Hands on ICT
Security Health Scan

Vanuit een gedegen 0-meting naar proactive cybersecurity

Powered by Hands on ICT

your365°

www.handsonict.nl

Inhoud

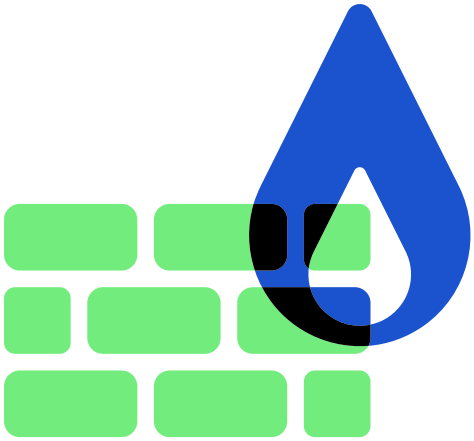
01	YourSecurity	3
02	Security Health Scan in detail	6
03	Security Health Scan Plus+ in detail	12
04	Security Management	17
05	Voorwaarden en condities	19
06	Bijlage 1 – Dienstenmatrix	20

Your Security

Het voorkomen van een aanval of hack stelt hoge eisen aan de security van je ICT-omgeving. Het is namelijk niet alleen de techniek die de beveiliging van je ICT-omgeving vormt, ook je medewerkers en de processen binnen je organisatie spelen een belangrijke rol. Om al deze aspecten van IT security te borgen, heeft Hands on ICT YourSecurity ontwikkeld. Vanuit YourSecurity gaan we pragmatisch aan de slag met je IT Security om deze structureel naar een hoger niveau te tillen.

Your Security in het kort

Met YourSecurity bieden we een scala aan diensten en producten om ervoor te zorgen dat je altijd en overal veilig aan het werk bent en dat bedrijfsdata goed geborgd is. Data behoort misschien wel tot het meest waardevolle bezit van iedere organisatie. Denk aan klantgegevens, personeelsbestanden, waardevolle bedrijfsdata en talloze andere voorbeelden van kritische data die niet buiten je organisatie terecht mogen komen en die je niet wilt verliezen. Gebeurt dit wel? Dan zijn de gevolgen vaak niet te overzien: financiële schade, operationele problemen en imagoschade zijn hier slechts enkele voorbeelden van.



Your Security in 3 stappen

Met onze YourSecurity-dienst werken we stap voor stap naar die goed beveiligde omgeving toe: we starten altijd met een Security Health Scan om de huidige situatie in kaart te brengen en komen vervolgens met een advies met bijbehorende acties om jouw IT security naar een hoger plan te tillen. Vervolgens zetten we in op periodieke metingen om je omgeving te monitoren en vroegtijdig te kunnen anticiperen op bedreigingen. We zorgen met YourSecurity voor een beveiligde omgeving die risico's minimaliseert én dat je medewerkers alert zijn op belangrijke signalen en hier juist op kunnen acteren.

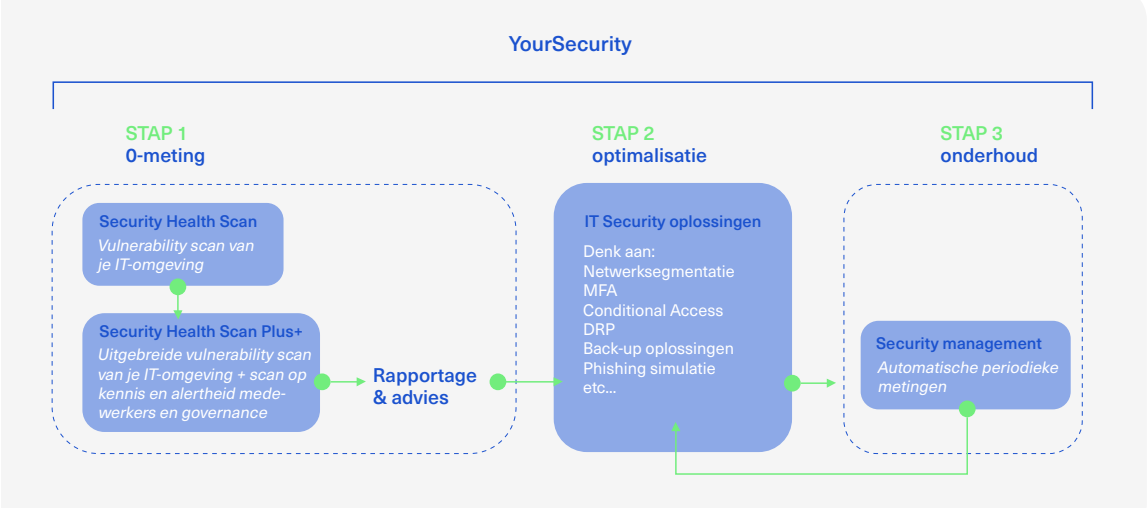
STAP 1 - Security Health Scan
Wil je direct aan het slag met het verbeteren van je IT security? Dan is het verstandig om te beginnen met één van de Security Health Scans die we aanbieden. We voeren hier een 0-meting uit van je gehele IT-omgeving, bekijken de processen om security te borgen en zien zo waar de grootste security issues zich bevinden. Op deze manier krijgen we goed inzicht in de huidige beveiligingsstatus van jouw omgeving. Hieruit volgt een helder adviesrapport waaruit blijkt waar de gaten zitten in jouw IT security en waar je dus direct actie op moet ondernemen.

