E-security: Onderneem Veiliger!

TRENDS

TRENDS ICT GROEP

www.trends.nl

Inhoudsopgave

Hoofdstuk 1

Waarom is e-security zo belangrijk?

Het bedrijfspand is voorzien van goede sloten. Alle ramen zijn anti-inbraak gemaakt. En er is een professionele alarminstallatie die inbrekers op afstand houdt. De fysieke beveiliging is misschien wel op orde, maar hetzelfde geldt vaak niet voor de beveiliging van computersystemen en digitale gegevens. Te vaak staan er virtuele achter- en voordeuren wagenwijd open waardoor kwaadwillenden ongehinderd naar binnen kunnen. En dat kan ondernemers op meerdere manieren de kop kosten. E-security is nu al van groot belang. Dat wordt de komende tijd alleen maar versterkt. Hoe houden ondernemers ook de virtuele achter- en voordeuren goed op slot? Moeten zij dat wel zelf doen of is het verstandiger om dat uit te besteden aan e-security experts? Het zijn vragen waarop in dit e-book antwoord wordt gegeven.

Tien miljard euro. Dat is de financiële schade die Nederlandse bedrijven en overheidsinstanties jaarlijks oplopen als gevolg van cybercriminaliteit, blijkt uit recent onderzoek uitgevoerd door het adviesbureau Deloitte. Het gaat daarbij om zowel de directe schade als de kosten die gemaakt moeten worden om bijvoorbeeld de levering van diensten en producten weer op gang te brengen.
Ook is er nog zoiets als reputatieschade als gevolg van een cyberaanval. Marktonderzoeksbureau TNS NIPO kwam in het voorjaar van 2015 eveneens met een onderzoek over e-security in het MKB. Een derde van de 529 ondervraagde ondernemers verwachtte dat het bedrijfsrisico door slechte cybersecurity in de komende vijf jaar zal stijgen. Het zijn slechts twee van de vele onderzoeken die de gevolgen van hackaanvallen en andere cybercriminele activiteiten in kaart hebben gebracht.

Hoewel de bedragen in de verschillende onderzoeken afwijken, staat één ding als een paal boven water: ondernemers die hun e-security niet op orde hebben, lopen kans op een aardige financiële aderlating.

Hoe gaan cybercriminelen te werk?

Waar zijn cybercriminelen op uit? In de praktijk gaat het om klantgegevens, financiële bedrijfsinformatie en data afkomstig van toeleveranciers. In zulke gevallen gaat het zowel om gerichte als 'brede' aanvallen van cybercriminelen. In het geval van gerichte aanvallen gaat het vaak om MKB-bedrijven die door hun activiteiten of producten erg aantrekkelijk zijn. Denk aan ondernemers die voor de defensie industrie werken of MKB'ers die over eigen vindingen en patenten beschikken.

Het Nederlandse MKB loopt grote kans op 'ongewenste intimiteiten' van cybercriminelen, als gevolg van zogenoemde 'brede aanvallen'. De meest bekende voorbeelden daarvan zijn: Distributed Denial of Service-aanvallen waardoor de website (de virtuele voordeur) onbereikbaar wordt en kwaadaardige software via mailtjes kan worden verspreid. De afgelopen maanden is met name dat laatste in opmars. Er gaat bijna geen dag voorbij of er stromen mailtjes binnen waarin wordt gevraagd om 'uw gegevens te wijzigen' door op een weblink te klikken of waarbij een 'belangrijk document' is bijgesloten.
Wie in dergelijke berichten trapt, kan rekenen op een

virus of zogenoemde 'ransomware'. Het virus kan er voor zorgen dat de ICT-systemen plat komen te liggen of dat er ongemerkt bedrijfsinformatie wordt verzameld en verstuurd naar kwaadwillenden. In het geval van ransomware worden bestanden versleuteld en in gijzeling gehouden.

Gegevens in gijzeling

Ransomware gaat openlijk te werk. Deze 'gijzelsoftware' doet precies wat de naam aangeeft: het versleutelt bestanden op het netwerk (en op de pc). Alleen na betaling aan de anonieme cybercriminelen worden de gegevens weer leesbaar. Tenminste: dat beloven de criminelen. Echter, de praktijk wijst uit dat het vaak niet het geval is, zoals een ondernemer onlangs merkte.

De ondernemer klikte op een bijlage in een mailtje dat afkomstig leek van zijn accountant. In plaats van de beloofde dringende financiële informatie, zat er ransomware in. In een mum van tijd werden alle bestanden op zijn laptop versleuteld en kwam er een mededeling dat hij binnen 72 uur moest betalen. Deed hij dat niet, dan kon hij naar zijn data fluiten. Gelukkig was zijn laptop toen niet met het netwerk verbonden. En bleven de bestanden op het netwerk veilig.

