifiëren en rapporteren met als doel de kwetsbaarheden weg te nemen.

Deze definitie kan worden gezien in een bredere context van definities betreft:

- Kwetsbaarheid (volgens de NIS2 richtlijn): "Een zwakheid, vatbaarheid of gebrek van ICT-producten of ICT-diensten die door een cyberdreiging kan worden uitgebuit".
- Cyberdreiging (Verordening EU/2019/881 - art. 2, lid 8): "Elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden".

3.5 Leeswijzer

De best practice is modulair opgebouwd en volgt de operationele cyclus van de operationele kant betreft kwetsbaarhedenbeheer. Daarmee is dit document goed te gebruiken voor het inrichten van de operationele processen van kwetsbaarhedenbeheer binnen uw organisatie. Kwetsbaarhedenbeheer is binnen veel organisaties als taak bij het security operations center (SOC) belegd. Afhankelijk van de organisatie kan dit ook elders worden belegd. Houd hiermee rekening bij het lezen van dit document; waar SOC is genoemd kan dit mogelijk binnen ow organisatie een ander onderdeel betreffen zoals de IT-beheerorganisatie. Gebruik deze best practice samen met de "Best practice kwetsbaarhedenscans Rijksoverheid" om zowel interne als externe kwetsbaarheden te beheren en om zowel de projectfase als de dagelijkse operatie af te dekken.

3.6 Definities

Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

4 Kwetsbaarhedenbeheer

Dit hoofdstuk geeft een verdieping op het proces voor kwetsbaarhedenbeheer en de verschillende fasen binnen het proces. In eerste instantie wordt een overzicht van het proces geschetst, waarna per onderdeel een verdiepingsslag zal worden gedaan.

4.1 Proces overzicht

Het kwetsbaarhedenbeheer proces bestaat uit een continue herhaling van een aantal fasen. Deze fasen zijn weergegeven in *Figuur 2: Kwetsbaarhedenbeheer proces*.

Figuur 2: Kwetsbaarhedenbeheer proces

De verschillende fasen kunnen kort worden samengevat als:

1. Discovery: Uitvoeren van een discovery-scan[1] om de componenten in het netwerk in kaart te brengen.
2. Identificeren: Systematisch en geautomatiseerd in kaart brengen van alle kwetsbaarheden in het netwerk.
3. Beoordelen: Analyseren van de uitkomst van het identificeren waarbij aandacht uitgaat naar het duiden, prioriteren en toewijzen van de kwetsbaarheden.
4. Oplossen: Verhelpen van de gevonden kwetsbaarheden door systeem- en/of proceseigenaren.
5. Verifiëren: Ophalen van terugkoppeling betreft het oplossen en met automatische scans technisch verifiëren van de oplos-fase.
6. Rapporteren: Voorzien in de informatiebehoefte van verschillende belanghebbenden betreft de uitvoering van het proces en het risicoprofiel van de organisatie.

[1] Discovery-scan is een technische term voor het geautomatiseerd in kaart brengen van alle IT-componenten in het netwerk.

4.2 Randvoorwaarden

Het goed kunnen uitlopen van het proces werkt alleen op basis van enkele randvoorwaarden die binnen de organisatie op voorhand belegd dienen te zijn:

- Zorg voor beleid op risicobeheersing en kwetsbaarhedenbeheer: Risicobeheersingsbeleid en kwetsbaarhedenbeheerbeleid zijn van essentieel belang om het proces goed te laten verlopen. Zorg dat deze beleidsdocumenten bestaan en dat bijbehorende processen zijn geïmplementeerd;
- Zorg voor beleid op administratie IT-middelen: Zorg dat de organisatie beleid heeft vastgelegd over het administreren van IT-middelen en wat hierbij de verantwoordelijkheden en consequenties zijn en hoe hierover gerapporteerd wordt;
- CMDB volledig en correct gevuld: Zorg dat de IT-middelen administratie (CMDB) aantoonbaar goed is bijgewerkt;
- Zorg voor toestemming: Voor het scannen van IT-infrastructuur is veelal toestemming nodig van verschillende eigenaren van middelen binnen de eigen organisatie en waar van toepassing van leveranciers.

4.3 Discovery


Discovery

De *discovery-fase* betreft voornamelijk het vaststellen van de scope voor het daadwerkelijk identificeren van de kwetsbaarheden. Deze fase is losgetrokken van het identificeren van de kwetsbaarheden zelf omdat deze fase, afhankelijk van de omvang en complexiteit van de ICT-infrastructuur, een omvangrijke stap kan zijn. Daarnaast is dit onderdeel niet alleen afhankelijk van techniek, maar voor een belangrijk deel van interne processen en afspraken en system- en proceseigenaren.

De discovery-fase is essentieel, immers voor componenten waarvan je niet weet dat je ze hebt, kan je ook niet op zoek gaan naar kwetsbaarheden. Niet geïdentificeerde componenten kunnen op deze manier een hoog risico voor een organisatie vormen. Dat maakt het van belang om het discovery-proces volledig en zorgvuldig in te richten. Kwetsbaarheden scanning tools beschikken standaard over functionaliteit om deze eerste inventarisatiefase goed in te richten.

