Hands on ICT
Security Audit

Vanuit een gedegen 0-meting naar een volledige security roadmap

www.handsonict.nl

Security Audit

Til je IT-beveiliging naar een hoger niveau

Met YourSecurity bieden wij diverse Securitydiensten aan waarbij we beheer en beveiliging van je organisatie overnemen, monitoren en/of verbeteren. De Security Audit is hierin cruciaal. Bij de Security Audit voeren we een totale IT Security 0-meting uit van je organisatie zodat je de IT-beveiliging van je organisatie naar hoger niveau kunt tillen. Hierbij richten we ons op technische inrichting van je ICT-omgeving maar ook op de mens & beleid kant van IT Security.

Wat is de Security Audit?

In de Security Audit onderzoeken we de belangrijkste facetten rondom IT Security en krijgen we een beeld van de huidige situatie. Met deze 0-meting hebben we een concrete set aan adviezen en aanbevelingen om je IT Security beter in te richten.

Naar aanleiding van de Security Audit wordt een rapport opgesteld met het doel om te voorzien van relevante en bruikbare inzichten om de organisatie te wapenen tegen beveiligingsrisico's. In dit heldere rapport geven we advies over de noodzakelijke verbeterpunten, welke impact de verbeterpunten hebben op de ICT-omgeving en de organisatie, en welke investeringen nodig zijn om deze punten te realiseren. We komen dit rapport op locatie presenteren en toelichten. De rapportage en het advies zijn inbegrepen in de eenmalige investering van de Security Audit.

Welke onderdelen zitten er in de Security Audit?

Bij het uitvoeren van de Security Audit worden de volgende onderdelen uitgelezen:

1. Systemen & netwerk(en)
2. Cloudomgeving (Microsoft Azure)
3. Active Directory
4. Endpoints
5. Microsoft 365
6. Security Awareness medewerkers
7. Governance & NIS2

Alle onderdelen worden hierna in detail beschreven.

1. Systemen & Netwerk

In dit onderdeel worden de kwetsbaarheden binnen je systemen & netwerk proactief geïdentificeerd en verholpen. We spreken ook wel van een vulnerability scan. Met de vulnerability scan worden de in gebruik zijnde IT-componenten geanalyseerd op mogelijke bedreigingen voor de bedrijfsvoering van je organisatie.

Systeemscan

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, om kwetsbaarheden in de webserverconfiguratie, SSL/TLSimplementaties en andere web technologieën te vinden.

Scan op netwerkapparaten

Een goed ingerichte 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 scan

Naast deze onderdelen voeren we ook een netwerk hardening scan doorgevoerd. 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.

2. Cloudomgeving (Microsoft Azure)

Cloud architecturen worden steeds complexer. 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.

3. Active Directory

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.

In de audit voor Active Directory worden diverse onderdelen uitgelezen, waaronder:

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

4. 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 beschermd worden met de nieuwste software.

In de audit voor Endpoints worden diverse onderdelen beoordeeld, waaronder:

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

5. 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?

Voor de audit van Microsoft 365 gebruiken we diverse audit methoden en tools, waaronder:

Office 365 Recommended Configuration Analyzer (ORCA)

ORCA is een tool die we gebruiken om de configuratie van Microsoft 365 e-mailimplementatie te controleren en te optimaliseren. Het identificeert problemen in de e-mailconfiguratie van Office 365 en verbetert de prestaties, beveiliging en beschikbaarheid van de service.

Microsoft Compliance Configuration Analyzer (MCCA)

MCCA haalt de huidige configuraties van je tenant op en valideert deze tegen de aanbevolen best practices van Microsoft 365. Het biedt een statusrapport om de configuratie van Microsoft 365 te verbeteren, gebaseerd op belangrijke voorschriften en normen voor gegevensbescherming.

Identity Secure Score

Identity Secure Score, ontwikkeld door Microsoft, helpt organisaties bij het verbeteren van de beveiliging van identiteiten en toegangscontrole. Deze tool is beschikbaar via het Microsoft 365 Security Center en biedt evaluaties en verbeteringen op basis van best practices.

Daarnaast kijken we naar de inrichting van diverse configuraties, waaronder:

Multifactor Authentication

We controleren in de scan of je organisatie momenteel gebruikmaakt van MFA en de juiste authenticatie- en verificatiemethoden hanteert.

Conditional Access

Conditional Access policies kunnen worden gebruikt om onder bepaalde voorwaarden toegang tot de Microsoft 365-omgeving toe te staan, zoals locatie, apparaat of gebruiker. We scannen welke policies er zijn en hoe deze zijn ingericht.

Azure Active Directory Risk Detection)

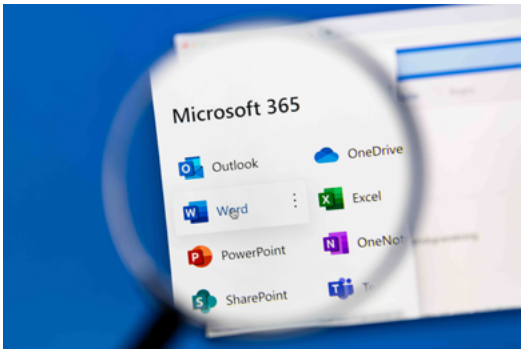
In een Microsoft 365-omgeving is de detectie van riskante aanmeldpogingen standaard niet ingeschakeld. We adviseren dit altijd in te schakelen voor beter inzicht.