Hij besloot om niet in te gaan op de eisen van de gijzelnemers. Het resultaat: de ondernemer was de bestanden en het werk van de laatste maand op zijn laptop kwijt. Een recente back- up was helaas niet voorhanden.

Andere vormen van cyberrisico's

Ondernemers hebben helaas niet alleen te maken met cybercriminelen. De kans op onbedoelde 'datalekken' is even groot. Dan gaat het om bijvoorbeeld USB-sticks die in taxi's worden vergeten. Of gevoelige bedrijfsinformatie die naar een privé mailaccount (zoals Google Gmail) wordt gestuurd. Als dat privé account vervolgens wordt gehackt, dan is het hek ook van de dam. Henk Kamp, minister van Economische Zaken, kan over dat laatste meepraten. Hij stuurde allerlei regeringsdocumenten door naar zijn Gmail-account. Dat mag eigenlijk niet, maar het was wel zo makkelijk: hij kon hierdoor ook onderweg en thuis aan de slag. Helaas voor Kamp werd zijn Gmail-account gehackt. Een wapenfeit dat door de hackers in kwestie triomfantelijk aan de pers werd gemeld.

Wie kent de wet op datalekken?

Eind oktober 2015, ruim twee maanden voordat de meldplicht op datalekken werd ingevoerd, kwam security specialist Sophos met de uitkomsten van een onderzoek verricht onder 262 ICT-managers, werkzaam bij zowel commerciële organisaties als overheidsinstanties. De resultaten waren niet hoopgevend.

De meerderheid van de ondervraagden (58 procent) wist destijds niet van de komst van de meldplicht.
Uit het onderzoek bleek verder dat niet iedere organisatie, die vertrouwd was met de aankomende meldplicht, al een plan de campagne had opgesteld. Slechts 29 procent van hen had des-

tijds al actie ondernomen. Een groot aantal (44 procent) van de ICT-managers meldde dat hun organisaties nog adequate maatregelen zouden gaan treffen. Zonder dat daar overigens al vast-omlijnde plannen voor waren bedacht. 15 procent gaf ronduit toe dat er nog niets was geregeld of bedacht. Terwijl 13 procent moest bekennen dat het niet wist hoe er binnen de organisatie (lees: de directie) over het onderwerp werd gedacht.

Begin april 2016 bracht de Autoriteit Persoons-gegevens naar buiten dat er vanaf 1 januari 2016 al circa 1000 meldingen van datalekken waren gedaan.
Volgens Wilbert Tomesen, vicevoorzitter van de privacy waakhond, was dat aantal relatief laag. Volgens een inventarisatie van de AP zijn er in Nederland zo'n 130.000 organisaties die gevoelige data hanteren.

Voorkomen is beter dan genezen

Het Rotterdamse advocatenkantoor Kneppelhout en Korthals heeft eind 2015 vier 'belangrijke voorbereidende maatregelen' gepubliceerd die organisaties preventief kunnen nemen als het gaat om datalekken:

- Organisaties moeten verplicht een logboek bij houden voor datalekken. Hier vraagt de Autoriteit Persoonsgegevens naar wanneer zich een datalek voordoet.
- Kijk kritisch naar de fysieke inrichting van de organisatie en wie er (in- en extern) toegang heeft tot gevoelige gegevens.
- Maak een draaiboek voor wanneer zich een datalek voordoet.
- Zorg dat toeleveranciers de contractuele plicht hebben een datalek te melden. Een melding moet binnen 72 uur na ontdekking plaatsvinden. Als de leverancier dat niet meldt, krijgt u de boete.

Hoofdstuk 2

E-security zelf in het bedrijf regelen?

De BV Nederland heeft in 2015 circa 520 miljoen euro uitgegeven aan e-security, wat neer komt op 0,08 procent van het Bruto Binnenlands Product (BBP). Dat heeft het onderzoeksbureau Ponemeon Institute vorig jaar becijferd. De verwachting is dat die investeringen de komende jaren alleen maar groter worden. De noodzaak daartoe houdt gelijke tred: het aantal cyberaanvallen op allerlei soorten organisaties (van overheid tot grootzakelijk en MKB) stijgt explosief. Het is een heuse wapenwedloop tussen cybercriminelen en organisaties geworden. Een wapenwedloop waarin grote ICT-investeringen en –kennis belangrijke rollen spelen.