Tijdens deze fase wordt bepaald wat er gescand moet gaan worden, en nog belangrijker, wat niet. Deze informatie komt in eerste instantie uit de aanwezige CMDB (Configuratie Management Database), maar dient zorgvuldig te worden geverifieerd met de eigenaren. Een belangrijk onderdeel van deze verificatie betreft het vaststellen welke componenten absoluut niet mogen worden gescand (sommige componenten zijn soms te oud of te gevoelig om veilig te kunnen scannen en dienen dus te worden uitgesloten). Vervolgens kunnen de eerste resultaten verder worden aangevuld met de gegevens van een discovery-scan op het netwerk.

Het eindresultaat van deze fase resulteert in een totaaloverzicht van alle op het netwerk aangesloten IT-middelen, zoals firewalls, servers, besturingssystemen, containers, virtuele machines, routers, printers, laptops, desktops en switches. Belangrijk hierbij is dat alle netwerksegmenten voor de discovery-scan bereikbaar en toegankelijk zijn.

De IT-omgeving van een organisatie is vaak een dynamische omgeving, waarin nieuwe componenten worden aangesloten. Hierdoor is een éénmalige scan niet voldoende, maar zal deze regelmatig uitgevoerd moeten worden. Vooral in (cloud) omgevingen waar gebruik gemaakt wordt van “vluchtige containers” (zoals MS Azure, Google Kubernetes, etc.) is discovery en registratie erg belangrijk om te weten wat er gescand moet worden.

Om ervoor te zorgen dat de discovery-fase effectief blijft in een veranderende IT-omgeving, is het cruciaal om nauw samen te werken met alle betrokken afdelingen. Het betrekken van netwerkbeheerders, systeembeheerders en applicatie-eigenaren zorgt ervoor dat wijzigingen in de IT-infrastructuur tijdig worden gecommuniceerd en de CMDB en discovery-scans up-to-date blijven.

4.3.1 CMBD-integratie

Voor een optimaal kwetsbaarhedenbeheer proces is een correct en volledig gevulde CMDB een randvoorwaarde. Het voeren van een CMDB is een standardaard onderdeel van IT-beheerprocessen en geen onderdeel van kwetsbaarhedenbeheer zelf, desondanks wordt het onderwerp hier toch kort aangeraakt.

Het is verstandig om de resultaten van de discovery-scan te gebruiken om de inhoud van de CMDB te valideren en waar nodig aan te vullen. Het is van groot belang om een controle uit te voeren of een door de discovery gevonden component die niet in de CMDB is geregistreerd is, een legitieme component is. Een van de aanvalsvectoren is een aanvaller die een geprepareerd apparaat ongeautoriseerd in de ICT-infrastructuur aanbrengt om als toegangspoort tot de ICT-infrastructuur te gebruiken. Richt dus binnen de organisatie een proces in dat zorgt voor een controleslag op de CMDB bij het toevoegen van nieuwe componenten zodat alleen geverifieerde componenten worden toegevoegd. Het automatisch opnemen zonder controleslag, *en daarmee het component automatisch als legitiem aan te merken*, is ten zeerste af te raden.

Daarnaast is het aanbevolen om een geautomatiseerd en geïntegreerd proces te implementeren dat zorgt voor voortdurende monitoring, validatie en bijwerking van de IT-middelen, een CMBD-beheer- / componentmanagementproces. Dit vermindert niet alleen de kans op menselijke fouten, maar draagt ook bij aan het verbeteren van de efficiëntie van het gehele kwetsbaarhedenbeheer-proces. Door regelmatig discovery-scans uit te voeren en de resultaten te vergelijken met de CMDB, kan een organisatie zowel de nauwkeurigheid van haar componentinventaris als de effectiviteit van haar beveiligingsmaatregelen waarborgen.

4.3.2 Best practices

- Werk samen en maak afspraken binnen de organisatie: Werk nauw samen met systeem-, applicatie- en proceseigenaren om vast te stellen wat wel en vooral ook wat niet gescand zal gaan worden. Maak voor componenten die niet gescand worden afspraken hoe hierop kwetsbaarheidsbeheer wordt uitgevoerd, wie hiervoor verantwoordelijk is en richt hiervoor een rapportagelijn in.
- CMDB-vulling automatiseren: Automatiseer het proces om de CMDB bijgewerkt te houden zoveel mogelijk (hoe groter de organisatie, hoe lastiger het wordt om dit handmatig te regelen).

4.4 Identificeren

Gedurende de stap *Identificeren* worden alle in de ICT-infrastructuur bekende componenten met behulp van een kwetsbaarhedenscanner onderzocht op de aanwezigheid van bekende kwetsbaarheden. Gevonden kwetsbaarheden worden automatisch verzameld[2] volgens een gestandaardiseerde conventie[3] en geprioriteerd op basis van het Common Vulnerability Scoring System (CVSS)[4].