STAP 2 - Security Optimalisatie
Naar aanleiding van het adviesrapport en bijbehorende oplossingen gaan we vervolgens aan de slag met het doorvoeren van verbeteringen om je IT security naar een hoger niveau te tillen. Denk hierbij aan technische maatregelingen op basis van diverse security producten, maar ook aan het trainen van personeel op security awareness en advies over het securitybeleid en gerelateerde processen.

Lees meer over Security oplossingen

STAP 3 - Security Management
Na de optimalisatiefase is het zeer belangrijk om de staat van de omgeving te blijven monitoren. Security is geen eenmalig project. Cybercriminaliteit ontwikkelt op een hoog tempo, zo ook de technieken die ervoor zorgen dat cybercriminelen minder kans maken om binnen te dringen. Met YourSecurity voeren we daarom op een periodieke basis scans en beheer uit op je omgeving zodat je ook in de toekomst zeker bent van een veilige omgeving. Op deze manier zorgen we ervoor dat bedreigingen van buitenaf direct en proactief worden gesignaleerd en opgelost.

Lees meer over Security Management



De voordelen van YourSecurity

Het goed inrichten van je IT-security is belangrijker dan ooit. Met de Security Health Scan heb je direct inzicht in je omgeving én weet je direct wat je moet doen om de veiligheid van je huidige omgeving te verbeteren. De voordelen van de scan op een rij:

- We bepalen een heldere security roadmap aan de hand van de Security Health Scan(s).
- De uitkomsten laten zien welke technologische, procedurele en menselijke acties je moet nemen om je beveiliging te verbeteren.
- Je organisatie beschikt vervolgens over een betrouwbaar en veilig IT-landschap. Door onze gedegen aanpak en jarenlange ervaring ben je verzekerd van effectieve IT security binnen je organisatie.
- Je hebt weinig omkijken meer naar je securitybeleid en bent verzekerd van een goede inrichting van je ICT-omgeving.
- Je gebruikers zijn zich bewust van de gevaren en weten hoe te handelen in kritische situaties. Dit verlaagt de kans op schade door lekken in je IT security enorm.
- Je securitybeleid is in lijn met de aangescherpte privacy- en securitywetgeving.
- Met YourSecurity doorlopen we een traject waarbij maatwerk geleverd wordt voor jouw organisatie op basis van de Security Health Scan(s). De oplossing sluit daardoor naadloos aan op jouw wensen en eisen.

Security Health Scan
in detail

Iedere ICT-omgeving staat bloot aan gevaren van buitenaf. Cybercriminelen bedenken steeds nieuwe en slimmere manieren om door digitale muren te breken. En vaak met succes. Dit kan grote impact hebben op jouw organisatie. Daarnaast stelt de bescherming van privacygevoelige data veel eisen aan de beveiliging van je ICT-omgeving. Het is belangrijk om je hierbij te realiseren dat een beveiligingsbeleid niet alleen gaat over de techniek, maar ook over de mensen die ermee werken en de manier waarop zij werken (processen).

We bieden hiervoor twee verschillende scans aan:

- Security Health Scan
- Security Health Scan Plus+

Security Health Scan
Met onze Security Health Scan krijgen we goed inzicht in de huidige beveiligingsstatus van jouw omgeving. Hieruit volgt een helder adviesrapport waaruit blijkt waar de gaten zitten in jouw IT security en waar je dus direct actie op moet ondernemen. Zo zorgen we samen voor een veilige omgeving die risico's minimaliseert.

Security Health Scan Plus+
Wil je, naast deze al zeer uitgebreide Security Health Scan, nog meer IT Security onderdelen onderzoeken? Dan bieden we de Security Health Scan Plus+ aan. In deze uitgebreide scan gaan we, naast de technische kant van ICT beveiliging, ook in op de mens en het proces.

In dit hoofdstuk lees je wat je met de Security Health Scan kunt verwachten. Vervolgens komt de Security Health Scan Plus+ aan bod.

