Hoe te werken met

Vulnerability Management

Whitepaper door SecurityHive

SECURITYHIVE

Inhoudsopgave

Inleiding

Wat klinkt beter: proactief potentiële bedreigingen bestrijden of zwoegen om de problemen op te lossen nadat een succesvolle aanval op je systeem heeft plaatsgevonden? Aangezien cyberaanvallen steeds complexer en gerichter worden, is proactief reageren belangrijker dan ooit. Vulnerability Management is de beste manier om het risico te minimaliseren voordat het te laat is. In deze Whitepaper beschrijven we hoe je kunt werken met Vulnerability Management.

1. Wat is Vulnerability Management?

Door een fout in de hardware of software van een bedrijf kan er een zwakte in je systeem zijn. Deze kwetsbaarheid zorgt ervoor dat het systeem blootstaat voor potentiële risico's. Vulnerability Management is een continu proces. Het is er niet alleen voor gemaakt om risico's in het netwerk te detecteren, maar ook om een plan te maken hoe deze risico's in de toekomst geen schade kunnen aanrichten. Om Vulnerability Management het meest effectief in te kunnen zetten, kun je het beste de technologie combineren met een team van beveiligingsexperts. Zo kan er proactief gereageerd worden op het detecteren van beveiligingsrisico's en kan hier op de juiste manier mee om worden gegaan.

Een nieuw incident dat potentie heeft om het systeem te beschadigen

Een kwetsbaarheid van een apparaat dat hackers kunnen exploiteren

De kans om schade te lijden wanneer de kwetsbaarheid misbruikt wordt

2. Vulnerability Management vs. Patch Management

Hoewel de termen vaak met elkaar worden gebruikt, zijn Vulnerability Management en Patch Management niet hetzelfde. Patch Management is het proces dat wordt gebruikt om de software en besturingssystemen bij te werken. Dit kunnen nieuwe functies zijn of beveiligingsoplossingen. Met een Patch Management systeem kun je ontbrekende patches op een asset markeren, classificeren en prioriteren.

Vulnerability Management omvat veel meer dan scannen en patchen. Er wordt hierbij een veel bredere kijk verwacht, om weloverwogen beslissingen te kunnen nemen over welke kwetsbaarheden als eerste moeten worden aangepakt. Ook moet er worden gekeken hoe deze beveiligingsrisico's kunnen worden verminderd.

3. Waarom is Vulnerability Management belangrijk?

Het aantal kwetsbaarheden neemt toe. In 2021 werden er wekelijks 446 bedrijven getroffen in Nederland. Dit is een stijging van 86% ten opzichte van het jaar daarvoor. Volgens het trend rapport van Gartner zet deze stijging komende jaren ook door. Bedrijven hebben ook steeds meer apparaten op het netwerk aangesloten staan, waardoor het moeilijker wordt om alle netwerkkwetsbaarheden proactief aan te pakken. Maar, er zijn nog meer redenen waarom Vulnerability Management belangrijk is:

1. Constante updates en patches
Hardware- en softwareleveranciers zijn constant opzoek naar bugs en kwetsbaarheden in hun eigen platformen. Daarom sturen zij regelmatig updates en patches naar bedrijven. Werknemers kunnen hierop klikken om de pop-ups op hun computers te negeren. Hierdoor kan er een beveiligingsrisico ontstaan.

2. Meer geavanceerde aanvallen
Hackers zullen steeds meer geavanceerde, aangepaste aanvallen doen op bedrijven in plaats van de algemene aanvallen. De aanvaller zal actief opzoek gaan naar kwetsbaarheden in de netwerken van hun doelwitten. Deze kwetsbaarheden geven hackers meer mogelijkheden om succesvol toegang te krijgen tot je netwerk.

3. Branchevoorschriften
In veel branches zijn de laatste tijd regelgevingen gekomen waardoor bedrijven verplicht worden om een proces voor Vulnerability Management te hebben. Dit is een goede motivatie om als bedrijf een strategie op te stellen om de mogelijke bedreigingen proactief te bestrijden en daarop te reageren.

4. De vijf stappen van Vulnerability Management

Het typische proces voor Vulnerability Management is op te delen in meerdere fasen die zijn gericht op het analyseren, prioriteren en beschermen van je netwerk:

1. Ontdekken
De beginfase van het proces draait om het voorbereiden van de kwetsbaarheidsscan en -testen. Het is belangrijk om in deze stap alle bedrijfsmiddelen te organiseren en alle vergeten apparaten op te sporen. Verzamel alle onderdelen binnen het bedrijf die je moet testen en bepaal wat het belang van deze apparaten zijn. Ook kun je in deze fase kijken wie toegang heeft tot deze apparaten, zijn dat alleen de beheerders of het hele team?