In de discovery-fase is al aangegeven dat sommige componenten misschien buiten de scan moeten worden geplaatst. In de identificatiefase is de overweging belangrijk dat door het scannen van kwetsbaarheden de kans bestaat dat systemen of de elementen ervan verstoord raken. Om verstoringen te voorkomen, kunnen vaak verschillende scanprofielen worden gedefinieerd met verschillende intensiteit zodat de kans op verstoring kleiner is. Andere overwegingen bij het samenstellen van profielen en de scheduling van scans is bijvoorbeeld dat wanneer de netwerkbandbreedte een uitdaging is, kan besloten worden netwerkscans uit te voeren tijdens daluren wanneer vaak meer netwerkbandbreedte beschikbaar is.

2 NVD - Home (nist.gov)
3 CVE - CVE (mitre.org)
4 Common Vulnerability Scoring System SIG (first.org)

Als kwetsbaarhedenbeheer in de basis is ingericht, kan voor een volgende stap in volwassenheid worden gedacht aan het optimaliseren van de effectiviteit van scanning. Om de effectiviteit van de Identificatiefase te optimaliseren, is het raadzaam om gebruik te maken van meerdere kwetsbaarhedenscanners die verschillende soorten kwetsbaarheden en technologieën kunnen detecteren. Het scannen van OT-omgevingen (Operational Technology), of bijvoorbeeld applicaties, vereist een andere scanmethode en scanner dan een IT-omgeving. Dit kan helpen bij het identificeren van zwakke punten die mogelijk door één enkele scanner over het hoofd worden gezien. Daarnaast is het belangrijk om de scanners up-to-date te houden met de nieuwste beveiligingsinformatie en updates om ervoor te zorgen dat ze in staat zijn om de meest recente kwetsbaarheden te detecteren.

4.4.1 Best practices

- Bijhouden kwetsbaarheden update-packs: Voorzie scanners altijd van de meeste recente kwetsbaarhedenupdates zodat de nieuwste kwetsbaarheden kunnen worden gedetecteerd.
- Handmatig doorvoeren kwetsbaarhedenupdates: Voor de kwetsbaarhedenupdates handmatig uit (niet geautomatiseerd) en beoordeel de updates goed zodat er niet onverwacht verstorende elementen worden geïntroduceerd die mogelijk kritische processen kunnen verstoren.
- Scan zoveel mogelijk typen IT-componenten: Zorg dat je alle type assets kan scannen die in jouw omgeving van toepassing zijn. Zet hier eventueel meerdere types scanners voor in als dat noodzakelijk is.
- Registreer uitzondering op het scanproces: Scan zoveel mogelijk componenten en registreer welke componenten niet worden gescand. Deze componenten vormen in principe een risico en dienen als zodanig in een risicobeheersingsproces behandeld te worden.
- Publiek blootgestelde diensten eerst: Voer in ieder geval voor Internet gekoppelde componenten additionele applicatieve kwetsbaarhedenscans uit.
- Scan slim, voorkom brede impact: Houd rekening met de netwerk architectuur bij het scannen.
    - Zet in afgezonderde netwerksegmenten zoveel mogelijk centraal gestuurde maar lokale scanners neer zodat niet door firewalls heen hoeft te worden gescand.
    - Plaats scanners, waar van toepassing, geografisch dicht bij de componenten die moeten worden gescand om bandbreedte onder controle te houden.
    - Houd rekening met beschikbare bandbreedte bij het schedulen van scans en zorg dat op basis van mogelijke (over) belasting de juiste tijdsloten worden gekozen voor verschillende componenten/segmenten.
- Informeer de omgeving: Zorg dat de scanners bekend zijn in de detectietechnologieën waar ze kunnen worden uitgesloten; dit voorkomt ruis en false positives.
- Plan scanning uitvoering: Kijk goed naar de mogelijkheden van de scan-frequentie. Continu scannen heeft lang niet altijd zin. Houd rekening met mogelijke netwerkoverbelasting, maar ook met interne procedures zoals oplostijden (elke dag dezelfde kwetsbaarheden vinden terwijl afgesproken oplostijden (bijv.) weken tot maanden betreft, heeft weinig toegevoegde waarde.

4.5 Beoordelen

De fase *beoordelen* houdt zich bezig met het inschatten van de risico's met betrekking tot de gevonden kwetsbaarheden. Na het prioriteren worden ze toegewezen aan de juiste entiteit binnen de organisatie om opgelost te kunnen worden. Om de prioriteit goed vast te kunnen stellen, is het verstandig om de gevonden kwetsbaarheden: 1) te contextualiseren, daarna 2) een risico inschatting te maken, om ze dan te 3) prioriteren waarna ze kunnen worden 4) toegewezen. Dit is de fase waarin de gestandaardiseerde CVSS score wordt heroverwogen en aangepast naar de context van uw organisatie omdat de standaard scores een goed vertrekpunt zijn maar nooit de volledige context kunnen bevatten.