De Security Health Scan bestaat uit een viertal onderdelen:

1. Systemen & netwerk
2. (Web)applicaties
3. Cloudomgeving (Microsoft Azure)
4. Rapportage & advies

Onderdeel 1

Systemen & netwerk

In dit onderdeel worden de kwetsbaarheden (CVE's) binnen je systemen & netwerk gedetecteerd. Met de scan die we uitvoeren brengen we kwetsbaarheden in kaart; we spreken dus 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 vulnerability scan worden de in gebruik zijnde IT-componenten geanalyseerd op mogelijke bedreigingen voor de bedrijfsvoering van je organisatie.

Systemen
Fysieke & virtuele servers zijn een essentieel onderdeel van je IT-infrastructuur en bevatten en belangrijke bedrijfsprocessen. Door servers te scannen, kunnen potentiële kwetsbaarheden en beveiligingslekken worden geïdentificeerd, zoals verouderde software, ongepatchte systemen, onjuiste configuraties of kwetsbaarheden in geïnstalleerde applicaties.

Binnen dit onderdeel worden onder andere de volgende systemen door ons beoordeeld:

- Besturingssystemen, zoals Windows Server, Linux-distributies (bijv. Ubuntu, Red Hat, CentOS) en Unix-gebaseerde systemen (bijv. FreeBSD) inclusief services.
- Applicatieservers. Beoordeling van applicatie specifieke kwetsbaarheden en configuratiefouten.
- Database servers, zoals Microsoft SQL Server, MySQL, Oracle Database, PostgreSQL. Identificeren van kwetsbaarheden in de databaseconfiguratie, toegangscontroles, patches en andere database gerelateerde aspecten.
- Webservers, zoals Apache HTTP Server, Microsoft IIS, Nginx, enz., om kwetsbaarheden in de webserverconfiguratie, SSL/TLS-implementaties en andere web technologieën te vinden.

Netwerk
Een goed ingericht en up-to-date netwerk is eveneens een belangrijk onderdeel. Steeds meer apparaten zijn met het internet gekoppeld en vormen hiermee een risico. Zwakke plekken in netwerkapparaten en configuraties zijn vaak een onbekende dreiging. Ook het gebruik van draadloze netwerken heeft een flinke vlucht genomen en heeft de juiste aandacht nodig voor de juiste inrichting en beveiliging.

Binnen dit onderdeel worden door ons alle netwerkapparaten beoordeeld op kwetsbaarheden die verbonden zijn met het bedrijfsnetwerk:

- Firewalls
- Switches
- Storage
- Wifi controllers & access points
- Printers
- OT/SCADA
- IoT
- Beveiligingscamera's

Netwerk hardening

Netwerk hardening is het proces waarbij een netwerkswitch wordt beveiligd door verschillende beveiligingsmaatregelen te implementeren. Het is belangrijk om switch hardening uit te voeren, omdat switches een belangrijke rol spelen in het netwerk en kwetsbaar kunnen zijn voor verschillende soorten bedreigingen.

Naast switch hardening is het ook belangrijk om netwerksegmentatie toe te passen. Zo kunnen minder veilige systemen niet vrij communiceren met de rest van het netwerk. In de scan onderzoeken we hoe het netwerk geconfigureerd is en of er bijvoorbeeld switch hardening is toegepast.

Onderdeel 2

(Web)applicaties

Het is belangrijk voor je organisatie om webapplicaties, zoals websites & portals, te scannen op kwetsbaarheden om zo potentiële beveiligingsproblemen te identificeren en op te lossen voordat ze worden misbruikt door aanvallers.

Web Application Scanning is het proces van het automatisch testen van een webapplicatie op kwetsbaarheden. Dit wordt gedaan met behulp van onze gespecialiseerde software die aanvallen op de applicatie simuleert om kwetsbaarheden te identificeren die door aanvallers kunnen worden uitgebuit.

Onze webapplicatiescanner is gebaseerd op DAST (Dynamic Application Security Testing) en SCA (Software Composition Analysis). Dit betekent dat we kwetsbaarheden vinden in de draaiende applicatie en in gebruikte componenten zoals WordPress en JavaScript-bibliotheken. In de scan gaan we uit van de niet-geauthentiseerde methode. Daarnaast wordt de laatste versie van de OWASP top 10 meegenomen binnen onze scan. Een geauthentiseerde methode, waarbij we de “binnenkant” van je applicatie ook scannen, is op aanvraag mogelijk.

Wij scannen de webapplicaties onder andere op de volgende onderdelen:

Webapplicatiekwetsbaarheden
SQL-injectie, cross-site scripting (XSS), onjuiste autorisatie, onveilige deserialisatie, directory traversal en andere veelvoorkomende kwetsbaarheden die misbruikt kunnen worden door aanvallers.

