Hands on ICT
Security Management

Een proactieve cybersecurity verdediging met periodieke scans op kwetsbaarheden

Powered by Hands on ICT

your365°

www.handsonict.nl

Security Management

Doorlopende cybersecurity verdediging geborgd

Met Security Management worden kwetsbaarheden proactief geïdentificeerd en verholpen. Hiermee wordt de kans op beveiligingslekken verminderd. Dit helpt organisaties om hun ICT-omgeving beter te beschermen tegen aanvallen en cybercriminaliteit.

IT security en je bewapenen tegen cyberaanvallen: het leek altijd ver weg, maar komt toch steeds dichterbij. Het besef dat veel ICT-omgevingen 'bloot' staan aan gevaren van buitenaf krijgt dan ook steeds meer aandacht. Cybercriminelen kunnen met de ICT-mogelijkheden van tegenwoordig steeds makkelijker binnenkomen in een niet-optimaal beveiligde omgeving.

Leaflet YourSecurity

Leaflet Security Health Scan

Het belang van doorlopend security beheer

Hands on ICT zet met Security Management volledig in op het doorlopend voorkomen van cyberaanvallen en het verkleinen van de risico's. Voordat we aan de slag gaan met het implementeren van diensten en producten willen we inzicht krijgen in de huidige situatie. Want hoe veilig is je ICT-omgeving op dit moment? Welke onderdelen van je netwerk en systemen vragen om extra aandacht? Dat onderzoeken we met onze Security Health Scans. Daarna gaan we aan de slag met het implementeren van de oplossingen om je IT security aanzienlijk te verbeteren. Maar dan begint het eigenlijk pas. Want de snelheid van cybercriminelen zorgt ervoor dat wat vandaag veilig is, dat morgen misschien niet meer is. Het is daarom van groot belang om je omgeving doorlopend te monitoren zodat je tijdig kunt anticiperen op bedreigingen.

Security is een continu proces

Met Security Management zorgen we er met periodieke metingen en actieve monitoring voor dat we doorlopend inzicht hebben in de kwetsbaarheden van de IT omgeving. Met deze oplossing wordt automatisch op gezette tijden een scan uitgevoerd inclusief opvolging van kwetsbaarheden. Binnen deze scan worden dus periodiek exact dezelfde onderdelen gescand die opgenomen zijn in de Security Health Scan. Naast de automatische scans heb je de mogelijkheid om dit tussentijds on demand te doen op het moment dat hier aanleiding voor is.

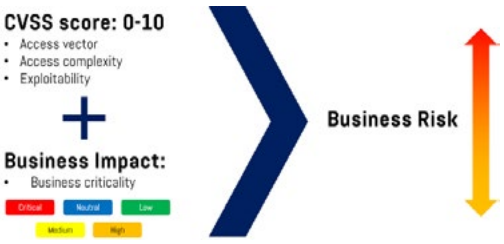
Security Management = vulnerability management

Met de scans die we periodiek uitvoeren brengen we kwetsbaarheden in kaart; we spreken hier ook wel van vulnerability management. Met vulnerability management worden kwetsbaarheden proactief geïdentificeerd en verholpen. Hiermee wordt de kans op beveiligingslekken verminderd. Dit helpt organisaties om hun ICT-omgeving beter te beschermen tegen aanvallen en cybercriminaliteit.

Om de risico's die de organisatie loopt binnen de IT-infrastructuur in kaart te brengen wordt de vulnerability oplossing geïmplementeerd binnen je eigen ICT-omgeving. Met een reguliere vulnerability scan worden de in gebruik zijnde IT-componenten geanalyseerd op mogelijke bedreigingen voor de bedrijfsvoering van je organisatie.

Risico gebaseerde aanpak

De scan is in staat om rekening te houden met de belangrijkste bedrijfsapplicaties en processen en zo op basis van deze gegevens een realistisch beeld te genereren van de risico's die specifiek gelden voor jouw organisatie. Met deze aanpak ben je in staat om de juiste mitigerende acties uit te voeren op de meest urgente risico's van de bedrijfsvoering.