4.5.1 Contextbepaling

Met duiding wordt bedoeld dat de gevonden kwetsbaarheden kunnen worden geplaatst en uitgelegd binnen de context van het systeem, de applicatie en/of bedrijfsproces waar het gevonden is. Ook worden incorrecte bevindingen (false positives) uitgefilterd. Een ander belangrijk onderdeel van deze fase is het uitlegbaar maken van een technische kwetsbaarheid naar de eigenaar van het component waarop het is vastgesteld. Kwetsbaarheden zijn vaak heel technisch van aard en vaak niet helder beschreven. Het uitlegbaar maken voor niet-specialisten is van groot belang om het belang helder uiteen te kunnen zetten.

De gevonden kwetsbaarheden worden bekeken en beoordeeld door een specialist. In eerste instantie worden incorrecte bevindingen uitgefilterd. Daarna worden de kwetsbaarheden verrijkt met diverse informatiecomponenten vanuit, onder andere, de CMDB en de eigenaar, om hierna een gedegen risico-inschatting te kunnen doen.

Voor een goede risicobeoordeling is het verstandig om vooraf de nodige informatie beschikbaar te verzamelen:

- Van welk bedrijfsproces is dit systeem onderdeel en is dit een kritisch bedrijfsproces (BIV-waarde);
- Wat is de rubricering van de informatie op dit systeem (VIRBI[5]);
- Bevat het systeem vertrouwelijke of persoonsgegevens en zo ja, hoeveel;
- Wie is de eigenaar het proces en de beheerder van het systeem? (De beheerder kan ook een leverancier zijn);
- Wat is de fysieke of logische locatie van het systeem? (i.v.m. beheerteams op verschillende locaties); en,
- In welke netwerkzonering zit dit component? (Extern toegankelijk/perimeter, DMZ, in datacenter maar alleen intern bereikbaar, OTA-omgeving, kantoor netwerk, etc.).

4.5.2 Risicobeoordeling & Prioritering

Als verrijking met de juiste contextinformatie heeft plaatsgevonden, kan het SOC de inschatting doen van het risico dat met deze kwetsbaarheden samenhangt. Om dit goed te kunnen beoordelen, wordt naar kans en effect gekeken. Overweeg gebruik te maken van de CVSS-calculator[6] waarbij rekening wordt gehouden met zowel technische als omgevingskenmerken om tot een goede beoordeling te komen. Hierbij kunnen per keer de o.a. de volgende overwegingen worden gemaakt.

Kans:

- Is dit een daadwerkelijke kwetsbaarheid of is het slechts een false positive?

[5] wetten.nl - Regeling - Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) - BWBR0033507 (overheid.nl)
[6] NVD - CVSS v3 Calculator (nist.gov)

- Heeft het NCSC een beveiligingsadvies voor de gevonden kwetsbaarheid gepubliceerd en zo ja, hoe is deze geclassificeerd?
- Hoe makkelijk is het deze kwetsbaarheid te exploiteren?
- Kan deze kwetsbaarheid vanaf extern/remote worden geëxploiteerd of is lokale toegang vereist?
- Zijn er al tools of scripts beschikbaar om deze kwetsbaarheid te misbruiken (exploit-code)?
- Wordt de kwetsbaarheid al misbruikt binnen de eigen organisatie en kunnen hier Indicators Of Compromise (IOC's) uit worden gedestilleerd.
- Wordt deze kwetsbaarheid elders al misbruikt of wordt dit op korte termijn verwacht?
- Is dit een nieuwe kwetsbaarheid, en hoe lang bestaat deze al in het netwerk? (Oudere kwetsbaarheden hebben vaak al exploits beschikbaar en vormen dus een hoger risico).
- Welke toegang is er nodig om de kwetsbaarheid te misbruiken?
- Zijn er credentials nodig om de kwetsbaarheid te misbruiken?
- Zijn er handelingen van gebruikers nodig om de kwetsbaarheid te misbruiken?

Impact:

Voor het bepalen van de impact zijn vier hoofdvragen van belang:

1. Hoe omvangrijk is de kwetsbaarheid: op hoeveel systemen, apparaten, diensten en processen heeft deze kwetsbaarheid potentieel impact?

2. Levert de kwetsbaarheid een risico op voor de beschikbaarheid bijvoorbeeld door verstoringen van het systeem en zo van de uitvoering van de processen.

3. Levert de kwetsbaarheid een risico op voor de integriteit van de gegevens en verloop van processen en daarmee voor onjuiste en missende gegevens, bijvoorbeeld door toepassing van ransomware en beschadigen van backups

4. Levert de kwetsbaarheid een risico op voor de vertrouwelijkheid van gegevens, bijvoorbeeld door datadiefstal en datalekken.