Configuratiefouten
De scan identificeert configuratiefouten die de beveiliging van uw webapplicaties kunnen beïnvloeden. Dit omvat mogelijke blootstelling van gevoelige informatie, onbeveiligde toegang tot bestanden of directories, onjuiste beveiligingsheaders en andere configuratie gerelateerde problemen. Daarnaast het onderzoeken van toegangscontroles, wachtwoordbeleid, sessiebeheer, HTTPS-implementatie en andere relevante beveiligingsinstellingen.

Verouderde softwarecomponenten
Binnen de scan wordt gecontroleerd of je webapplicaties verouderde softwarecomponenten bevatten, zoals frameworks, bibliotheken of plug-ins. Deze verouderde componenten kunnen bekende kwetsbaarheden bevatten die door aanvallers kunnen worden misbruikt.

Foutbeheer en debuginformatie
De scan identificeert of er foutbeheer- of debuginformatie beschikbaar is in de productieomgeving van je webapplicatie. Het blootstellen van dergelijke informatie kan aanvallers waardevolle inzichten geven en de kans op succesvolle aanvallen vergroten.

Onderdeel 3

Cloudomgeving (Microsoft Azure)

Het opsporen en voorkomen van kwetsbaarheden en compliance-overtredingen wordt steeds lastiger nu cloud architecturen steeds complexer worden. Inzicht is de eerste stap naar een sterk beveiligingsbeleid. Het compliant en veilig houden van je cloud omgeving begint met weten welke resources je hebt, waar ze zich bevinden en hoe veilig ze zijn.

Cloudconfiguraties
Onze scan controleert op mogelijke misconfiguraties in je Azure omgeving. Dit omvat het beoordelen van toegangscontroles, firewallregels, beveiligingsgroepen, netwerkconfiguraties en andere cloud specifieke instellingen die van invloed kunnen zijn op de beveiliging.

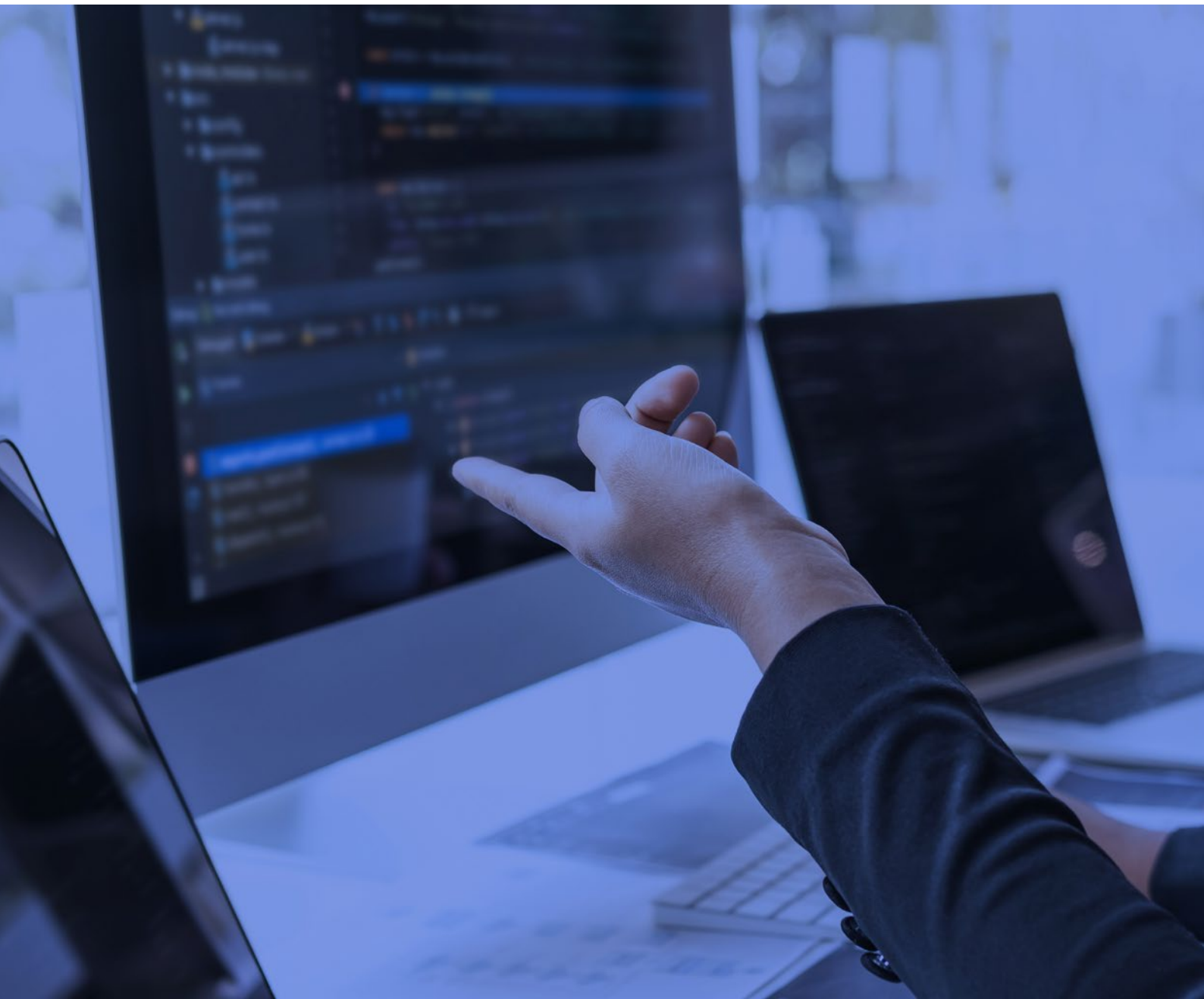
Identity and Access Management (IAM)
IAM-configuraties in Azure worden gescand om te controleren op onjuiste machtigingen, overmatige privileges, onveilige authenticatie-instellingen en andere beveiligingsrisico's met betrekking tot gebruikersaccounts, groepen en rollen.