Dit wordt er gescand

Enkele van de belangrijkste componenten die worden gescand:

- Netwerkapparaten: Dit omvat routers, switches, firewalls en andere netwerkapparaten die verbonden zijn met het bedrijfsnetwerk. Kwetsbaarheden in de configuratie en firmware worden hierbij geïdentificeerd.
- Servers: Fysieke en virtuele servers worden gescand om potentiële kwetsbaarheden te ontdekken. Het omvat besturingssystemen, applicatieservers, databaseservers en andere configuraties, services en software die op de servers operationeel zijn.
- Webapplicaties: Cross-site scripting (XSS), SQL-injectie, onjuiste configuraties en andere beveiligingsrisico's die kunnen leiden tot gegevenslekken of ongeautoriseerde toegang.
- Cloudomgevingen: Microsoft Azure of Amazon Web Services.

Heb je, met je eigen IT omgeving in gedachte, voldoende inzicht in de volgende vragen?

- Hoe snel reageer je op dit moment op nieuwe kwetsbaarheden?
- Welke risico's loop je met je kritieke bedrijfsapplicaties?
- Wordt er gerapporteerd aan management over potentiële bedrijfsrisico's'?

Automatisch én on demand scannen

De netwerkscans scannen automatisch en continu het netwerk en de systemen op een steeds groter wordend aantal kwetsbaarheden. De netwerkscans detecteren o.a. kwetsbaarheden zoals verouderde software, verkeerd geconfigureerde systemen & zwakke wachtwoorden. Daarnaast brengt de service automatisch uw netwerk in kaart zodat je een duidelijk overzicht krijgt van alle systemen – ongeacht de geografische locatie en of het in eigen beheer is of niet.

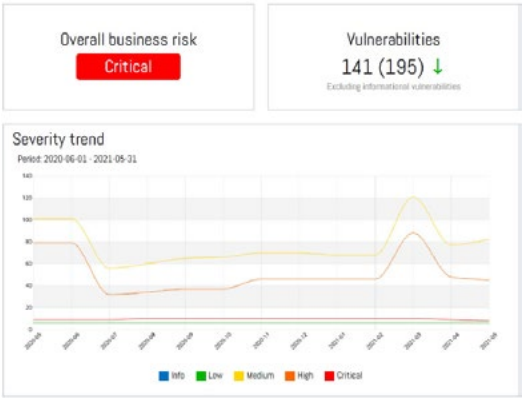
Met behulp van uitvoerige rapportages, slimme en effectieve tools en onze support, prioriteer en herstel je snel en effectief de kwetsbaarheden die worden ontdekt voordat ze worden benut door iemand met kwade bedoelingen. Parallel aan het automatisch scannen van netwerken en systemen, kun je op elk gewenst moment on demand scannen, bijvoorbeeld in verband met plotselinge veranderingen die optreden in de omgeving.

Gecentraliseerd beheer

Vanuit het Security Center is centraal beheer mogelijk over de detectie en opvolging van alle kwetsbaarheden inclusief trends & analyses.

Rapportages

De Security Management oplossing stelt de IT-afdeling in staat om te rapporteren over bedrijfsrisico's die de organisatie loopt richting het management. De kwetsbaarheid van de ICT-omgeving wordt inzichtelijk gemaakt met het executive report. Het executive report geeft een totaal weergave voor het management en is voorzien van een trendanalyse. Het management is hiermee in staat om te sturen op en blijft in controle over de bedrijfsrisico's.



Belangrijke feiten uit de praktijk

- 90% van de organisaties weet niet hoe kwetsbaar de ICT -omgeving is.
- 75% van de organisaties heeft geen routinematige cybersecurity aanpak
- 80% van de organisaties heeft meer kwetsbaarheden dan systemen

Het doorlopende Security Management proces

Security Management is een continu proces. We starten periodieke scans op waarmee we proactief kwetsbaarheden opsporen en verhelpen. Voordat we hiermee beginnen vindt er een intake plaats en zorgen we voor de juiste configuratie. Als dit afgerond is kunnen de periodieke scans plaatsvinden en kunnen we de monitoring opstarten.