Overzicht van Risk Detections

We onderzoeken welke accounts door Azure als 'at risk' zijn gemarkeerd.

OAuth-applicaties

We maken een overzicht van de applicaties die zijn toegevoegd aan de tenant. Dit varieert van beperkte toegang tot volledige toegang tot mailboxen.



6. Security Awareness 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.

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.

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. Leer ze bijvoorbeeld phishing e-mails te identificeren en te rapporteren en altijd alert te zijn op de bedreigingen. Binnen dit onderdeel van de audit beoordelen of er voldoende aandacht is voor het trainen van je medewerkers op het gebied van cybersecurity. Daarnaast adviseren we welke stappen zinvol zijn om de security awareness van je medewerkers te vergroten.

7. Governance en 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.

In dit onderdeel van de Security Audit bekijken we welke documentatie al beschikbaar is binnen jullie organisatie. Daarna leggen we jullie huidige situatie naast de nieuwe NIS2 richtlijnen en geven hierbij een advies zodat je weet welke stappen je nog moet ondernemen om compliant te zijn. In het adviesgesprek zal NIS2 ook worden meegenomen.

De Security Audit in 4 stappen

Van voorbereiding tot adviesgesprek; hieronder vind je de stappen die we gaan ondernemen om een Security Audit voor je te draaien.

Stap 1 – Scoping & voorbereiding

We verzamelen informatie over je IT-infrastructuur en identificeren de belangrijkste risico's die we wilt aanpakken. Hierbij moeten we, indien niet al van toepassing, toegang krijgen tot de juiste systemen. Daarnaast moet de benodigde documentatie en gegevens beschikbaar zijn voor de audit vanuit de klant zoals beleidsdocumenten, configuraties, gebruikerslijsten en andere relevante informatie.

Stap 2 - Uitvoering van de audit

Onze ICT-consultants voeren een grondige beoordeling uit van je IT-omgeving. Dit omvat het verzamelen van bewijsmateriaal (documentatie, screenshots, configuratiebestanden) en het uitvoeren van technische tests en analyses.

Stap 3 – Rapportage & Advies

Op basis van de Security Audit 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. 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.

Stap 4 – 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.

De voordelen van de Security Audit

De Security Audit biedt essentiële inzichten en bescherming door inzichtelijk te maken hoe je huidige beveiliging ervoor staat. Zaken die moeten worden aangepakt worden adresseert. Zo kan een gedegen security roadmap worden opgezet om de algehele IT-beveiliging te versterken en helpen je organisatie om cyberdreigingen effectief te beheren. Daarnaast weet je exact welke stappen je moet gaan zetten om NIS2-compliance te worden.

- Door de audit worden **potentiële kwetsbaarheden** blootgelegd.
- Het auditrapport biedt **waardevolle aanbevelingen** voor verdere verbetering van de IT-beveiliging.
- Zorgt ervoor dat je voldoet aan **NIS2** en andere relevante wet- en regelgeving.
- Versterkt de maatregelen ter **beveiliging van bedrijfs- en klantgegevens.**
- Met de **uitgebreide rapportage** worden kennis en alertheid verhoogd over cybersecurity.

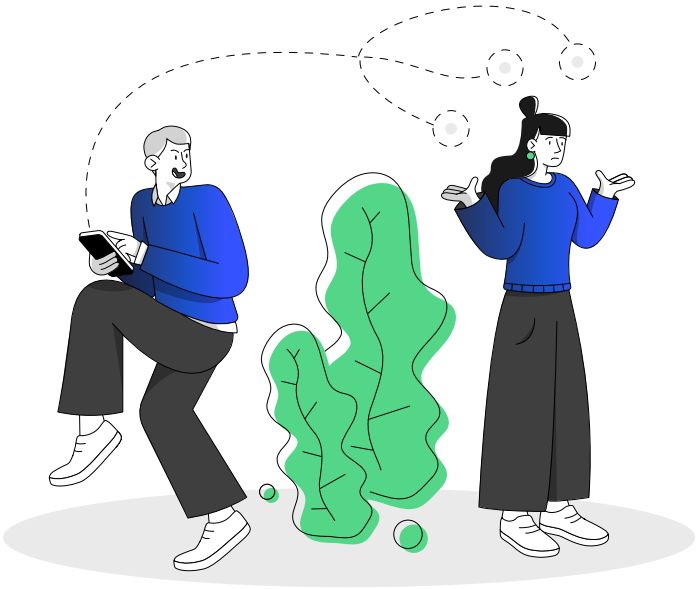
Pricing

De Security Audit wordt slechts eenmalig in rekening gebracht. De prijs van de Security Audit is afhankelijk van een aantal zaken. Heeft Hands on ICT bijvoorbeeld al toegang tot jullie omgeving of moeten de systemen nog ingericht worden voor toegang, hoeveel endpoints zijn er ingericht, hoe zit de tenant in elkaar (aantal domeinen etc). Onze ICT-consultants zullen in de offertefase een inventarisatie doen om de exacte prijs te bepalen.

yoursecurity

Security Audit: Onderdeel van YourSecurity

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. Een belangrijk onderdeel hiervan is Managed Security waarbij we beheer en beveiliging van IT-systemen en netwerken overnemen.
Dit omvat een breed scala aan beveiligingsdiensten en -oplossingen die continu worden beheerd en bewaakt om dreigingen te detecteren, te voorkomen en erop te reageren.



Meer informatie

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