Beveiligingsgroepen en netwerkbeveiliging
Controle op de configuratie van beveiligingsgroepen en netwerkconfiguraties in

je Azure omgeving. We identificeren potentiële blootstellingen, openstaande poorten, onjuiste regels en andere netwerk gerelateerde kwetsbaarheden die kunnen leiden tot ongeautoriseerde toegang.

Opslag- en databasebeveiliging
We scannen op mogelijke beveiligingslekken in Azure Storage, inclusief onbeveiligde toegang, blootstelling van gevoelige gegevens en configuratiefouten. We controleren ook op kwetsbaarheden in database-instances, zoals onjuiste toegangscontroles, onversleutelde verbindingen en verouderde softwarecomponenten.

Compliance en best practices
We controleren of je Azure omgeving voldoet aan de best practices en compliance standaarden, zoals de Azure Security Center aanbevelingen. We identificeren mogelijke afwijkingen en bieden suggesties voor verbeteringen om te voldoen aan beveiligingsrichtlijnen.



Onderdeel 4

Rapportage & advies

Op basis van de Security Health Scan ontvang je een rapportage met hierin geprioriteerde aanbevelingen en acties om jouw IT security naar een hoger niveau te tillen. Hierbij heb je inzicht in wat je als organisatie zelf kunt oppakken en wat Hands on ICT voor je kan uitvoeren om je organisatie beter te beveiligen. Een onmisbare eerste stap om je organisatie gericht en efficiënt te beschermen tegen cyberaanvallen.

Adviesgesprek

Op het moment dat het rapport beschikbaar is, maken we een afspraak om de bevindingen en daaraan verbonden conclusies en aanbevelingen door te nemen. Voor bepaalde geavanceerde security settings is het wellicht nodig dat we nog wat meer onderzoek doen, om vervolgens op basis hiervan de juiste acties te ondernemen. Dit alles wordt besproken tijdens het adviesgesprek.

Plan van aanpak

Vervolgens gaan we op basis van de uitkomsten aan de slag met een plan van aanpak. Samen bepalen we de prioriteiten en komen we tot een project- en optimalisatieplan. Zo weten jullie én onze consultants exact wat er te doen staat. Normaliter geldt bij de totstandkoming van een projectplan de volgende stelregel: we voeren eerst alle quick wins uit en maken hiermee een snelle verbeterslag waarmee de basis direct al een stuk betrouwbaarder is. Vervolgens gaan we voor eventuele bijzondere security issues meer de diepte in en schakelen we indien nodig met een partner voor meer geavanceerde oplossingen.

Security Health Plus+
in detail

Met de Security Health Scan Plus+ onderzoeken we naast de al zeer uitgebreide Security Health Scan nog een aantal andere onderdelen om je IT Security naar een hoger niveau te tillen. Het gaat hier naast additionele technische zaken vooral om kennis en alertheid van je medewerkers en governance en beleid op het gebied van security.

Veel bedrijven benaderen IT security vanuit het technische aspect, maar IT security gaat verder dan dat. Naast technologie gaat IT security om mensen en processen binnen een organisatie. Als mens, proces en techniek perfect samenkomen, dan pas kan IT security goed worden geregeld. Vanuit deze drie invalshoeken is deze Security Health Scan Plus+ ontwikkeld. Deze scan kijkt verder dan alleen techniek. In dit hoofdstuk lees je wat je met de Security Health Scan Plus+ kunt verwachten, bovenop onze reguliere scan.

