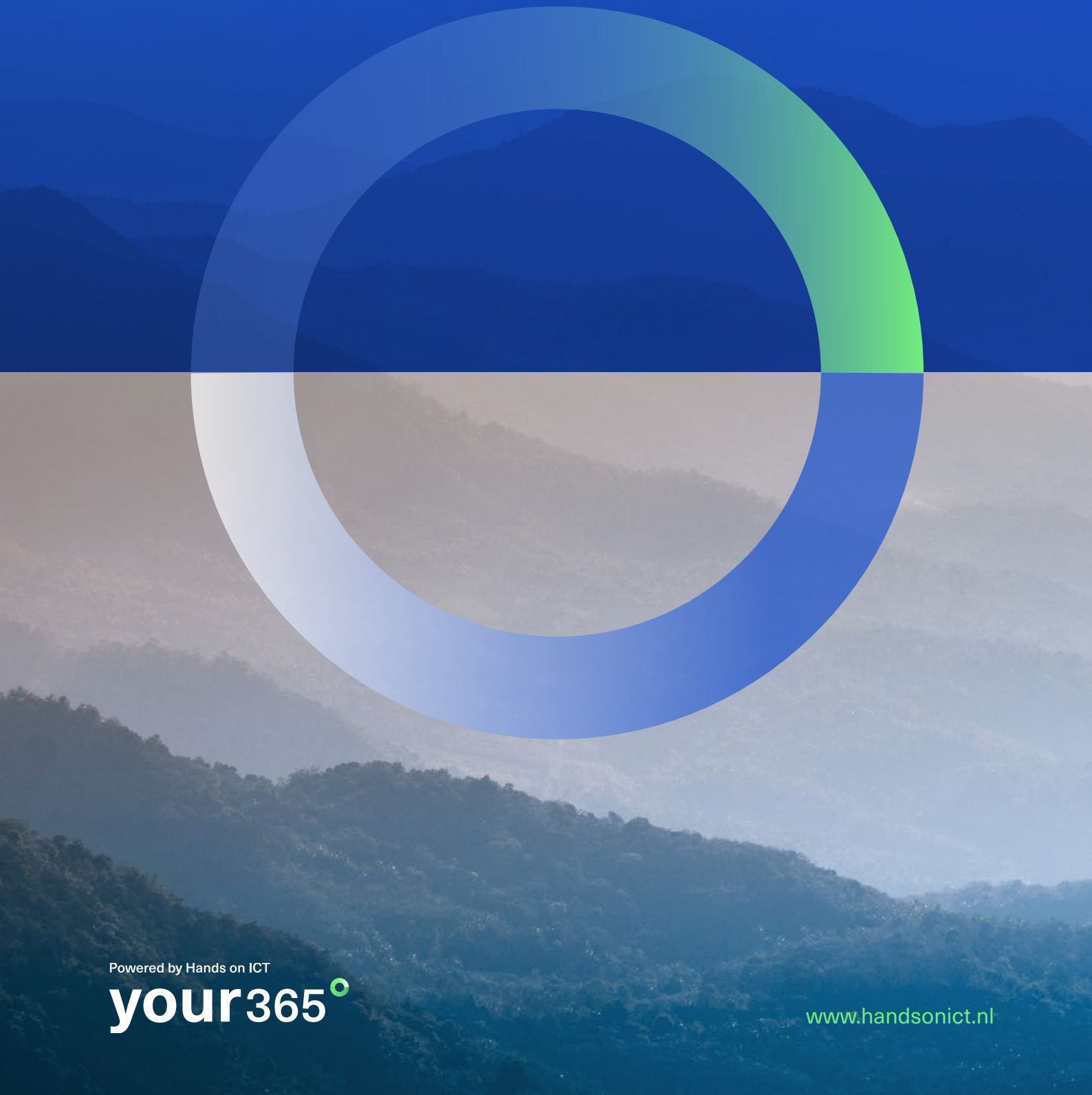
Hands on ICT
Dienstbeschrijving
YourSecurity

Slimme ICT-oplossingen voor succesvolle business



Powered by Hands on ICT

your365°

www.handsonict.nl

Inhoud

YourSecurity

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 gemakkelijker binnenkomen in een niet-optimaal beveiligde omgeving.