2. Beoordelen
Na het verzamelen van alle apparaten moet er in deze stap voor gezorgd worden dat elk apparaat zowel nauwkeurig als efficiënt wordt gescand. Het gaat er niet alleen om dat de kwetsbaarheden naar boven komen, maar ook dat er een tijdige en efficiënte toegang is tot de informatie. Dat betekent dat de gegevens van een betrouwbare bron moeten komen. Zodra je inzicht hebt gekregen in de mogelijke risico's op de apparaten, is de volgende stap het prioriteren van de kwetsbaarheden. Het grootste risico moet als eerste worden opgelost.

Enkele factoren om te overwegen zijn:
- Hoe makkelijk kan iemand misbruik maken van deze kwetsbaarheid?
- Heeft de kwetsbaarheid gevolgen voor de beveiliging van ons product?
- Wat zou de zakelijke impact zijn als deze kwetsbaarheid wordt misbruikt?
- Beschikken we over bestaande beveiligingsprotocollen die de kans op het misbruiken van deze kwetsbaarheid verkleind?

3. Rapporteren
Alle gegevens over de kwetsbaarheden worden gecompileerd in een aangepast rapport. Hierin staan de details over de kwetsbaarheden en hoe deze geprioriteerd moeten worden. Het rapport bevat aanbevelingen over het beste plan om de risico's snel te kunnen beoordelen. De te nemen acties worden ook beschreven inclusief een stapsgewijze instructie over hoe het probleem opgelost moet worden. Het doel van het rapport is om de beveiligingsrisico's van de apparaten op een praktische manier te verminderen.

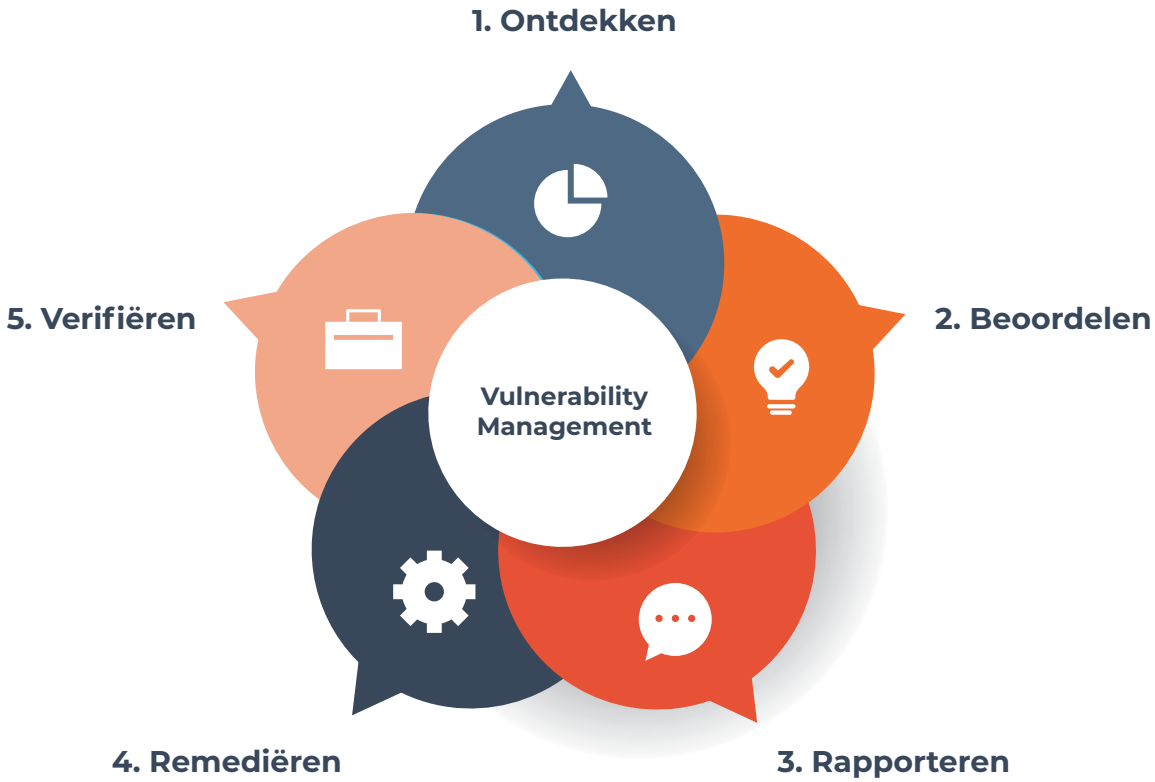
Er zijn drie algemene routes die je kunt nemen:
- **Remediëren:** het volledig voorkomen van een aanval door het patchen, corrigeren of vervangen van een code die een kwetsbaarheid bevat.
- **Mitigatie:** het verkleinen van de kans of impact van de kwetsbaarheid. Dit is meestal een tijdelijke oplossing die bedrijven gebruiken totdat de kwetsbaarheid definitief verholpen kan worden.