De Security Health Scan Plus+ bestaat, buiten de al eerder genoemde scanonderdelen van de Health Scan, uit de volgende PLUS-onderdelen:

5. Active Directory
6. Microsoft 365
7. Endpoints
8. Kennis & alertheid medewerkers
9. Governance & NIS2

Onderdeel 5

Active Directory

De Active Directory is een belangrijk doelwit voor cyberaanvallers, omdat een aanval op de Active Directory toegang tot gevoelige bedrijfsgegevens kan bieden. Het is daarom belangrijk om beveiligingsmaatregelen te treffen om de Active Directory goed te beveiligen. De beveiliging bestaat bijvoorbeeld uit het uitschakelen van oude cyphers en onnodige features of het updaten van de servers met de laatste patches. We beoordelen de algehele status van de Active Directory gebaseerd op verschillende indicatoren.

De volgende onderdelen worden uitgelezen:

- DNS Domains
- Known tenant
- Configuration
- Company Info
- Policies
- AD Connect
- Applications and Permissions
- Roles
- Users
- Foreign domains

Onderdeel 6

Microsoft 365

Microsoft 365 is een platform dat functionaliteit en veiligheid combineert. Microsoft 365 biedt veel mogelijkheden om de beveiliging te controleren, aan te scherpen en te bewaken. Tegelijkertijd betekent 'meer beveiliging' vaak 'minder gebruiksvriendelijkheid'. Maar weet je welke mogelijkheden er zijn en hoe je deze optimaal kunt inzetten? Wat zijn de risico's als je niets doet?

In dit onderdeel lichten we de volgende onderdelen binnen Microsoft 365 door.

Office 365 Recommended Configuration Analyzer (ORCA)
Office 365 Recommended Configuration Analyzer (ORCA) is een tool die we gebruiken om de configuratie van Microsoft 365 email implementatie te controleren en te optimaliseren. Het is een belangrijke tool voor organisaties die Microsoft 365 gebruiken, omdat het problemen in de e-mailconfiguratie van Office 365 identificeert en de prestaties, beveiliging en beschikbaarheid van de service verbetert.

Microsoft Compliance Configuration Analyzer (MCCA)
De Microsoft Compliance Configuration Analyzer (MCCA) is een hulpprogramma dat de huidige configuraties van je tenant ophaalt en deze configuraties valideert tegen de aanbevolen best

practices van Microsoft 365. Deze best practices zijn gebaseerd op een reeks controles, waaronder belangrijke voorschriften en normen voor gegevensbescherming en algemeen gegevensbeheer. MCCA bied je vervolgens een bruikbaar statusrapport om de configuratie van Microsoft 365 te verbeteren.

Identity Secure Score
Identity Secure Score is een tool die speciaal is ontwikkeld door Microsoft om organisaties te helpen bij het verbeteren van de beveiliging van identiteiten en toegangscontrole. Deze tool is beschikbaar via het Microsoft 365 Security Center en biedt organisaties de mogelijkheid om hun identiteitsbeveiliging en toegangscontrole te evalueren en te verbeteren op basis van best practices en normen op dit gebied.

Multifactor Authentication
We controleren in de scan of je organisatie op dit moment gebruik maakt van MFA & de juiste authenticatie- en verificatiemethoden.

Conditional Access
Conditional Access policies kunnen gebruikt worden om onder bepaalde voorwaarden toegang tot de Microsoft 365 omgeving toe te staan. Dit kan op basis van locatie zijn, het soort apparaat, of de gebruiker die probeert in te loggen. We scannen welke policies er zijn en hoe deze zijn ingericht.

Azure Active Directory Risk Detection
In een Microsoft 365 omgeving staat de detectie van riskante aanmeldpogingen niet als default ingeschakeld. We adviseren om dit altijd te doen om inzicht te krijgen in wat er gebeurt.

Overzicht van Risk Detections
We onderzoeken welke accounts volgens Azure 'at risk' zijn gemarkeerd.

OAuth-applicaties
We maken een overzicht van de applicaties die zijn toegevoegd aan de tenant. Een applicatie kan variëren van alleen toegang tot naam en e-mailadres (voor het aanmaken van een account op een website die Microsoft-login aanbiedt) tot complete toegang tot alle mailboxen.

Onderdeel 7

Endpoints

Het overal en altijd werken, waar en wanneer je dat wilt, heeft ervoor gezorgd dat we meerdere mobiele devices per persoon gebruiken. Niet alleen zakelijk, maar ook persoonlijke apparaten gebruiken we steeds meer om werk te verrichten. Dit heeft nieuwe uitdagingen met zich meegebracht voor je ICT-omgeving. Is iedere persoonlijke laptop of smartphone wel goed beveiligd of up-to-date? Het is van belang om hier vooraf de juiste beveiligingsmaatregelen voor te treffen en dit vast te leggen. Om je bedrijfsgegevens veilig te stellen moeten zowel de zakelijke als persoonlijke mobiele devices beschermt worden met de nieuwste software.

