handsonict

whitepaper

Een veilige ICT-omgeving, hoe regel je dat?

Aandachtspunten binnen IT-security

Het belang van goede beveiliging

ICT-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 omgevingen. Wanneer er door digitale muren van je organisatie heen wordt gebroken heeft dat grote impact op je organisatie. Het voorkomen van een aanval of hack vraagt hoge eisen aan de security van je ICT-omgeving. Het is niet alleen de techniek die de beveiliging van je ICT-omgeving vormt, ook de mensen en de processen binnen je organisatie spelen hier een belangrijke rol in. In deze whitepaper nemen we je mee in alle belangrijke aspecten van ICT-security zodat jij je organisatie beter weerbaar maakt tegen Cybercriminaliteit.

In deze whitepaper ontdek je:

- De zwakke plekken binnen de ICT-omgeving
- De evolutie van ICT-security
- Een veilige ICT-omgeving: het BDA-principe als leidraad
- Hoe Hands on ICT je kan helpen met je IT-beveiliging

De zwakke plekken binnen de ICT-omgeving

Veel bedrijven benaderen ICT-security vanuit het technische aspect, maar ICT-security gaat verder dan dat. Naast technologie gaat ICT-security ook over de mensen en processen binnen een organisatie. Bij techniek gaan we voor een ICT-omgeving die goed is ingericht, deugdelijk is beveiligd én voorzien is van de laatste versies van applicaties en software. 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. Ten slotte is de mens, oftewel de medewerkers, een belangrijke factor binnen ICT-beveiliging. Voor een sterke cybersecurity is het van belang dat medewerkers het bewustzijn hebben dat ze ook een belangrijke rol spelen in de beveiliging van hun organisatie en dat een mogelijke inbreuk op je ICT-omgeving vrijwel altijd onverwachts plaatsvindt. De medewerkers moeten ten aller tijden 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.

De mens

Binnen het beveiligingsproces zijn medewerkers vaak de zwakste schakel. Het menselijk handelen vormt bij meer dan 70% van alle lekken en hacks de belangrijkste oorzaak. Dit komt mede doordat het bij medewerkers vaak schort aan kennis over online veiligheid. Zo blijkt dat maar 3 op de 10 medewerkers zijn kennis op online veiligheid als (zeer) goed schat. Daarnaast wordt de kans op cybercriminaliteit door 7 op de 10 medewerkers als niet hoog ingeschat. Terwijl de kans op cybercriminaliteit in werkelijkheid alsmaar groeit. Het onjuiste gedrag en de onwetendheid van medewerkers kan hiermee de kans op een beveiligingslek in je ICT-omgeving enorm vergroten.

ICT-oplossing: Organiseer Security Awareness trainingen

Om dit te voorkomen is het belangrijk dat medewerkers altijd alert zijn en blijven op alle gevaren die op hen af kunnen komen. Om dit te realiseren kun je je mensen trainen op alertheid en awareness. Een goede security awareness training kan de risico's op een data-inbreuk beperken. De Security Awareness trainingen van Hands on ICT maken je medewerkers wegwijs om digitaal veilig aan de slag te gaan.

ICT-oplossing: Voer phishingtesten uit

Daarnaast kan je de alertheid van je medewerkers testen via een phishingtest. Bij een phishingtest kan er een levensecht scenario gesimuleerd worden, waarin een medewerker een schijnbaar legitieme e-mail ontvangt van bijvoorbeeld een collega. Hierin plaatsen wij dan een onschuldige link, die normaliter tot een cyberaanval had kunnen leiden. Aan de hand van een phishingtest weet je zo al snel of je medewerkers bewust zijn van frauduleuze e-mails en of je hierop verdere actie moet ondernemen.

De processen

Heldere en juiste processen binnen een organisatie zijn van belang voor het beveiligen van je ICT-omgeving. Maar wat als deze processen niet duidelijk zijn vastgelegd binnen het governancebeleid van een organisatie? Het governancebeleid is bedoeld om de processen die je organisatie veilig houden te borgen. Een onduidelijk of incompleet governancebeleid kan een zwakke plek vormen binnen de organisatie. Hierdoor zijn de processen rondom het borgen en delen van informatie niet op orde en blijft de kans op een datalek of cyberaanval sterk aanwezig. Daarnaast zijn medewerkers niet voldoende op de hoogte over de ICT-beveiliging, waardoor ze niet weten hoe te handelen bij eventuele cyberaanvallen. Het resultaat: een organisatie die niet sterk voorbereidt is vóór een aanval, tijdens een aanval of na een aanval.