Wanneer er door de digitale muren van je organisatie heen wordt gebroken, heeft dat grote impact. 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.

YourSecurity 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.

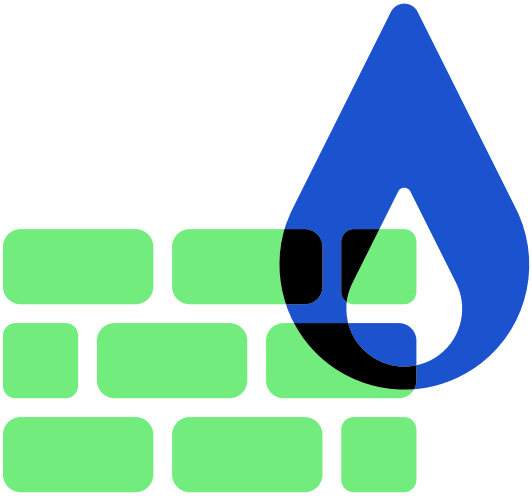
Hands on ICT zet met YourSecurity volledig in op het voorkomen van cyberaanvallen en het verkleinen van de risico's. We hanteren hierbij het NIST-framework én de Zero Trust-aanpak. Deze twee modellen benaderen IT-security vanuit een andere invalshoek, waardoor we een stabiele basis voor onze dienstverlening creëren.

Het NIST-framework gaat uit van een stappenplan om met ICT-beveiliging aan de slag te gaan en geeft concrete handvatten voor dit proces. Zero Trust baseert zich juist meer op elke laag binnen je IT-infrastructuur, waarbij elke laag een gevaar kan vormen. Dit maakt dat ze complementair aan elkaar zijn en op deze manier samen zorgen voor een 365-graden aanpak rondom IT-security. Zo combineren we een gedegen aanpak met alle inhoudelijke lagen binnen je organisatie. Deze combinatie vormt het uitgangspunt voor onze YourSecurity-dienst.

Het belang van IT-security

Vroeger was IT-security nog vrij eenvoudig. Er was één kantoor met alle werkplekken en servers binnen de kantoormuren. Destijds was thuiswerken nog geen optie. Hierdoor was er slechts één connectie met het internet, alleen die van het kantoor. Dit zorgde voor een hoge mate van controle, want de ICT-afdeling bewaakte die toegang tot het internet. Zodra er een buitenstaander naar binnen wilde dringen, was die simpele controle voldoende om de omgeving te beschermen.

Tegenwoordig is dat anders en hebben (mobiele) devices steeds vaker de mogelijkheid om een connectie te maken met jouw ICT-omgeving. Dat komt onder andere door het Internet of Things, de cloud, hybride werken, applicaties van derden en BYOD (Bring Your Own Device). Hierdoor zijn er veel meer toegangspoorten tot jouw ICT-omgeving. Dit zorgt voor een lagere mate van controle.



Daarnaast blijft cybercriminaliteit zich flink vernieuwen: malware, phishing, cryptolockers, ransomware en CEO-fraude zijn zaken die we dagelijks tegenkomen. Dit vraagt om een sterker cybersecuritybeleid. We adviseren daarom iedere organisatie om binnen het securitybeleid het BDA-principe (Before, During, After) te hanteren. Hierin kijk je naar wat je moet doen om vooraf een aanval te voorkomen, hoe je handelt tijdens een aanval en hoe je snel kan herstellen na een aanval.