Een multinational of een grote overheidsinstantie geeft er jaarlijks miljoenen aan uit: e-security. Het gaat dan niet alleen om de aanschaf van speciale hard- en software. Bij dergelijke organisaties is bijvoorbeeld ook een batterij ICT-experts werkzaam (of ingehuurd) om de e-security op peil te houden.

Het zijn kosten die voor de gemiddelde MKB'er niet zijn te dragen. En toch is het voor ondernemers van levensbelang geworden dat de e-security van het bedrijf op orde is. Het is een kwestie van hetzij zelf regelen of het uitbesteden aan ICT-bedrijven.

Werkplekbeveiliging

Wie de e-security in eigen beheer wil houden, wordt geconfronteerd met een omvangrijk en kostbaar vraagstuk. Er is namelijk geen allesomvattende beveiliging oplossing voor de gehele ICT van het bedrijf. Allereerst is er de beveiliging van de zogenoemde 'clients': de apparaten waarmee met applicaties en data wordt gewerkt. Vroeger was dat nog redelijk overzichtelijk. Er stond hooguit één bureau-pc per werkplek met hier en daar een (netwerk)printer. Dat is inmiddels wat complexer geworden. In een gemiddelde onderneming is tegenwoordig een mix te vinden van bureau-pc's, laptops, smartphones en tablet computers. Op al die apparaten moet op zijn minst goede antivirussoftware zijn geïnstalleerd. Daarmee hou je zowel computervirussen als malware zoveel mogelijk buiten de deur. Ook moeten al die apparaten steeds met de laatste softwareversies zijn uitgerust.

Bij de mobiele clients is het ook verstandig om extra te investeren in de beveiliging, zowel van het apparaat zelf als de toegang tot bedrijfsapplicaties en –data. Zodat bij diefstal of verlies van bijvoorbeeld een tablet computer, er niet zomaar iemand aan de haal kan gaan met gevoelige informatie zoals klantgegevens of financiële data.

Serversystemen en netwerk

De tweede belangrijke ICT-component bestaat uit het netwerk en de verbindingen met de buitenwereld. Dan gaat het om bijvoorbeeld de netwerkservers en de bijbehorende centrale gegevensopslag. Ook hier is software tegen kwaadaardige programma's voor benodigd. Het netwerk zelf kent verschillende onderdelen die afgeschermd moeten worden voor ongewenste indringers. Een firewall (waarmee, onder andere, verdacht dataverkeer wordt tegengehouden) is bijvoorbeeld van essentieel belang. Er zijn ook andere netwerkapparaten die afdoende moeten zijn beveiligd (denk aan routers). Ook hier geldt weer: zorg er voor dat alle hardware (van

netwerkservers tot firewalls en routers) van de meest recente softwareversie zijn voorzien. Dat geldt uiteraard ook voor de servers waarop de bedrijfswebsite draait. In het ideale geval worden de gegevens ook versleuteld via een beveiligde verbinding, zoals de vaste internetverbinding en WiFi-punten. Zodat ongewenste 'luistervinken' geen kans krijgen.

En: vergeet niet om applicaties en data te back-uppen! Mocht er toch iets misgaan, dan is het cruciaal dat er een (recente) kopie van de programma's en gegevens voorhanden is.