5. Resulteert de kwetsbaarheid in mogelijke impact op fysieke veiligheid.

Voor het bepalen van de impact kan verdere diepgang worden bereikt met behulp van een aantal verdiepingsvragen:

- Levert de kwetsbaarheid een risico voor rechtenescalatie (privilege escalation)
- Levert de kwetsbaarheid een risico op tot het uitvoeren van willekeurige code?
- Hoe veel componenten worden getroffen door deze kwetsbaarheid?
- Is de veiligheid van andere systemen afhankelijk van de veiligheid van betreffende component c.q. systeem waarin de kwetsbaarheid is gevonden?
- Bestaat er een ketenafhankelijkheid voor één of meer processen met betrekking tot een kwetsbaar systeem.
- Is er een patch beschikbaar?
- Zijn er al maatregelen geïmplementeerd op het netwerk die het risico of de impact van de kwetsbaarheid mitigeren?
- Wat zijn de gevolgen indien de informatie in dit systeem niet toegankelijk is of als de informatie uit het betreffende systeem gelekt wordt, verloren of gemanipuleerd raakt. Denk hierbij aan:

    - Impact op de uitvoering van wettelijke taken.
    - Maatschappelijke impact en zo ja met welke omvang?
    - Bestuurlijke c.q. politieke commotie.
    - Wat zijn eventuele gevolgen van negatieve pers, reputatieschade, klantverlies, etc?
    - Financiële impact.

Uiteindelijk levert de combinatie van kans en impact een geprioriteerde lijst van kwetsbaarheden op, die via aan de juiste partij dienen te worden toegewezen.

4.5.3 Toewijzing

Als laatste dienen de kwetsbaarheden toegewezen te worden aan de juiste partij binnen de organisatie volgens de bestaande interne procedures zodat deze kan worden verholpen. Het is verstandig om dit via een geautomatiseerd softwaresysteem te doen (bijv. een ISMS-toepassing) zodat registratie, toewijzing, oplossing en terugkoppeling allemaal zijn geborgd. Als de toewijzing correct en geautomatiseerd is belegd, wordt het maken van rapportages ook sterk vereenvoudigd waarbij het mogelijk zou moeten zijn om dashboards van de huidige stand van zaken te maken.

4.5.4 Best practices

- Elimineer foutieve meldingen: Door technische beperkingen van scantooling worden ook dingen gevonden die mogelijk geen kwetsbaarheid zijn, of met opzet op een bepaalde wijze zijn geconfigureerd. Niet elke gevonden kwetsbaarheid is dus ook een echte kwetsbaarheid. Dit kan bijvoorbeeld afhangen van software versienummers;
- Bepaal risicocontext: Beoordeel risico binnen context, niet elke technische kwetsbaarheid is automatisch een risico en de prioriteitsbepaling vanuit de kwetsbaarhedenscanner is niet automatisch het risiconiveau voor de organisatie. Zo is bijvoorbeeld een web server in een test omgeving mogelijk veel minder belangrijk dan in een productieomgeving;
- Verschaf heldere uitleg aan oplossende partij: Maak de technische kwetsbaarheden uitlegbaar zodat niet-technische collega's snel en eenvoudig kunnen begrijpen wat met welke prioriteit dient te worden opgepakt;
- Automatiseer het kwetsbaarhedenbeheer proces: Automatiseer registratie, toewijzing, oplossing en terugkoppeling zodat het huidige risiconiveau altijd snel inzichtelijk kan worden gemaakt.

4.6 Oplossen

In deze fase wordt de gevonden kwetsbaarheden opgepakt door de eigenaren of gedelegeerde beheerders van het betreffende (informatie)systeem.

Afhankelijk van de organisatie is de informatie, applicatie, proces of systeemeigenaar verantwoordelijk voor het (laten) oplossen van gevonden kwetsbaarheden. Het oplossen dient te gebeuren binnen de tijdslijnen die hiervoor in het beleid zijn vastgelegd. De taken voor het technisch oplossen van de kwetsbaarheden kunnen door de eigenaar worden gedelegeerd aan beheer afdelingen of externe leveranciers. Het is noodzakelijk om beheerafspraken met zowel interne afdelingen als externe partijen vast te leggen. Afspraken met interne organisaties worden over het algemeen in OLA's (Operating Level Agreements) vastgelegd, terwijl afspraken met externe partijen in SLA's (Service Level Agreements) zijn vastgelegd.

Indien de kwetsbaarheid niet binnen de gestelde oplostijd kan worden verholpen, door bijv. ontwikkel- en testtijden, dient dit binnen het risicoproces te worden opgevolgd. Daarnaast zal het risicoproces ook voorzien in het accepteren van risico's en het maken van uitzonderingen met bijbehorende looptijden. Het is vooral belangrijk dat deze zaken duidelijk in het organisatiebeleid is vastgelegd.

4.6.1 Best practices

- Neem kwetsbaarhedenbeheer op in uitbestedingscontracten: Bij uitbesteding van IT-dienstverlening dient het beleid te reflecteren in de overeenkomsten met leveranciers zodat verantwoordelijkheden, rapportages en consequenties vooraf helder zijn uitgesproken.

- Uitbestedingscontracten bevatten oplostijden en patchbeleid: Binnen deze processen dient opgenomen te zijn dat het verhelpen van kwetsbaarheden samen moet gaan met het regelmatig en gepland patchen van IT-componenten. Dit voorkomt frequente ad-hoc patching en het oplossen van kwetsbaarheden op een issue voor issue basis. Uitzonderingen hierop zijn kwetsbaarheden die dusdanig kritisch zijn dat ze direct risico voor de organisatie opleveren. Wat hiervoor de criteria zijn, dient ook in beleid te zijn vastgelegd.