IT-security is van bijzaak een noodzaak geworden. Een cyberaanval of hack kan cruciale bedrijfsprocessen platleggen en leiden tot verlies van gevoelige data. De feiten liegen er niet om. Een paar voorbeelden:

- Organisaties hebben tot 220 dagen nodig om een datalek te identificeren en te dichten
- Menselijke fouten zijn verantwoordelijk voor 95% van alle datalekken
- Elke 39 seconden vindt er een cyberaanval plaats
- Gemiddeld is slechts 5% van de mappen van bedrijven goed beveiligd

Onze visie op IT-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 belichten we binnen YourSecurity verschillende onderdelen vanuit IT-security waarvoor iedere organisatie zaken geregeld moet hebben. Op deze manier ontstaat er een 365-graden securitybeleid, dat van toepassing is op alle lagen binnen je organisatie.

De mens
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 om de mens, 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.

Het proces
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.

De techniek
Tot slot gaat het hier natuurlijk om de techniek (tools, software, en hardware) die kan worden ingezet, geïntegreerd en geautomatiseerd om snelle detectie en de beperking van bedreigingen te vergemakkelijken. Bij techniek gaan we voor een ICT-omgeving die goed is ingericht, deugdelijk is beveiligd én is voorzien van de laatste versies van applicaties en software.

In 5 stappen naar een verbeterde IT-security

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. Zo zorgen we voor een veilige omgeving die risico's minimaliseert en dat je medewerkers alert zijn op belangrijke signalen en hierop kunnen acteren.

Onze YourSecurity-dienst voeren we uit aan de hand van de volgende stappen:

Stap 1 Security Health Scan | de 0-meting
We starten met een Security Health Scan van je organisatie. In deze health scan onderzoeken we de belangrijkste facetten rondom IT-security. Met deze 0-meting krijgen we goed inzicht in de huidige beveiligingsstatus van jouw omgeving.

Stap 2 Rapportage & advies
Met de gemaakte 0-meting hebben we een concrete set aan adviezen en aanbevelingen om je IT-security beter in te richten. Uit dit advies komt de aanbeveling van de verschillende diensten die beschikbaar zijn binnen onze YourSecurity-dienstverlening.

Stap 3 Inrichting Security 2.0
Naar aanleiding van het advies kunnen we maatwerkoplossingen bieden om je IT-security naar een hoger niveau te tillen. Denk hierbij aan het trainen van personeel, de MFA-inrichting, het bepalen van securitybeleid of de inrichting van policies.

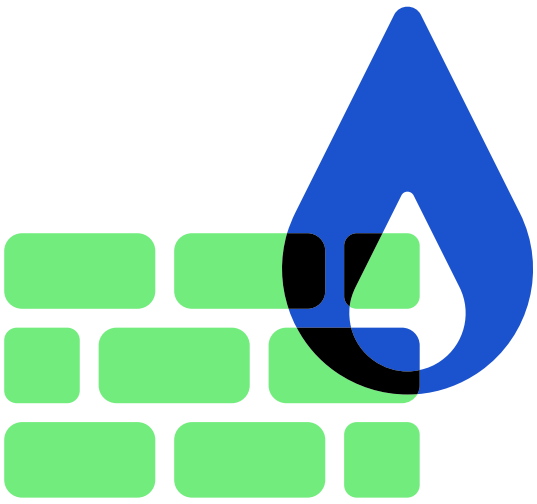
Stap 4 Periodieke Security Health Scans
Cybercriminaliteit ontwikkelt op een hoog tempo, zo ook de technieken die ervoor zorgen dat cybercriminelen minder kans maken om binnen te dringen. Met YourSecurity voeren we regelmatig een tussentijdse scan op je omgeving uit, zodat je ook in de toekomst geborgd bent van een veilige omgeving.

Stap 5 Monitoring & Support
Naast de health scans zullen we diverse monitoringstools inrichten om ervoor te zorgen dat bedreigingen van buitenaf direct en proactief worden gesignaleerd en opgelost. Denk hierbij aan endpoint detection, onderhoud en het doorvoeren van updates. Let op: het maken van back-ups is geen onderdeel van YourSecurity.