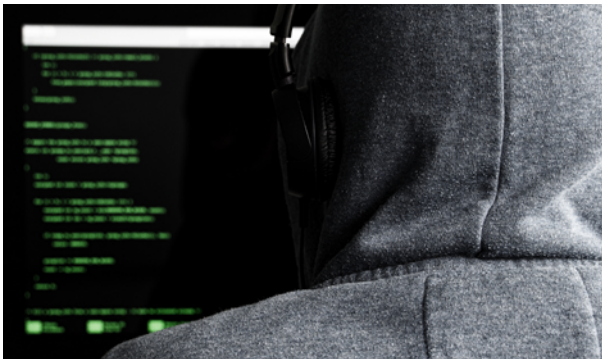
Kennis en testen

Cybercriminelen en hackers zitten niet stil. De cybercriminaliteit is een miljardenindustrie geworden, waarin onderzoek en ontwikkeling een belangrijke rol speelt. Er worden telkens weer nieuwe manieren gevonden om bedrijfsnetwerken binnen te komen, gevoelige informatie te stelen of in gijzeling te nemen. Op de hoogte blijven van de nieuwste criminele snufjes en foefjes en daar weer tegenmaatregelen op bedenken: het is letterlijk een dagtaak voor gespecialiseerde ICT'ers. Die investering in tijd, middelen en geld is helaas wel broodnodig.
Een ander belangrijk, en vaak vergeten, onderdeel is het testen van de beveiliging. De meeste MKB-bedrijven hebben periodieke, onaangekondigde, brandalarmoefeningen. Het is even vervelend voor de medewerkers die direct van hun werkplek weg moeten, maar in tijden van een echte brand zorgt het hopelijk wel voor een grotere overlevingskans.
Hetzelfde geldt voor de e-security. Onaangekondigde simulaties van een cyberaanval, leggen genadeloos de kwetsbare plekken van de bedrijfs-ICT bloot. Anders dan bij een brandalarm-oefening, volstaat het hier niet om een eigen medewerker als 'cyber-BVA' te benoemen. Een dergelijke cyberoefening is het werk van gespecialiseerde ICT-bedrijven waar medewerkers (ook bekend als 'white hat hackers') zich dagelijks buigen over cyberbedreigingen.

Beleid uitstippelen

De e-security is te belangrijk geworden voor organisaties om het alleen een zaak voor de ICT-afdeling te laten zijn. Immers: als de automatisering 'plat gaat' of als er zich datalekken voordoen, dan zijn de consequenties ingrijpend. Voor zowel de reguliere bedrijfsvoering als de financiële positie van het bedrijf. Het is cruciaal dat er goed door de ondernemer en zijn ICT'ers wordt nagedacht over e-security en mogelijke noodprocedures. Dat moet weer leiden tot een e-securitybeleid dat ook binnen het bedrijf wordt verspreid.

Alle technologische maatregelen ten spijt, is de mens vaak nog de zwakste schakel als het gaat om e-security. Onderdeel van een goed e-securitybeleid is interne voorlichting. De medewerkers moeten er van doordrongen zijn dat wachtwoorden en andere inloggegevens niet zomaar mogen worden opgeschreven. Want zelfs met het sterkste slot en de beste alarminstallatie kunnen inbrekers gewoon binnenkomen als de sleutel van het pand en de toegangscode van het alarm onder de deurmat voor de ingang liggen.



Gegevens in gijzeling: Hoe het gierend mis kan gaan

Op een woensdagochtend in juni vorig jaar klikt een nietsvermoedende ambtenaar in Amstelveen op een link naar een website in een ogenschijnlijk bonafide privé mailtje. Op de bewuste website staat een zogenoemde 'ransomware applicatie' die zich direct in de pc van de ambtenaar nestelt. Niet lang daarna zijn alle gegevensbestanden op de werkplek-computer 'gegijzeld' (dusdanig versleuteld dat zij niet meer zijn te openen). De volledige ICT van de gemeente Amstelveen wordt een volle dag stil gelegd om het probleem aan te pakken. Burgers en bedrijven kunnen gedurende die tijd geen gebruik maken van dienstverlening waar ICT voor nodig is (zoals de afgifte van paspoorten en vergunningen). Volgens de gemeente is er geen 'losgeld' betaald aan de cybercriminelen van wie de ransomware afkomstig was.

Los Angeles, de Verenigde Staten. In het Hollywood Presbyterian Medical Center gaat begin februari 2016 na een argeloze klik op een malafide link in een mailtje het volledige ICT-systeem plat. Ook de bestanden van de administratie-afdeling worden in een oogwenk versleuteld en gegijzeld. De cybercriminelen eisen een losgeld van 3,4 miljoen dollar. Uiteindelijk betaalt de ziekenhuisleiding 'slechts' 17.000 dollar voor de code waarmee de versleuteling van de bestanden wordt teruggedraaid.
In de Amerikaanse stad Wichita vindt in het Kansas Heart Hospital een soortgelijk incident plaats. Ook hier klikt een medewerker op een link in een mailtje. Resultaat: de hierdoor binnengekomen ransomware slaagt er in cruciale gegevens te versleutelen. De directie gaat eveneens in op de losgeldeisen van de cybercriminelen en betaalt een onbekend bedrag. Helaas laten de cybercriminelen na ontvangst van het bedrag niets meer van zich horen. Het Kansas Heart Hospital blijft met de gebakken peren achter.
Hoe moet een ondernemer zich wapenen tegen ransomware? Met technologie (goede en up-to-date antivirussoftware, goede periodieke back-ups) én een duidelijk e-security beleidsplan, dat ook door de medewerkers in de praktijk wordt gebracht.

Hoofdstuk 3

Veiliger in de cloud

Het kost ondernemers behoorlijk wat tijd, middelen en geld om de e-security voor hun bedrijf zelf te regelen. Toch is de informatiebeveiliging inmiddels van essentieel belang geworden. Niet alleen voor de dagelijkse bedrijfsvoering, maar ook door de veranderde wetgeving. Het lijkt een stevig dilemma. Maar er is een oplossing: stap over naar de cloud. Daarmee worden de kosten voor e-security flink verminderd.