4.7 Verifiëren

In deze fase van het proces vindt terugkoppeling en controle plaats. De (gedelegeerd) verantwoordelijke voor het oplossen van een kwetsbaarheid is ook verantwoordelijk voor het geven van terugkoppeling over de stand van zaken. Daarnaast worden in vervolgscan rondes de verschillende componenten opnieuw onderzocht op kwetsbaarheden waarmee een automatische controle gebeurt op de terugkoppeling die is geleverd.


Verifiëren

Afhankelijk van de behoefte binnen een organisatie, kan een oplospartij ook ad-hoc controle scans aanvragen als specifieke werkzaamheden zijn verricht. Verder kunnen tussentijdse ad-hoc scans worden uitgevoerd op basis van, bijvoorbeeld, lopende incidenten waarbij specifieke kwetsbaarheden voor de organisatie zo kritisch kunnen zijn dat kort cyclische scans nodig zijn voor de bewaking van voortgang.

4.7.1 Best practices

- Terugkoppeling is belegd binnen het proces: Zorg dat terugkoppeling is vastgelegd binnen het risicoproces.

- Geautomatiseerde verificatie: Zorg dat het toetsen van opgeloste kwetsbaarheden automatisch wordt uitgevoerd binnen het scan-proces.

4.8 Rapporteren

Meten is weten! Dit maakt de rapportage binnen het kwetsbaarhedenbeheerproces een uiterst belangrijk onderdeel. Om goed te kunnen rapporteren is het van belang dat scherp beleid is geformuleerd zowel betreft risicobeheersing als ook voor kwetsbaarhedenbeheer. Binnen dit beleid worden processen en oplostijden vastgelegd. Als dit goed is beschreven wordt het meten van de processen middels indicatoren en statistieken, en het rapporteren hierover eenvoudiger.


Rapporteren

4.8.1 Indicatoren en statistieken

Indicatoren dienen in beleid te zijn geformuleerd op basis van risiconiveau, oplostijden, uitzonderingen met bijbehorende voorwaarden, en risicoprofiel van de organisatie. Als deze onderdelen goed zijn geformuleerd, kan hier bij het implementeren van de processen en het kiezen van de technische oplossingen rekening mee worden gehouden.

- Indicatoren en statistieken: Bepaal op basis van het beleid en het risicoprofiel van de organisatie wat de juiste prestatie indicatoren zijn en welke statistieken interessant zijn om te meten in relatie tot processen en het risicoprofiel.

- Data: Bij het vaststellen van “wat” te meten is het van groot belang om stil te staan bij “hoe” dit te meten. Het heeft weinig zin om allerlei statistieken en indicatoren op te stellen waarbij het op voorhand al duidelijk is dat de juiste data niet beschikbaar is. Tegelijkertijd

is het van belang om te bepalen wat de organisatie zou willen meten zodat dit als eisen en wensen mee kan worden genomen bij het bepalen van de juiste technische implementatie.

Bekijk op basis van het beschreven beleid wat de juiste risico indicatoren (KRI) en prestatie indicatoren (KPI) zijn. Houdt hierbij in het achterhoofd dat prestatie indicatoren de beschreven processen zouden meten en dat de risico indicatoren aangeven welke prioriteiten de organisatie zou moeten stellen. Een aantal bruikbare indicatoren zijn in een eerder document beschreven[7] en kunnen verder worden aangevuld op basis van organisatiebeleid.

4.8.2 Rapportage en communicatie

De verschillende indicatoren en statistieken dienen in verschillende vormen samengebracht te worden om in de communicatie met verschillende stakeholders binnen de organisatie te voorzien. Houd bij het samenstellen van de verschillende rapportages rekening met de doelgroep en boodschap die overgebracht moet worden. Voor verschillende doelgroepen zijn in Tabel 1 verschillende aandachtsgebieden benoemd.

Stakeholder	Verantwoordelijkheid	Rapportagetype
SOC	Het SOC is verantwoordelijk voor de dagelijkse gang van zaken en heeft voornamelijk operationele informatie nodig om het scannen en oplossen van kwetsbaarheden in goede banen te leiden.	Aantal kwetsbaarheden opgedeeld naar prioriteit.
		Aantal kwetsbaarheden per prioriteit opgedeeld naar eigenaar.
		Openstaande kwetsbaarheden en doel oplosdatum.
		Openstaande kwetsbaarheden die de afgesproken oplostijd hebben overschreden.
	De CISO heeft voornamelijk samenvattende informatie nodig om te kunnen sturen en eventueel escaleren. Daarnaast heeft de CISO inzicht nodig over de risico-posture van de organisatie.	Aantal openstaande kritische en hoge prioriteit kwetsbaarheden voor de hele organisatie en opgedeeld naar eigenaar.
		Lange termijn trend betreft de aanwezigheid en oplostijden van kwetsbaarheden.
		Overzicht van belangrijke kwetsbaarheden die resulteren in een direct risico voor de organisatie.
		Oplostijden, en overschrijdingen hiervan, opgedeeld naar eigenaar.
	Proceseigenaren zijn eigenaar van en verantwoordelijk voor kwetsbaarheden en bijbehorende risico's die betrekking hebben op de IT-componenten binnen hun verantwoordelijkheidsgebied.	Kwetsbaarheden opgedeeld naar prioriteit en IT-component.
		Oplostijden, en overschrijdingen hiervan, voor de verschillende kwetsbaarheden relevant voor hun IT-domein.
		Trendrapportages die betrekking hebben op doorlooptijden van het oplossen van kwetsbaarheden.