Voordat we kunnen starten met Security Management:

Intake & Configuratie
De eerste stap die gezet moet worden is de intake met de verantwoordelijke van jullie organisatie. Hierin wordt besproken hoe vulnerability management wordt opgezet. Details die besproken worden zijn onder andere:

- Welke ICT architectuur & applicatielandschap is er aanwezig?
- Afstemming toegang & bevoegdheden
- Doorlooptijd, succes criteria & deliverables
- Wat wordt de scope van de scan?
- Welke assets zijn aanwezig?
- Wat zijn de business impact applicaties?

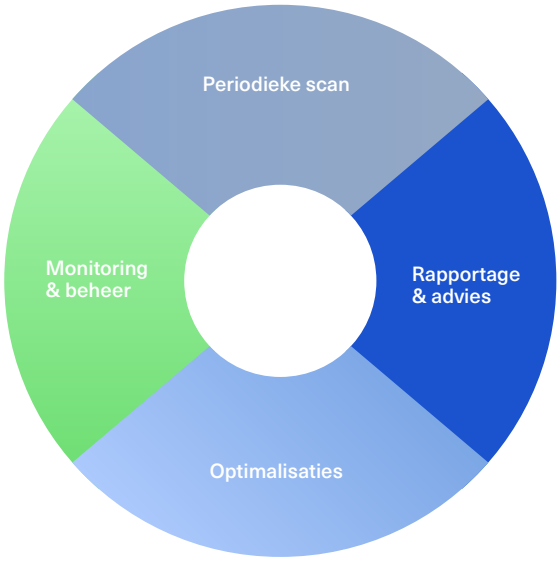
Scan
Binnen deze stap gaan onze ICT consultants aan de slag en zorgen dat de oplossing gereed is voor de eerste vulnerability scan. Wij zullen hier onder andere de volgende werkzaamheden uitvoeren:

- Onboarding binnen het platform
- Netwerk configuratie voor scanner appliance
- Installatie scanner appliance in ICT-omgeving
- Asset inventarisatie
- Configuratie asset structuur
- Configuratie scan profiel
- Uitvoering eerste vulnerability scan

Rapportage & advies
Na de eerste scan worden de resultaten weergegeven in het security center.
Onze ICT-consultants zullen de rapportages configureren en de kwetsbaarheden beoordelen. Middels de rapportages & het security center wordt ons advies vervolgens besproken met de ICT-verantwoordelijke van jullie organisatie.

Optimalisaties
Binnen deze stap zullen wij opvolging geven aan het besproken advies aangaande de gedetecteerde kwetsbaarheden binnen jullie ICT-omgeving. Deze stap is van essentieel belang voor het verhogen van het security niveau binnen jullie organisatie.

Monitoring & beheer
Vulnerability management is een continu proces. Binnen deze stap wordt de reguliere frequentie van de scans besproken en zullen scan, rapportage + advies en optimalisatie stap worden herhaald. Hiermee vindt er proactief beheer plaats op security bedreigingen.



IT security als topprioriteit

Het goed inrichten van je IT security is vandaag belangrijker dan ooit. Met YourSecurity bieden wij een scala aan diensten en producten om ervoor te zorgen dat je altijd en overal veilig aan het werk bent en dat je waardevolle bedrijfsdata goed geborgd is. Met YourSecurity zorgen we daarnaast voor continu inzicht in de kwaliteit van jouw IT security en helpen we je met de juiste diensten en producten je ICT-omgeving betrouwbaar en veilig te houden. Vraag nu een offerte aan voor een Security Health Scan of meer informatie over onze security producten en aanpak.

Vraag offerte aan

Contactgegevens
Hands on ICT
Nesland 5a
1382 MZ Weesp
+31(0)88 - 181 1300

info@handsonict.nl
www.handsonict.nl

www.handsonict.nl

Powered by Hands on ICT

your365