Als het beleid wel vast staat, kan een organisatie alsnog een aantal dingen uit het oog verliezen. Het is namelijk belangrijk om beleid te toetsen en hier controles op uit te voeren. Wanneer je een vastgelegd proces nooit toetst, is het niet duidelijk welke acties er periodiek genomen moeten worden om de beveiliging op niveau te houden.

Tegenwoordig kunnen we overal en altijd werken, het zogeheten hybride werken. Zowel persoonlijk als zakelijk worden er meerdere mobiele devices gebruikt om werk te verrichten. Denk bijvoorbeeld aan laptops, pc's, tablets en smartphones. Maar wat als er een persoonlijke laptop of smartphone niet up-to-date is, maar wel wordt gebruikt om werkzaamheden uit te voeren? Hoe ver kun je überhaupt gaan in het beveiligen van een privé apparaat? Zaken waar je vooraf een duidelijk proces over moet vastleggen.

ICT-oplossing: Stel een governancebeleid op

Om dit te voorkomen is het als organisatie belangrijk een sterk governancebeleid te schrijven en alle processen concreet vast te leggen. Daarnaast moet dit duidelijk gecommuniceerd worden naar de medewerkers, zodat zij op de hoogte zijn van de ICT-beveiliging en het hen helpt om op een veilige wijze digitaal te werken. Om zeker te zijn dat je niets vergeet in het governancebeleid is het raadzaam om dit samen met een ICT-partner op te stellen.

ICT-oplossing: Maak Mobile Device Management een prioriteit

Altijd en overal werken is tegenwoordig vanzelfsprekend, maar als organisatie is het van belang dat je weet hoe je hiermee omgaat en hoe je de juiste beveiligingsmaatregelen treft. Het is belangrijk om dat verantwoord te doen en dat de omgang met privacygevoelige informatie volgens een proces verloopt. Om je bedrijfsgegevens veilig te stellen moeten de besturingssystemen up-to-date zijn en alle mobiele devices beschermt worden met de nieuwste software. Hiermee bescherm je medewerkers die (onbewust) onveilig omgaan met bedrijfsdata en ben je als organisatie beter beschermd tegen virussen en malware. Het opstellen van een overzicht van mobiele devices en diens beveiliging wordt georganiseerd in het 'Mobile Device Management'.

De techniek

Een gevaar binnen de techniek is dat de software van je organisatie verouderd raakt. Wanneer alles binnen je organisatie prima verloopt, wil dat niet zeggen dat alles up-to-date is. Denk hierbij aan nieuwe versies van je applicaties, besturingssystemen of devices. Daarnaast kunnen er ook security-gerelateerde risico's zijn die nog niet aan het licht zijn gekomen. Wist je namelijk dat een cyberaanval veel voorbereiding vergt? Vaak zijn de criminelen al enkele maanden aanwezig in je ICT-omgeving, voordat ze overgaan tot het platleggen van al je apparaten en systemen. Het is daarom van groot belang om de ICT-infrastructuur onder de loep te nemen en ervoor te zorgen dat je systemen up-to-date en in beheer zijn. Een onjuiste perceptie over de veiligheid van ICT-security kan een gevaar vormen. Laat je daarom goed adviseren en informeren door een ICT-partner die oog heeft voor de beveiliging van jouw omgeving. Enkele basale toepassingen zouden al kunnen zorgen voor een goede start, denk hierbij aan:

ICT-oplossing: Voer een Pentest uit

Om het risico op een aanval te verminderen, is het goed om af en toe in de rol van cybercrimineel te kruipen. Bij een pentest wordt er geprobeerd om je omgeving binnen te komen, om zo vooraf eventuele zwakke punten binnen je ICT-omgeving op te sporen en te verhelpen. Dit wordt gedaan door een team van deskundigen en consultants op het gebied van cyberbeveiliging die proberen van binnenuit en buitenaf in te breken in je ICT-omgeving zonder ontdekt te worden. Hierdoor worden direct de kwetsbaarheden binnen een organisatie aangepakt nog voordat ze een probleem vormen. Een ICT-partner kan je goed helpen om jouw ICT-omgeving weer veilig te maken.

ICT-oplossing: Gebruik Microsoft Defender

Een andere effectieve oplossing om je organisatie beter te beveiligen en risico's te verminderen, is Microsoft Defender. De Microsoft Defender (ook wel 'Defender for Office 365 genoemd) is een uitbreiding op je Microsoft 365 abonnement die jouw ICT-omgeving beter beschermt tegen bedreigingen van buitenaf. De uitbreiding biedt extra beveiligingsfuncties voor je e-mail, bestanden en Office 365-toepassingen. Bijvoorbeeld, inkomende e-mailberichten worden niet alleen maar gecontroleerd op de inhoud, maar ook op de inhoud in de bijlagen en links in de tekst en bijlagen. Hierdoor is je Microsoft 365 omgeving nog beter beschermd tegen verschillende vormen van cybercriminaliteit.