4. De vijf stappen van Vulnerability Management

- **Geen actie:** erkennen en accepteren van de kwetsbaarheid. Dit doen bedrijven vaak alleen als de kosten van het verhelpen van de kwetsbaarheid hoger zijn dan de kosten als gevolg van een succesvolle cyberaanval.

4. Remediëren
Zoals in stap 3 benoemd zijn er drie algemene routes die genomen kunnen worden. De meest ideale route is die van het remediëren. Wanneer kwetsbaarheden worden gedetecteerd en gerapporteerd, wordt in deze stap van het Vulnerability Management proces ervoor gezorgd dat de kwetsbaarheden worden gecorrigeerd en verwijderd. Dit kan bijvoorbeeld door een nodige update te draaien of door het patchen. Deze fase wordt vervolgens herhaald wanneer er nieuwe kwetsbaarheden worden ontdekt. Het netwerk en de apparaten moeten continu worden gecontroleerd op kwetsbaarheden die een potentiële dreiging zijn voor de beveiliging.

5. Verifiëren
De laatste stap is om het succes van het hele proces te verifiëren. Het doel van deze stap is dat je kunt zien dat de mitigatie succesvol was. Bovendien zorgt het ook voor transparantie en verantwoordelijkheid in het hele bedrijf. Dankzij Vulnerability Management wordt het 'aanvalsoppervlak' verkleind. Ook wordt er een manier gevonden om de dreiging van een aanval te minimaliseren door kwetsbaarheden te verminderen. Door van kwetsbaarheidsbeoordelingen een routinepraktijk te maken, krijg je inzicht in de doeltreffendheid en snelheid van het Vulnerability Management programma.



5. Wat is een Vulnerability Management programma?

Een programma voor Vulnerability Management is uniek ontworpen voor iedere organisatie. Er wordt rekening gehouden met:

• De beveiligingsbedreigingen waarmee het bedrijf wordt geconfronteerd
• De technologieën die het bedrijf gebruikt
• De juridische en geografische beperkingen
• De klant- en marktvereisten

Over het algemeen worden de volgende componenten toegevoegd in een succesvol Vulnerability Management programma:

• Kwetsbaarheidsbeoordeling
Vulnerability Management bouwt voort op de kennis die is opgedaan met de kwetsbaarheidsbeoordeling. Op basis hiervan worden effectieve maatregelen genomen om het risico en de impact te behandelen. Omdat de aanschaf van nieuwe technologieën en updates steeds weer bijbehorende risico's met zich meebrengen, is het belangrijk dat het programma blijvend zal evalueren tijdens de veranderingen in het bedrijf.

• Systematisch proces
In het programma zit vaak een formeel proces om de kwetsbaarheidsbeoordeling en de behandeling uit te voeren als een doorlopende activiteit. In dit proces worden de volgende onderdelen gevolgd en gedocumenteerd:
- Het beleid van het bedrijf
- De technologieën van het bedrijf
- De zakelijke operaties
- De inspanningen om nieuwe kwetsbaarheidsrisico's te verminderen

• 'Blind spot' detectie voor DevOps
"Je kunt niet beheren wat je niet kunt meten", zo luidt het gezegde. Het continu monitoren is een onderdeel van het Vulnerability Management programma. Dit is vooral belangrijk in de DevOps-omgevingen. Dit is een team samenstelling van Developers (ontwikkelaars) en Operations (beheer). In deze omgeving worden door de snelle veranderingen in de infrastructuurconfiguraties kwetsbaarheidsrisico's blootgelegd. Als deze nieuwe systemen niet worden gescand, kunnen kwetsbaarheden als blinde vlekken bestaan.

