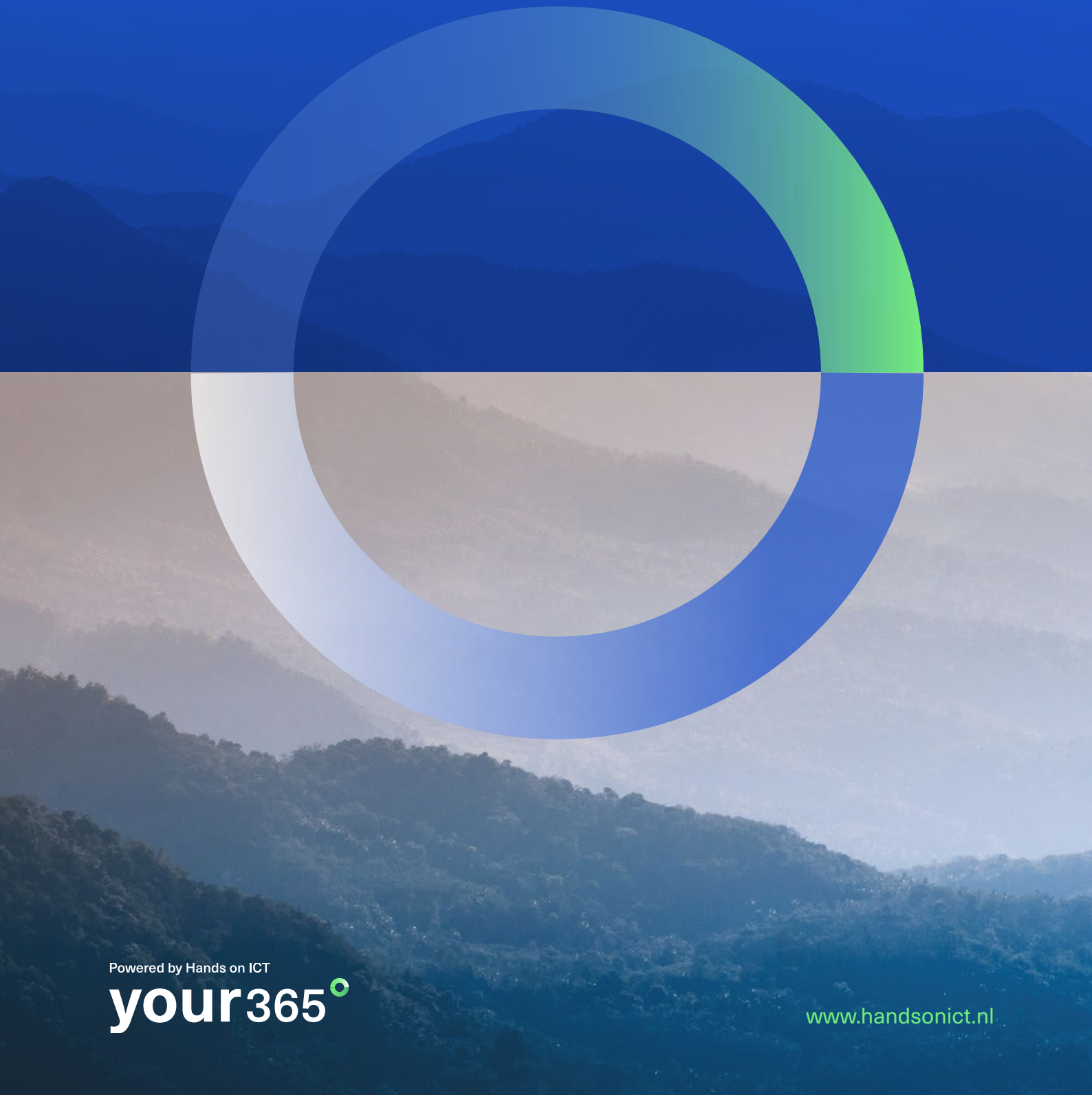
Hands on ICT
Dienstbeschrijving
YourSecurity

Slimme ICT-oplossingen voor succesvolle business



Powered by Hands on ICT

your365°

www.handsonict.nl

Inhoud

01	YourSecurity	3
02	In 3 stappen naar een verbeterde IT security	6
	Stap 1 - Security Health Scan	8
	Stap 2 - Security Optimalisatie	10
	Stap 3 - Security Management	11
03	Voorwaarden & condities	12

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.

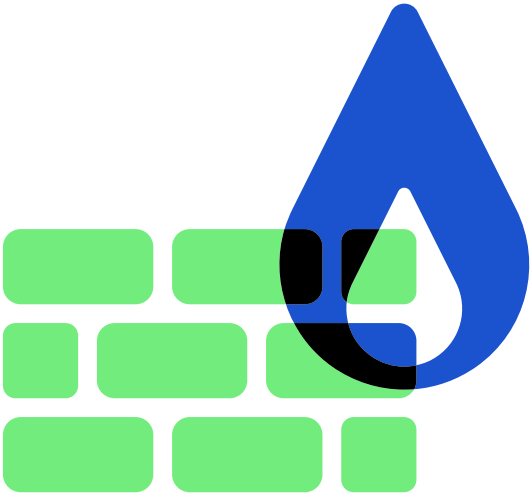
Hands on ICT zet met YourSecurity volledig in op het voorkomen van cyberaanvallen en het verkleinen van de risico's. We hanteren hierbij het NIST-framework én de Zero Trust-aanpak. Deze twee modellen benaderen IT-security vanuit een andere invalshoek, waardoor we een stabiele basis voor onze dienstverlening 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 het voorkomen van schade door 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 3 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. 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.