De voordelen van YourSecurity

Het goed inrichten van je IT-security is belangrijker dan ooit. Met de YourSecurity-dienstverlening 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 YourSecurity 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 waterdicht 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.
- Je betaalt een vast maandtarief per gebruiker. Simpel en transparant, zodat je precies weet wat de kosten zijn en wat je van ons kunt verwachten.
- Met YourSecurity doorlopen we een standaardtraject 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.



Stap 1
Security health scan

Met de Security Health Scan voeren we een 0-meting uit op het gebied van IT-security binnen jouw organisatie. Dit doen we op de niveaus: mens, proces en techniek.

De Security Health Scan bestaat uit een viertal onderdelen:

1. Algemene informatiebeveiliging en controles
2. Active Directory
3. Azure Active Directory
4. Office 365

Belangrijk voor de aanvang van deze scan is dat Hands on ICT toegang heeft tot deze onderdelen:

- Werkplek met netwerkverbinding
- PingCastle Auditor-licentie
- Login Office 365/Azure tenant
- Login voor firewall en switches
- Login op een managementserver
- Netwerktekening; Server- en functielijst

Zodra aan deze requirements voldaan is, kunnen we starten met de scan.

Hieronder worden alle onderdelen die we in de scan uitvoeren besproken.

Algemene informatiebeveiliging en controles

In dit hoofdstuk worden verschillende aspecten van informatiebeveiliging gemeten en gerapporteerd, waaronder gebeurtenissen en uitgevoerde controles.

Firewall Scan
Een goede firewall is belangrijk, omdat deze de veiligheid van een netwerk waarborgt. Een firewall is een software- of hardwarematige barrière die inkomend en uitgaand verkeer tussen een netwerk en het internet controleert en beperkt. Een firewall kan ongewenst verkeer zoals malware, virussen en hackers, blokkeren en voorkomen dat deze het netwerk binnendringen en schade aanrichten.

Het is daarom van belang dat de licenties niet verlopen zijn, de laatste firmware geïnstalleerd is en dat de security rating zo hoog mogelijk is. Daarnaast is het belangrijk dat alle features om het netwerk te beschermen zijn geactiveerd.

Security Rating
Bij een firewall kun je de overall score zien van de firewall-oplossing. Alle punten die hier beschreven staan, kunnen worden opgepakt door het verbeteren van de configuratie of het verder uitbreiden van licenties en functionaliteiten.

Firmware-updates
We controleren of de firewall draait op de laatste firmware. Ons advies is om de laatst beschikbare firmware voor productieomgevingen te installeren.

VPN-encryptie en -authenticatie
Lage VPN-encryptie verwijst naar het gebruik van zwakke encryptieprotocollen of -algoritmen in een VPN-verbinding. Dit kan de beveiliging van de VPN-verbinding aanzienlijk verminderen en het risico op onderschepping van gevoelige informatie vergroten. De VPN-encryptie dient voor de beveiliging van data op AES-256 te zijn ingesteld. Zodra er nog gebruik wordt gemaakt van 3DES en MD5 dienen deze VPN-verbindingen aangepast te worden.

Inkomend verkeer
We controleren welke externe IP-adressen gekoppeld zijn met interne servers. Zijn deze koppelingen nog actueel en kloppen de bijbehorende policies van Untrust -> Trust of Untrust -> DMZ nog?

Functionaliteiten
Gebruik van geavanceerde functies van de firewall, zoals IPS, content filtering en URL-filtering, is essentieel om de beveiliging van je netwerk te verhogen. Deze functies helpen bij het blokkeren van geavanceerde bedreigingen, het beschermen van gevoelige gegevens, het waarborgen van naleving van voorschriften en het optimaliseren van netwerkbeheer. Wordt er gebruikgemaakt van antivirus, web filtering, video filter, DNS-filter, en IPS op inkomende en uitgaande policies?