[7] Centrale SOC-voorziening – Strategische aanbevelingen (2023, VSSR)

Stakeholder	Verantwoordelijkheid	Rapportagetype
		Overzicht van bestaande, gemitigeerde en geaccepteerde risico's met betrekking tot kwetsbaarheden.
	Afhankelijk van de organisatie zijn er mogelijk één of meerdere externe partijen waarvoor een meldplicht bestaat. Breng dit voor de eigen organisatie in kaart.	Welke zaken dienen te worden gerapporteerd zal afhankelijk zijn van de organisatie waaraan gerapporteerd moet worden. Stel dit per keer vast.

Tabel 1 Doelgroepen & aandachtsgebieden

Een belangrijk onderdeel van rapportage is communicatie. Als het mogelijk is, zorg dan dat het SOC een digitale portal heeft waar alle informatie in de vorm van een dashboard per stakeholder beschikbaar wordt gesteld, waarbij rekening is gehouden met het type rapportage dat de stakeholder nodig heeft. Stel in het dashboard ook statusrapportages beschikbaar zodat deze documenten niet bijv. maandelijks naar mailboxen worden verstuurd. Ga daarnaast ook regelmatig met de verschillende stakeholders in gesprek om rapportages op essentiële onderdelen toe te lichten en om te zien of deze aansluiten bij de behoefte van de stakeholder.

4.8.3 Best practices

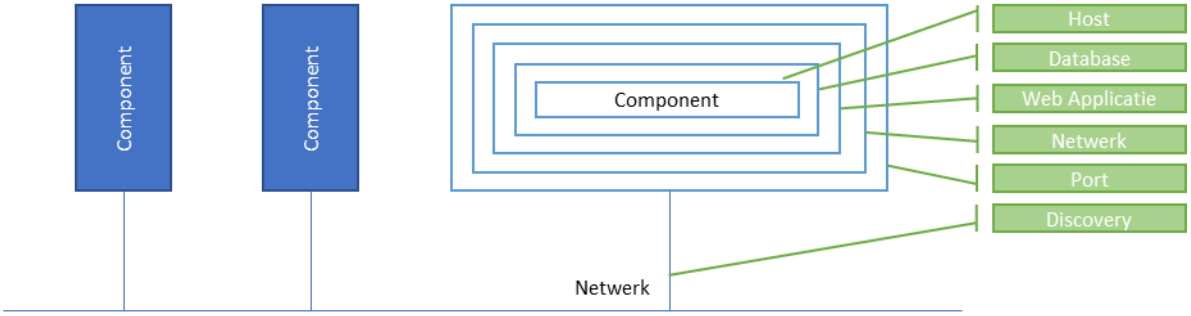
- Indicatoren vastgesteld in beleid: Zorg dat helder beleid aanwezig is om indicatoren op in te richten.
- Meet proces en risico: Meet processen en risico om goed te kunnen sturen.
- Communiceer met stakeholders: Zorg voor heldere communicatie via periodieke rapportage en dashboards die de meest recente stand van zaken weergeven.

Bijlage I – Toelichting kwetsbaarhedenscan methoden

In hoofdlijnen kan kwetsbaarheden scanning in een aantal typen worden opgedeeld:

1. Discovery scan;
2. Poort scan;
3. Netwerk kwetsbaarheden scan;
4. Web Application kwetsbaarheden scan;
5. Host-based kwetsbaarheden scan;
6. Database kwetsbaarheden scan;
7. Source Code kwetsbaarheden scan;
8. Cloud kwetsbaarheden scan.

De verschillende typen scans kijken telkens een laagje dieper in het systeem om zo alle onderdelen onder de loep te nemen waardoor een compleet beeld van alle kwetsbaarheden ontstaat. Een schematisch overzicht is hieronder in Figuur 3 weergegeven.



Figuur 3 Schematisch weergave scan-types

Discovery Scan

Een discovery scan is bedoeld om snel en efficiënt alle componenten in de IT-infrastructuur in kaart te brengen. Dit type scan kijkt nog niet naar kwetsbaarheden maar is wel essentieel om te weten hoe de IT-infrastructuur erbij ligt en kan worden gebruikt om een controle uit te voeren op de component database van de organisatie. In veel gevallen worden tijdens de discovery scan veel componenten gevonden die niet in de component database zijn opgenomen.