Binnen dit onderdeel beoordelen we de volgende aspecten:

- Mobile Device Management
- Bring Your Own Device beleid
- Endpoint Detection & Response
- Toegangsbeleid (hardware en software)
- Updatebeleid OS & applicaties

Onderdeel 8

Kennis & alertheid medewerkers

Binnen een organisatie zijn de medewerkers vaak onbewust de zwakste schakel. Een van de belangrijkste oorzaken van alle lekken en hacks is namelijk het menselijk handelen. Vaak is dit een gevolg van een gebrek aan kennis over online veiligheid bij medewerkers van een organisatie. Het onjuiste gedrag en de onwetendheid van medewerkers vergroot hiermee de kans op een beveiligingslek in je ICT-omgeving. Het kan als organisatie daarom van belang zijn om de kennis over online veiligheid bij medewerkers te testen. Dit kan onder andere door middel van een phishingtest.

In cybersecurity is het van belang dat medewerkers bewust zijn van hun rol in de beveiliging van de organisatie en dat een mogelijke inbreuk op je ICT-omgeving vrijwel altijd onverwachts plaatsvindt. Medewerkers moeten te allen tijde alert zijn (en blijven) op alle (potentiële) gevaren die op de organisatie afkomen. Het is belangrijk voor bedrijven om zich te realiseren dat de mens vaak de zwakste schakel is binnen de beveiliging van je omgeving en data.

Als het gaat over de mens en het verbeteren van IT security, dan hebben we het vooral over het trainen van medewerkers in het identificeren en vermijden van cyberbedreigingen. Menselijk handelen is namelijk bij meer dan 95% van alle lekken en hacks de belangrijkste oorzaak. Dit komt mede doordat het bij medewerkers vaak schort aan kennis over online veiligheid. Leer ze bijvoorbeeld phishing e-mails te identificeren en te rapporteren.

Binnen dit onderdeel geven we daarom voorlichting en advies over de te nemen stappen voor het verhogen van de kennis bij je medewerkers over online veiligheid.

Onderdeel 9

Governance & NIS2

Ook al is de techniek vaak de basis van de beveiliging van je ICT-omgeving, de processen rondom het borgen en delen van informatie moeten op orde zijn. Dit verkleint de kans op een inbreuk op je ICT-omgeving. Bij het proces gaat het over business- en IT- processen die de organisatie weerbaarder, transparanter en compliant maken. Ook zijn er strategieën aanwezig om proactief een cyberbeveiligingsincident te voorkomen en snel en effectief te reageren. Denk hier bijvoorbeeld aan aanvaardbaar gebruik, externe toegang definiëren en incident respons.

Je hebt wellicht al gehoord van NIS2. NIS is de afkorting van Network & Information Systems en biedt namens de EU een kader voor de beveiliging van netwerk- en informatiesystemen die van algemeen belang zijn voor de openbare veiligheid. In andere woorden, het doel van de NIS is om binnen de EU het cyberweerbaarheidsniveau te verhogen. Door de NIS-richtlijn is de cyberveiligheid van de EU-landen dan ook over het algemeen groter geworden. Maar gezien de toenemende dreigingen en de grote mate van afhankelijkheid van de digitalisering die met de coronacrisis nog sterker naar voren kwam is gebleken dat de huidige richtlijn niet voldoende is. Daarom wordt de bestaande NIS richtlijn vervangen door de Network & Information Systems versie 2: NIS2.

De NIS2 is op 27 december 2022 gepubliceerd. Echter hebben alle Europese landen tot 17 oktober 2024 om de richtlijn in nationale wet- en regelgeving te implementeren. Dat is daarmee ook direct de datum dat NIS2 volledig doorgevoerd moet zijn binnen de bedrijfsvoering. Deze NIS2 is echter nog niet volledig door het besluitvormingsproces gegaan. De verschillen tussen de huidige NIS-richtlijn (NIS1) en NIS2 zijn te vinden op het gebied van sectoren en aanbieders, beveiligingseisen en toezichtmaatregelen.

In dit onderdeel leggen we de Secuity Health Scan naast de huidige richtlijnen van NIS2 zodat je op de juiste weg bent richting deze aankomende wetgeving. Wil je meer informatie over NIS2 en of jouw organisatie hieraan moet voldoen, dan kun je terecht op onze website. Uiteraard gaan we hier ook graag met je over in gesprek.

Security Management

Met onze Security Health Scan heb je de ideale basis om je IT security vervolgstappen vorm te geven. Wat zijn de quick wins, welke solutions heb je nodig om de deur van je IT omgeving (nog) beter dicht te houden en welke acties zijn nodig om security ook voor langere termijn op de radar te hebben. Ons advies is om met proactief Security Management aan de slag te gaan.