ICT-oplossing: Multi-factor authenticatie instellen

Om jouw Microsoft 365 omgeving veiliger te maken is een Multi-factor authenticatie (MFA) tegenwoordig praktisch verplicht om te gebruiken. Hierdoor moeten gebruikers hun authenticiteit/identiteit op meerdere manieren verifiëren. Dit biedt een extra beveiliging waardoor een gebruiker niet zomaar toegang kan verkrijgen. Ook het beveiligen van de fysieke werkplek met de juiste software is van belang. Het is belangrijk om het besturingssysteem up-to-date te houden en de nieuwste software te gebruiken. Hierdoor wordt de kans op beveiligingsproblemen verminderd.

ICT-oplossing: Proactief beheer en monitoring

Een sleutel tot het vroeg herkennen van een mogelijk security-risico is het inrichten van proactief beheer en monitoring. Een monitoring-tool zorgt ervoor dat jouw ICT-omgeving met alle devices, netwerkapparatuur en software continu wordt gecontroleerd op downtime, verstoringen, maar ook op security-risico's. Wordt er iets vreemds gesignaleerd, dan gaat er meteen een melding naar ICT-specialisten die de melding gaan bekijken. Middels het proactief beheer worden de monitoring-meldingen dan nader bekeken en waar nodig wordt meteen geschakeld. Op deze manier kun je waarborgen dat zowel downtime om technische redenen, als downtime door security-risico's altijd in de kiem wordt gesmoord. Hands on ICT is een Managed Services Provider en is gespecialiseerd op het gebied van monitoring en beheer. Het beheer van Hands on ICT richt zich niet alleen op individuele werkplekken, maar ook op het beheer van gedeelde werkplekken, datacenters, netwerken, servers en tenants.

De evolutie van ICT-security

Vroeger was ICT-security nog vrij eenvoudig. Er was één kantoor met alle werkplekken en servers binnen de kantoorgrenzen. Destijds was het 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 binnen wilde dringen was die simpele controle voldoende om de omgeving te beschermen.

Tegenwoordig is dat anders en hebben (mobiele) devices steeds meer de mogelijkheid om een connectie te maken met jouw ICT-omgeving. Dat komt onder andere door the Internet of Things, Cloud, hybride werken, cloudapplicaties en BYOD (Bring Your Own Device). Hierdoor zijn er van buitenaf veel meer toegangspoorten tot jouw ICT-omgeving. Dit zorgt voor een lagere mate van controle. Daarnaast blijft de cybercriminaliteit zich ook flink innoveren: malware, phishing, cryptolockers, ransomware en CEO fraude zijn zaken die we dagelijks tegenkomen. Dit vraagt voor een sterker cybersecuritybeleid. Om dit te realiseren is het als organisatie belangrijk om aandacht te hebben voor het BDA principe (Before, During, After). Hierin kijk je 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.

Een veilige ICT-omgeving: het BDA principe als leidraad

Als je ICT-security serieus neemt, dan zorg je ervoor dat alles goed geregeld is aan de voorkant van je organisatie met de technologie, de processen en de medewerkers. Maar daarnaast is het ook van belang dat je weet wat je moet doen als er een aanval is geweest (bijvoorbeeld, wie ga je bellen?) en dat je aan de achterkant regelt dat de infiltratie stopt en je als organisatie kan blijven doorwerken (geen of zo min mogelijk downtime). Een te lange downtime kan namelijk zorgen voor desastreuze gevolgen.
Organisaties denken bij het beveiligen van hun ICT-omgeving vaak aan een anti-virus, firewall en VPN. Maar is dit voldoende? Om hier meteen antwoord op te geven: nee. Maar wat moet je dan doen om je ICT-omgeving beter te beveiligen? Dat gaan we je vertellen. Maar om te beginnen: zorg ervoor dat je je ICT-beveiliging op orde hebt vóórdat je te maken krijgt met een aanval.
We leggen het hier uit aan de hand van het BDA-principe (Before, During, After). Het is namelijk belangrijk om goed na te denken wat je vóór, tijdens en na een cyberaanval of inbreuk op je ICT-omgeving moet doen.

During: wat als er iets misgaat?