Licenties
Bij aankoop van een firewall-licentie is er vaak ook toegang tot software-updates en technische ondersteuning. Als de licenties zijn verlopen, heb je geen recht meer op deze services. We controleren daarom regelmatig of de licenties nog actief zijn.

End-of-life of end-of-sale
We controleren of het gebruikte device end-of-life of end-of-sale is.

Netwerkscan
Switch hardening is het proces waarbij een netwerkswitch wordt beveiligd door verschillende beveiligingsmaatregelen te implementeren. Zo wordt het risico op ongeautoriseerde toegang of aanvallen kleiner. 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 netwerkscan onderzoeken we hoe het netwerk geconfigureerd is en of er bijvoorbeeld switch hardening is toegepast.

Installatie securityupdates & firmwareupdates
Voor een goede beveiliging is het belangrijk dat de firmware van netwerkapparatuur up-to-date is, vooral de apparaten die met het internet zijn gekoppeld. Hierbij kijken we naar het apparaat, op welke locatie die staat, of deze geïnstalleerd is en of het device beschikbaar is. Deze scan voeren we uit op de volgende apparaten:

- Firewall
- Core switches
- Edge switches
- Fysieke servers
- SAN
- NAS
- Wifi Controllers
- Wifi Access Points
- Beveiligingscamera's
- Printers

Status van Microsoft Defender for Endpoint
De serveromgeving en de werkplekken moeten voorzien zijn van antivirussoftware met de laatste updates. Het is daarnaast van belang dat de systemen regelmatig worden gescand op mogelijke bedreigingen. In de scan onderzoeken we of dit correct is ingericht met Microsoft Defender for Endpoint.

Privéapparaten
Naast Intune bevat Microsoft Defender for Endpoint ook een controle op privéapparaten. We onderzoeken of conditional access is ingericht en of er een accuraat overzicht is van privé apparaten.

Status 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. Via PingCastle zien we de algehele status van de Active Directory gebaseerd op verschillende indicatoren.

Binnen de Active Directory scannen we de volgende zaken:

Server inventarisatie: OS-versie, patches level, etc.
In de scan onderzoeken we welke Windows-versies gebruikt worden in de omgeving en of deze zijn gepatcht naar de laatste versie. Er zijn een aantal servers waarvan de Windows Server-versie end-of-life is. Daarnaast hebben meerdere servers niet de laatste patches geïnstalleerd.

Start-up datum
We onderzoeken wanneer de servers zijn opgestart. Als dit meer dan 30 dagen geleden is, dan zijn bij de recente OS-versie niet de laatste updates geïnstalleerd. Updates bevatten vaak beveiligingspatches die bekende kwetsbaarheden in het besturingssysteem dichten. Door deze patches te installeren, zorg je ervoor dat je computer minder vatbaar is voor aanvallen van hackers en malware.

Printspoolers
We onderzoeken of de printspoolerservice uitgeschakeld is op alle servers behalve de printservers. In de printspooler zitten een aantal beveiligingslekken die je zeker niet wilt hebben op bijvoorbeeld domain controllers.

Windows Firewall
De Windows Firewall biedt een basisniveau van bescherming tegen ongeoorloofde toegang tot je computer vanaf het internet of een ander netwerk. De firewall kan inkomende en uitgaande verbindingen blokkeren op basis van vooraf gedefinieerde regels en instellingen. We controleren welke firewalls actief zijn.

MB-versies
Het netwerk wordt onderzocht op welke SMB-versies er gebruikt worden. Het advies is om SMBv1 nergens meer te gebruiken, omdat dit een verouderd protocol is. Een van de grootste problemen met SMBv1 is dat het geen ondersteuning biedt voor moderne beveiligingsprotocollen zoals encryptie en digitale certificaten. Hierdoor kunnen aanvallers het protocol gebruiken om ongeautoriseerde toegang te krijgen tot systemen om gevoelige informatie te stelen.