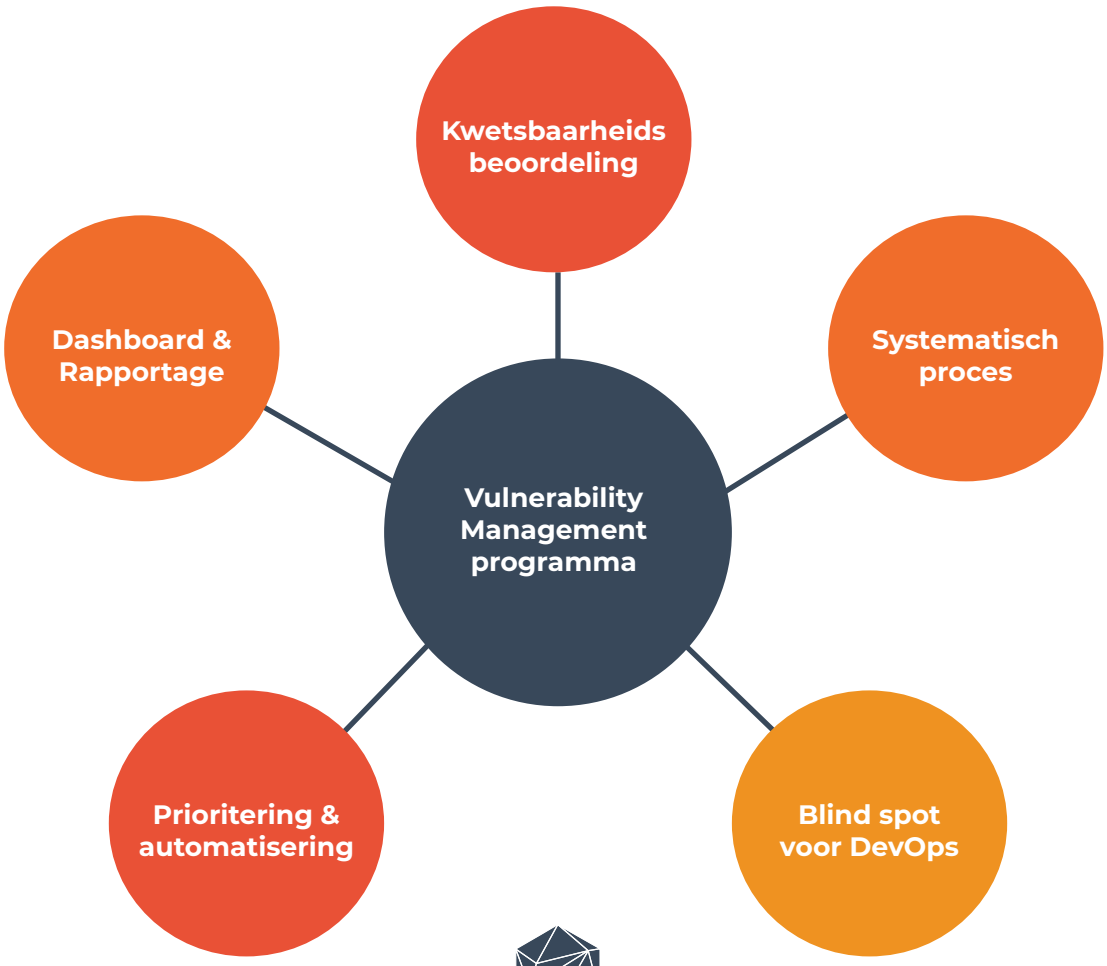
Geautomatiseerde detectiemogelijkheden helpen om de beveiligingsrisico's te ontdekken en te verhelpen. Dit gebeurt dankzij de installatie van beveiligingspatches.

5. Wat is een Vulnerability Management programma?

• Prioritering en automatisering
Het handmatig oplossen van een kwetsbaarheid kan veel inspanningen vergen binnen een bedrijf. Wanneer het continu moet worden herhaald wordt het steeds vatbaarder voor menselijke fouten. Een effectief Vulnerability Management programma bewaart beslissingen die genomen worden bij het behandelen van kwetsbaarheden en hergebruikt ze wanneer nieuwe kwetsbaarheden zich voordoen. Door herstelprocessen te automatiseren kunnen de beveiligingsrisico's worden geminimaliseerd met behulp van geavanceerde technologieën.