Poort-scan

Scannen van de IT-infrastructuur op open poorten op componenten in het netwerk. Een open poort op een IT-component is een ingang op een systeem waar een service op wordt aangeboden. Een van de meest bekende diensten op het Internet is een web-service. Hier worden websites op aangeboden die met een browser kunnen worden opgevraagd. Deze service wordt typisch via poorten 80 (niet versleuteld) en 443 (versleuteld) aangeboden via webserver software.

Netwerk kwetsbaarheden scan

Als eenmaal is vastgesteld welke poorten beschikbaar zijn op een component en welke service via deze poort wordt aangeboden, is de volgende stap om per service vast te stellen welke bekende kwetsbaarheden aanwezig zijn. Effectief gezien wordt de server software, welke de service aanbiedt, gecontroleerd op bekende kwetsbaarheden. Daarnaast wordt vaak ook direct gekeken of

er valide accounts kunnen worden gevonden die toegang geven tot afgeschermde delen van de website.

Web Applicatie kwetsbaarheden scan

Web applicaties zijn vaak publiek beschikbaar op het internet en zijn dus continu blootgesteld aan dreigingsagenten. Hierdoor zijn dit type applicaties kwetsbaarder dan applicaties die afgeschermd van het internet zijn opgesteld (bijvoorbeeld binnen de kantoorautomatiseringsinfrastructuur). Daarnaast zijn er specifieke kwetsbaarheden die voornamelijk van toepassing zijn op dit type applicaties en die veelal voortkomen uit coderingsfouten en veel minder zijn gerelateerd aan de onderliggende software waar de kwetsbaarheden veelal op worden gevonden en geclassificeerd. Dit type kwetsbaarheden vereist dan ook een eigen manier van scanning waar speciale software voor nodig is. Meer informatie over web applicatie fouten en kwetsbaarheden is terug te vinden op de OWASP web site[8].

Host-Based kwetsbaarheden scan

Bij deze vorm van scanning wordt veelal op systemen zelf gekeken naar mogelijke kwetsbaarheden met behulp van een lokaal geïnstalleerde agent. Dit type scan geeft veelal meer detail informatie over het systeem (informatie die met scans van buitenaf niet te verkrijgen is) en biedt ook de mogelijkheid om meer gedetailleerde informatie zoals, versienummers van software, te verkrijgen.

Database kwetsbaarheden scan

Een database scan wordt in principe alleen uitgevoerd op database systemen en kijkt naar specifieke kwetsbaarheden en configuratiefouten die bij databases kunnen voorkomen. Dit zijn heel specifieke scans die lang niet overal worden uitgevoerd en zijn alleen van toepassing op een kleine subset van IT-componenten.

Source Code kwetsbaarheden scan

Dit type scans wordt vaak uitgevoerd als onderdeel van een software development life-cycle (SDLC) om te zien of in specifieke programmeerfouten voorkomen in de broncode van software. Dit type scan is heel specifiek en eigenlijk alleen van toepassing in ontwikkelstraten voor software. Voor veel organisaties (die vooral software afnemen en gebruiken) is dit niet van toepassing.

Cloud kwetsbaarheden scan

Een kwetsbaarheden scan op de Cloud-infrastructuur is in principe niet anders dan andere scans maar is specifiek gericht op Cloud-infrastructuur. Naast de reguliere scan onderdelen zijn er een aantal componenten die specifiek op Cloud-infrastructuur van toepassing zijn[9].

[8] OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation

[9] https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

Bijlage II – Cheatsheet randvoorwaarden en best practices

<table>
<tr><td colspan="2">Randvoorwaarden

• Zorg voor beleid op administratie IT-middelen;
• Zorg voor beleid op risicobeheersing en kwetsbaarhedenbeheer;
• CMDB volledig en correct gevuld.</td></tr>
<tr><td>Discovery

• Werk samen en maak afspraken binnen de organisatie;
• CMDB vulling automatiseren.</td><td>Identificeren

• Bijhouden kwetsbaarheden update-packs;
• Handmatig doorvoeren kwetsbaarhedenupdates;
• Scan zoveel mogelijk typen IT-componenten;
• Registreer uitzondering op het scanproces;
• Publiek blootgestelde diensten eerst;
• Scan slim, voorkom brede impact;
• Informeer de omgeving;
• Plan scanning uitvoering.</td></tr>
<tr><td>Beoordelen

• Elimineer foutieve meldingen;
• Bepaal risicocontext;
• Verschaf heldere uitleg aan oplossende partij;
• Automatiseer het kwetsbaarhedenbeheer proces.</td><td>Oplossen

• Neem kwetsbaarhedenbeheer op in uitbestedingscontracten;
• Uitbestedingscontracten bevatten oplostijden en patchbeleid.</td></tr>
<tr><td>Verifiëren

• Terugkoppeling is belegd binnen het proces;
• Geautomatiseerde verificatie.</td><td>Rapporteren

• Indicatoren vastgesteld in beleid;
• Meet proces en risico;
• Communiceer met stakeholders.</td></tr>
</table>

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://vssr.rijksapplicaties.nl/

vssr.info@minjenv.nl

Maart 2024