Uit de Security Health Scan volgt een helder rapport met aanbevelingen om je IT Security te verbeteren. Hieruit volgt een gedegen plan van aanpak op basis van prioriteit van de acties en het gevolg hiervan voor je omgeving. Denk hierbij aan de implementatie van security oplossingen zoals Mobile Device Management, Endpoint Detection & Response, Conditional Access of het inzetten van Sensitivity Labels.

Maar zoals gezegd is IT security geen eenmalig project. Belangrijk is om je omgeving te blijven monitoren en bij te blijven met de laatste ontwikkelingen zodat hackers geen kans krijgen. Wil je daarom naar een proactieve aanpak van je IT Security? Dan is de volgende stap onze Security Management oplossing. Met Security Management worden kwetsbaarheden periodiek en proactief geïdentificeerd en verholpen. We zetten hierbij volledig in op het doorlopend voorkomen van cyberaanvallen en het verkleinen van de risico's door de inzet van periodieke metingen en actieve monitoring. Zo wordt IT Security niet een eenmalig project binnen je organisatie, maar blijft het dichthouden van de deur een constante prioriteit.

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

Voorwaarden & condities

Copyright
Niets uit deze dienstbeschrijving mag zonder voorafgaande schriftelijke toestemming van Hands on ICT verveelvoudigd en/of openbaar worden gemaakt door middel van druk, offset, kopie of in enige digitale, elektronische, optische of andere vorm of (en dit geldt zo nodig in aanvulling op het auteursrecht) gereproduceerd worden ten behoeve van een onderneming, organisatie of instelling of voor eigen oefening, studie of gebruik.

Disclaimer
Bij het samenstellen van deze dienstbeschrijving is de grootste zorg besteed aan de juistheid van de hierin opgenomen informatie. Hands on ICT BV kan echter niet verantwoordelijk worden gehouden voor eventuele onjuiste informatie verstrekt via deze dienstbeschrijving.

Algemene voorwaarden
Hands on ICT is aangesloten bij het ICT-collectief NLdigital. Derhalve zijn op al onze leveringen de algemene voorwaarden van de ICT-branche organisatie NLdigital van toepassing. Deze algemene voorwaarden zijn door NLdigital gedeponeerd bij de Rechtbank Midden-Nederland, locatie Utrecht. De voorwaarden zijn vanuit onze website in te zien en te downloaden via: Algemene voorwaarden (handsonict.nl)

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

Contact

Bijlage 1 - Dienstmatrix

Onderdeel 1 – Systemen & Netwerk	Security Health Scan	Security Health Scan Plus+
Kwetsbaarheden (CVE) scan op alle netwerkdevices zoals Windows servers, Linux distributies, Firewalls, Switches, Storage, Wifi apparatuur, Printers, OT/SCADA, IoT, Beveiligingscamera's.	✓	✓
Onderdeel 2 – Webapplicaties		
Webapplicatie scan op kwetsbaarheden door SQL-injectie, cross-site scripting (XSS), onjuiste autorisatie, onveilige deserialisatie, directory traversal, configuratiefouten & verouderde softwarecomponenten.	✓	✓
Onderdeel 3 – Cloudomgeving (Microsoft Azure)		
Kwetsbaarheden scan binnen Microsoft Azure op de configuratie, IAM, beveiligingsgroepen, netwerkbeveiliging, opslag- & databasebeveiliging. Compliance & best practice beoordeling.	✓	✓
Onderdeel 4 – Rapportage & advies		
Rapportage & advies	✓	✓
Onderdeel 5 –Active Directory		
Scan op DNS Domains, Known tenant, Configuration, company Info, policies, AD Connect, applications and Permissions, roles, users, foreign domains.		✓
Onderdeel 6 – Microsoft 365 Security		
Office 365 Recommended Configuration Analyzer (ORCA), Microsoft Compliance Configuration Analyzer (MCCA), Multifactor Authentication, Conditional Access, Azure Active Directory Risk Detection, Overzicht van Risk Detections, Failed sign ins, OAuth-applicaties.		✓
Onderdeel 7 – Endpoints		
Controle & advies over Mobile Device Management, Bring your own Device beleid, Endpoint Detection & Response, Toegangsbeleid, Updatebeleid OS & applicaties.		✓
Onderdeel 8 – Endpoints		
Advies over de te nemen stappen voor het verhogen van de kennis & alertheid bij je medewerkers over online veiligheid.		✓
Onderdeel 9 – Governance & NIS2		
Advies over ICT beveiligingsbeleid en de NIS2 richtlijnen.		✓

N.B. Benodigde licenties maken geen onderdeel uit van de scan en worden separaat geleverd.

www.handsonict.nl

Powered by Hands on ICT

your365