• Dashboard en rapportage
Oplossingen voor Vulnerability Management hebben toegang tot logbestanden van een uitgebreid netwerk en bewaken de infrastructuur continu. In een SecOps-team werken mensen die bezig zijn met Security (beveiligen) en Operations (beheer). Dit team kan overweldigd raken door de hoeveelheid informatie die beschikbaar is om beslissingen te kunnen nemen over het beheer van kwetsbaarheden.

Een gebruiksvriendelijk dashboard en rapportage zijn daarom belangrijke onderdelen voor het Vulnerability Management programma. Hierin wordt de juiste informatie over lopende kwetsbaarheidsbeoordelingen beschikbaar, wat bijdraagt aan een effectief herstelproces.



6. Hoe kies ik de juiste Vulnerability Management KPI's?

Met zoveel verschillende Vulnerability Management tools is het relatief eenvoudig om gegevens te krijgen over kwetsbaarheden. Alleen, door alles te beoordelen en te meten word je overspoeld door eindeloze grafieken en cijfers. Om Vulnerability Management effectief aan te pakken, moet de aandacht gericht worden op de cijfers die ertoe doen. De juiste statistieken zorgen ervoor dat je hackers een stap voor bent. Daarnaast is het tonen van de juiste cijfers ook de beste manier om belanghebbenden te overtuigen dat het Vulnerability Management programma de juiste middelen krijgt die je nodig hebt. Hieronder worden vijf belangrijke KPI's beschreven waarmee je aan die informatie kunt komen:

1. Dekking
Clouds, Microservices, Containers. Er zijn vast enkele van deze voorbeelden die onderdeel uitmaken van de inventaris van het bedrijf. Het is belangrijk om bij te houden wat je organisatie gebruikt, om te kunnen bepalen of het Vulnerability Management programma alle systemen dekt. Daarom is het goed om op de hoogte te zijn van de softwarefactuur (SBoM), om deze met succes te kunnen volgen en kwetsbaarheden aan te kunnen pakken die zich in het systeem bevinden.

2. Tijd tot detectie
Wat is de tijd die nodig is voordat je kwetsbaarheden in je systeem detecteert? Detectie is een belangrijke fase in het proces van Vulnerability Management. Om ervoor te zorgen dat je organisatie het goed doet, moet de gemiddelde tijd tot een detectie een van de meetgegevens zijn voor Vulnerability Management. In het programma zitten vaak 'Issue trackers'. Deze bevatten gegevens zoals het tijdstip van optreden van de kwetsbaarheden, het aantal kwetsbaarheden en het tijdstip van de detectie.

3. Tijd tot herstel
Deze meetgegevens tonen de tijd die nodig is om een gedetecteerde kwetsbaarheid te verhelpen. In de moderne programma's voor Vulnerability Management wordt het automatisch herstellen van kwetsbaarheden aangeboden. Dit helpt om kwetsbaarheden al snel en vroeg in de ontwikkeling op te lossen. Vaak is in het Vulnerability Management programma ook te zien op welke datum de kwetsbaarheid verholpen is.

4. Patchsnelheid
Dit is een iets ingewikkeldere indicator om te maken, maar kan toegepast worden om de strategie voor patchbeheer te verbeteren. Door het meten van de patchsnelheid kan er gezien worden hoeveel patches en correcties er in een bepaalde tijd zijn toegepast.

5. Activa risico's
Hoeveel gebruikers hebben beheerderstoegang? Hebben we activa die vatbaarder zijn voor beveiligingsproblemen waardoor de kans op een cyberaanval toeneemt? Deze informatiebeveiligingsstatistieken kunnen je vertellen welke activa de grootste zakelijke impact hebben. Door hierachter te komen kun je zien welke kwetsbaarheden prioriteit vragen als het gaat om herstel, tijd en financiële middelen.

OVER SECURITYHIVE

"Iemand heeft een slechte bijlage geopend"
mag nooit de reden zijn waarom het hele bedrijf niet kan werken.

SecurityHive - opgericht in 2017 door Nederlandse techneuten - ontwikkelt oplossingen om cybersecurity maximaal eenvoudig te maken. Het is ons doel om bedrijven een veilige toekomst te bieden en zo ongestoord te groeien. Het resultaat van onze visie is dat cybersecurity toepasbaar en begrijpelijk is voor iedereen. Wereldwijd vertrouwen partners en organisaties op de technologie van SecurityHive. Samen met het beste netwerk aan partners, beschermen wij grote en kleine bedrijven in elke sector.

Kom in contact met SecurityHive-experts voor meer informatie.

Securityhive.nl | LinkedIn.com/SecurityHive

SECURITYHIVE