Encryptie
We controleren of Bitlocker geactiveerd is op servers of werkplekken.

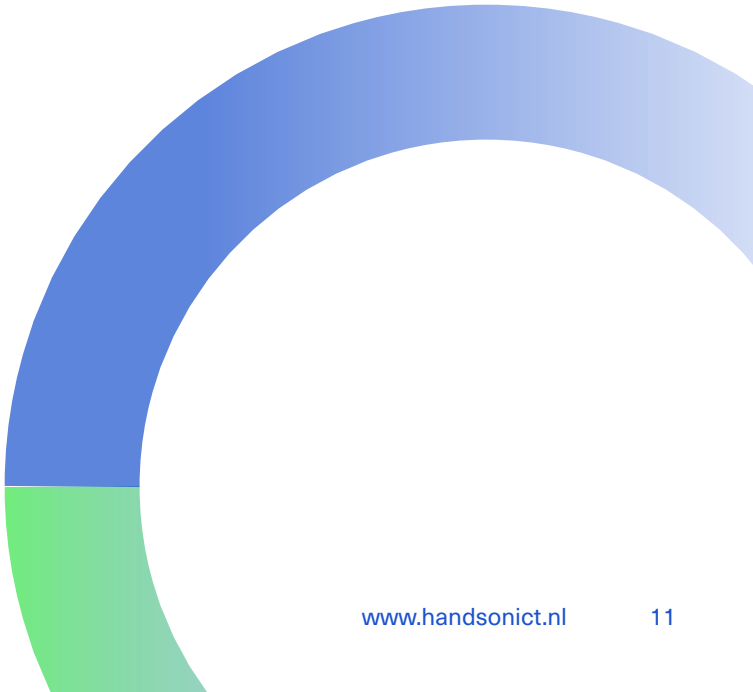
Antivirus
Een server kan vatbaar zijn voor malware, virussen, wormen, Trojaanse paarden en andere schadelijke software. Antivirussoftware helpt om deze bedreigingen op te sporen en te elimineren voordat ze de server kunnen beschadigen of gevoelige informatie kunnen stelen. We controleren of de antivirus correct is ingeregeld.

Status Azure Active Directory

Ping Castle Cloud is een tool die is ontworpen om snel het Azure AD-beveiligingsniveau te beoordelen met een methodologie die is gebaseerd op risicobeoordeling en een volwassenheidskader. De tool is niet gericht op een perfecte evaluatie, maar eerder op een efficiëntiecompromis. Vanuit hier kunnen we in detail eventuele aandachtspunten verder bekijken.

De volgende onderdelen worden uitgelezen:

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



Office 365-security

Als laatste stap lichten we de verschillende onderdelen binnen Office 365 toe.

Office 365 Recommended Configuration Analyzer (ORCA)
Office 365 Recommended Configuration Analyzer (ORCA) is een tool die we gebruiken om de configuratie van Office 365-implementaties te controleren en te optimaliseren. Het is een belangrijke tool voor organisaties die Office 365 gebruiken, omdat het problemen in de configuratie 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 op PowerShell gebaseerd 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 biedt 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 gebruikmaakt van Microsoft Authenticator voor het afdwingen van Multifactor Authentication.

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 Office 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.

Failed sign ins
Het is verstandig om periodiek de failed sign-ins te beoordelen. Grote aantallen foutieve inlogpogingen kunnen wijzen op een (geautomatiseerde) aanval op accounts. We verstrekken een overzicht van apps met een lagere (<80%) success rate.

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.

Overzicht VPN-gebruikersaccounts
De laatste stap in de Office 365 Security Scan is het aanmaken van een overzicht van medewerkers die de mogelijkheid hebben om met een VPN-verbinding toegang te krijgen tot jullie omgeving.

Stap 2
Rapportage en advies

Op basis van de Security Health Scan ontvang je een rapportage met hierin geprioriteerde aanbevelingen om de juiste maatregelen te nemen 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 eventueel 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.