Stel dat er toch iets misgaat en je organisatie krijgt te maken met een aanval van buitenaf? Wat doe je dan tijdens een aanval? Dit proces heb je als het goed is vastgelegd in je governancebeleid. Via je securitycontroles en rapportages, zoals die van je mobile device management kun je ontdekken wat er misgaat. Wanneer er een potentieel security-risico wordt gedetecteerd, zijn er een aantal acties die je moet ondernemen. Wie ga je bijvoorbeeld bellen? En wat ga je doen om de infiltratie te minimaliseren? Daarnaast is het belangrijk dat je medewerkers weten hoe dit beleid uitgevoerd moet worden. Zorg er voor dat je medewerkers hier vooraf van op de hoogte zijn. Controleer daarnaast ook in je tools en rapportages dat er niet op meerdere plekken “infecties” zijn opgetreden. Net zoals we al jaren doen aan brandoefeningen, is het goed om ook bij dit beleid de proef eens op de som te nemen. Immers hoop je in geval van een brand er ook niet achter te komen dat je rookmelders defect zijn en je nooddeur op slot zit. Neem daarom periodiek je hele governancebeleid en BDA-procedure goed onder de loep.

After: hoe beperk en herstel je de schade?

Bij schade in je ICT-omgeving is je disaster recovery plan een belangrijk onderdeel om zo snel mogelijk alles weer ‘normaal’ te laten verlopen. Een goed disaster recovery plan zorgt normaliter voor een zo klein mogelijke inbreuk op bedrijfsdata en processen. Het disaster recovery plan heeft twee uitgangspunten: Recovery Time Objective (RTO) en Recovery Point Objective (RPO). De RTO is de tijd waarin de handelsprocessen weer in werking moeten zijn, zoals voor de ramp. RPO geeft de maximale tijdsperiode aan waarin bedrijfsdata verloren kunnen gaan tussen de laatste back-up en de aanval. Deze tijdsperioden kunnen verschillen per organisatie. Toch is het van belang dat je deze als organisatie vaststelt, omdat dit implicaties heeft voor de maatregelen die je treft in je disaster recovery plan.

Een ander belangrijk onderdeel van je disaster recovery plan is het maken van een back-up van je kritische bedrijfsdata en processen. Een goede back-up is essentieel om binnen afzienbare tijd een inbreuk op je ICT-omgeving te verhelpen.

Een back-up voldoet niet meer aan de huidige veiligheidseisen van je ICT-omgeving. Daarom is een goede strategie nodig. Een sterke back-up voldoet aan de stelregel: 3-2-1-1-0 voor een kopie van je kritische data en processen. De stelregel geldt als volgt:

- Maak 3 back-ups van je bedrijfsgegevens;
- Bewaar de back-ups op 2 verschillende locaties, zoals één interne- en één externe opslag;
- Zorg dat 1 kopie op een andere locatie staat dan waar de andere back-ups en originele data staat;
- Maak van de back-ups 1 offline back-up;
- Wees er zeker van dat 0 back-ups fouten bevatten, dus dat alle kopieën vrij zijn van bijvoorbeeld ransomware.

Een eerste stap in de goede richting is dus een goede back-up hebben. Net zoals bij je governance, moet je je back-up testen of het eenvoudig teruggeplaatst kan worden in je omgeving. Is dat niet het geval, dan wil je daar niet pas te laat achter komen.

Hands on ICT helpt je verder

Hands on ICT is als ICT-businesspartner actief in heel Nederland. Met 125 ervaren specialisten, verdeeld over drie locaties in het land, zijn we altijd dichtbij om jou te helpen met uiteenlopende ICT-vraagstukken. Wij zijn ervan overtuigd dat elke branche haar eigen uitdagingen kent en daarom vraagt om specifieke oplossingen en expertise. Daarom werken we bij Hands on ICT met specialistische brancheteams die zich focussen op (ICT-)uitdagingen en -oplossingen binnen hun branche.

Zo hebben we dankzij onze jarenlange ervaring (meer dan 25 jaar) uitgebreide kennis in huis van de specifieke uitdagingen binnen de IT-security. Als Microsoft Partner beschikt Hands on ICT over gespecialiseerde vaardigheden op het vlak van implementatie van security oplossingen binnen de Microsoft Suite.

Wil jij meer uit je ICT-omgeving halen en er voor zorgen dat deze zo veilig mogelijk is ingericht? Zowel op het gebied van techniek, proces als mens? Dan helpen wij je graag! Wij ondersteunen al een hoop organisaties met het afstemmen van het securitybeleid op de behoeften en wensen van organisaties en eindgebruikers.

Wil je meer weten? Schakel direct met onze ICT-specialisten en neem contact met ons op.

Neem contact op

Locaties: Weesp | Venlo | Zwolle
info@handsonict.nl
www.handsonict.nl