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

Stap 1 Security Health Scan

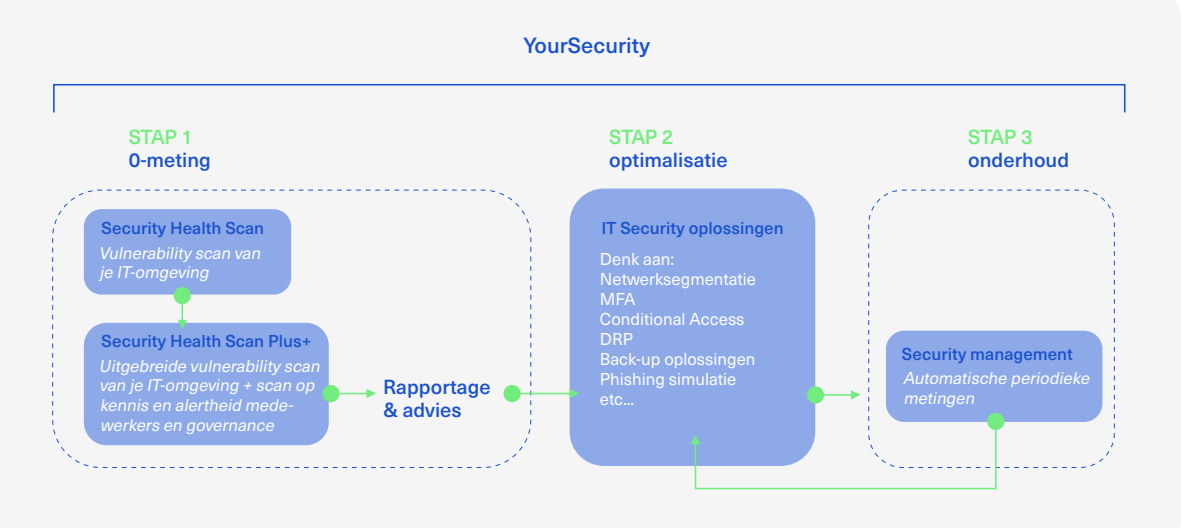
Wil je direct aan het slag met het verbeteren van je IT security? Dan is het verstandig om te beginnen met één van de Security Health Scans die we aanbieden. We voeren hier een 0-meting uit van je gehele IT-omgeving, bekijken de processen om security te borgen en zien zo waar de grootste security issues 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.

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.



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 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.

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 drie niveaus: mens, proces en techniek.

We bieden hiervoor twee verschillende scans aan:

- Security Health Scan
- Security Health Scan Plus+

Met beide scans brengen we de huidige status van je omgeving en IT security in kaart. Onderstaand vind je meer informatie over beide scans.

Security Health Scan

Met deze scan krijg je direct inzicht én controle over de veiligheid in je netwerk en systemen door het scannen van meer dan 100.000 kwetsbaarheden.

Ongeacht of je IT zelf beheert of dat dit wordt uitbesteed, deze scan is een uiterst effectieve manier om inzicht te krijgen in hoe veilig je bent tegen externe bedreigingen om vervolgens kwetsbaarheden te kunnen verhelpen.

Onze cloudscanners scannen de openbare netwerken en systemen, die toegankelijk zijn via het internet. Door één of meer Scanner Appliances te installeren in je lokale omgeving, achter de firewalls, kunnen we het gehele netwerk scannen, zelfs als de IT-omgeving zich op verschillende fysieke locaties bevindt. Alle scangegevens die door onze Scanner Appliances worden verzameld, worden gepresenteerd in ons Security Center.

We zetten deze scan dus enerzijds in om een startpunt te bepalen van de status van de algehele IT security. Anderzijds is dit een terugkerend onderdeel van YourSecurity om ook tussentijds een beeld te krijgen van de status van de omgeving. Daarom zetten we deze scan ook in als een recurring onderdeel van je gehele IT security. Meer informatie hierover vind je bij onze dienst Security Management.

Samenvatting Security Health Scan

De scan bestaat uit een viertal onderdelen:

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

Leaflet Security Health Scan

Security Health Scan Plus+

Met onze Security Health Scan Plus+ scannen we je omgeving naast de al zeer uitgebreide Security Health Scan op nog meer essentiële onderdelen om je IT Security naar een hoger niveau te tillen.

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, boven op onze reguliere scan.

Samenvatting Security Health Scan Plus+
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

Leaflet Security Health Scan

Uitkomsten Security Health Scan

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 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 betrouwbare en veilige IT security.

Stap 2
Security Optimalisatie

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.

Leaflet Security oplossingen

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

- Firewalls optimalisatie
- Mobile Device Management
- MFA optimalisatie
- Conditional access
- Endpoint Detection & Response
- Anti-spam- / Anti-virusoplossingen
- Phishing simulatie
- Awareness trainingen voor medewerkers
- Governance plan opstellen
- Data retentie & recovery
- Patch- & update beleid

Stap 3
Security Management

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.

Naast de periodieke scans die we uitvoeren binnen Security Management kunnen we diverse monitoringstools inrichten om te zorgen dat kwetsbaarheden 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.

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

- 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.
- Cloudomgeving: Microsoft Azure

Leaflet Security Management

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.

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
info@handsonict.nl
www.handsonict.nl
+31(0)88 - 181 1300

Weesp
Nesland 5a
1382 MZ Weesp

Zwolle
Schrevenweg 5
8024 HB Zwolle

Venlo
Prinsessesingel 20-26
5911 HT Venlo

Wormerveer
Vrijheidweg 38
1521 RR Wormerveer

Powered by Hands on ICT
your365

www.handsonict.nl