Vervolgstappen
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 projectplan. 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.

Met het doorvoeren van de eerste nodige aanpassingen kunnen we vervolgens het securityniveau van jouw organisatie naar een hoger plan tillen: een waterdichte IT-security.

Stap 3

Inrichting security 2.0

In deze fase gaan we, afhankelijk van het adviesrapport en jullie wensen en beschikbare budgetten, aan de slag met de uitvoering van het projectplan: de securityproducten of diensten die ingericht moeten worden om de IT-security naar een (nog) hoger niveau te krijgen.

Producten en diensten waar je aan kunt denken bij het verbeteren van je IT-security zijn:

- Firewalls inrichten of instellen
- Mobile Device Management inzetten
- MFA instellen
- Conditional access toepassen
- Anti-spam- / Anti-virusoplossingen toepassen
- Inrichting sensitivity labels
- Phishingtest
- Pentest
- Awareness trainingen voor medewerkers
- Governance plan opstellen
- Data recovery plan opstellen

Stap 4

Periodieke security health scans

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 een periodieke scan op je omgeving uit, zodat je ook in de toekomst verzekerd bent van een veilige omgeving. Dit is dezelfde scan die we uitvoeren bij de 0-meting, waardoor we gedurende de tijd inzicht krijgen in de verbetering van de scores binnen de diverse onderdelen van de scan.

Stap 5
Monitoring & support

Naast de health scans richten we diverse monitoringstools in om te zorgen dat bedreigingen van buitenaf direct en proactief worden gesignaleerd en opgelost. Op deze manier kunnen we tussen de periodieke metingen door de omgeving in de gaten houden en proactief ingrijpen op het moment dat dit nodig is. Denk hierbij bijvoorbeeld aan endpoint detection, onderhoud, en het doorvoeren van updates. Let op: het maken van back-ups is geen onderdeel van YourSecurity.

Een aantal zaken die we vast opnemen in onze monitoring zijn:

- Firewall
- ORCA-rapportage (Exchange-omgeving)
- Compliance analyzer

Support

Zijn er buiten de tussentijdse metingen om vragen, dan zijn onze supportmedewerkers beschikbaar om je te helpen.

Onze supportmedewerkers zijn elke werkdag van 07.30 tot 17.30 uur bereikbaar en staan voor gebruikers klaar om vragen te beantwoorden of verstoringen op te lossen.
Iedere melding die bij ons binnenkomt, wordt geregistreerd in ons ticketsysteem. Op basis van de informatie gegeven door de gebruiker wordt er een classificatie gemaakt van het type melding en de impact van het incident. Vervolgens gaan wij direct aan de slag om de melding naar behoren op te lossen.

Zijn er technische issues met andere device gerelateerde componenten zoals printers of tablets? Ook daarvoor biedt Hands on ICT support.

Service levels

De algemene service levels van Hands on ICT zijn beschreven in de Service Level Agreement (SLA). In deze dienstbeschrijving wordt benoemd welke zaken specifiek voor de YourSecurity-dienst van toepassing zijn.

Servicewindow
Binnen de YourSecurity-dienst is het service window gelijk aan de kantoortijden: van maandag tot en met vrijdag van 07:30u tot 17:30 uur.

Periodieke scans
Periodieke scans vinden standaard 4 keer per jaar plaats. Dit is in feite een scan die vergelijkbaar is met de 0-meting, waarbij we de voortgang meten, inclusief het effect van de aanpassingen die zijn doorgevoerd. Op basis hiervan krijgen we inzicht in de status van de IT-security door de tijd heen en kunnen we op basis hiervan gaan werken met een roadmap voor de toekomst.

Rapportage
Na iedere scan ontvang je een uitgebreide rapportage met hierin de resultaten en aanbevelingen. Deze zullen we net als bij de 0-meting gezamenlijk bespreken en eventuele acties bepalen.

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

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

www.handsonict.nl

Powered by Hands on ICT
your365