Tegenwoordig kan een groot aantal applicaties, diensten én communicatie-producten 'uit de cloud' worden afgenomen. Het gaat om bijvoorbeeld kantoorsoftware (Microsoft Office 365), back-up en restore van data en telefonie plus videoconferencing. Ondernemers profiteren zowel van financiële voordelen als van een grotere flexibiliteit door het 'betaal-naar-gebruik'-model dat aan de cloud ten grondslag ligt. Tegelijkertijd zorgt cloud computing er voor dat MKB'ers zelf minder hoeven te investeren in e-security.

E-security experts

De ICT-dienstverleners die cloud-oplossingen aanbieden, is veel gelegen aan een zo optimaal mogelijke beveiliging van hun datacenters. Dat begint al met zaken als fysieke toegangscontroles. Als het gaat om de e-security, zetten de cloud aanbieders een extra tandje bij. Zo hebben zij de nodige experts in dienst, die zich louter bezighouden met e-security: van implementatie tot en met de controle op ongewenste 'bezoekers'. Ook volgen zij de meest recente e-securityontwikkelingen op de voet. Dat laatste is letterlijk een dagtaak: cybercriminelen en hackers komen dagelijks met een ongekend hoog aantal nieuwe bedreigingen op de proppen. De meeste ICT-dienstverleners met een cloud aanbod laten daarnaast zowel hun experts als de e-security van hun datacenters onaangekondigd op de proef stellen door 'white hackers'. Deze onafhankelijke deskundigen weten eventuele kwetsbaarheden genadeloos bloot te leggen. Dit soort gesimuleerde aanvallen zorgen er mede voor dat de e-security op een zo hoog mogelijk niveau blijft.

Beveiliging applicaties en data

Verder investeren cloud aanbieders op grote schaal in de beveiliging en in de talrijke netwerkservers, waarop de applicaties en data van hun klanten zijn te vinden. Ook de applicaties (zoals databases en websites) zelf worden continu 'bewaakt'. Vaak wordt daarbij de data versleuteld opgeslagen, wat weer een extra drempel opwerpt voor ongenode indringers. En, niet onbelangrijk: alle software is bijgewerkt met de nieuwste versies en beveiligingsupdates.

Diverse cloud aanbieders bieden tevens security-software, waarmee bijvoorbeeld mobiele apparaten (zoals smartphones en tablet computers) zijn te beveiligen. Met dergelijke 'Enterprise Mobility software' is bijvoorbeeld te regelen dat bij diefstal van het apparaat bedrijfsgevoelige data op afstand wordt verwijderd.

Een welkome extra is het feit dat de ICT-dienstverlener alle e-security incidenten vastlegt. Mocht er zich onverhoopt toch een datalek voordoen, dan verlangt de toezichthouder (in dit geval de Autoriteit Persoonsgegevens) een 'boekhouding' waarin dat soort informatie is opgenomen.

Firewalls en meer

Cloud aanbieders steken ook veel middelen en geld in de beveiliging van de verbindingen met de buitenwereld. Denk daarbij niet alleen aan beveiligde versleutelde verbindingen, routers en firewalls. Maar ook aan geavanceerde hard- en software, waarmee ongeautoriseerde gebruikers worden gesignaleerd en geblokkeerd ('intrusion detection'). Dergelijke oplossingen zijn veelal door hun prijs (en de benodigde expertise) onbereikbaar voor het Midden- en Kleinbedrijf.

Back-up en restore

Een andere goede reden om de ICT vanuit de cloud af te nemen, is het feit dat de ICT-dienstverleners standaard zorg dragen voor de back-up van applicaties en gegevens. Ook wordt er gecontroleerd of de back-ups goed zijn gelukt. Iets dat bij MKB-bedrijven niet altijd even zorgvuldig gebeurt. Bij veel cloud aanbieders wordt de informatie en software continu op meerdere plekken veiliggesteld. Zodat er altijd weer door kan worden gewerkt. Ook als het op één computerserver even mis dreigt te gaan.

Zelf op orde hebben

Ondernemers die voor cloud computing kiezen, hoeven zich niet meer druk te maken over omvangrijke e-security investeringen in mensen en middelen. Maar overstappen op ICT vanuit de cloud is niet zaligmakend als het gaat om e-security. Een ondernemer zal zelf nog steeds de nodige zaken op orde moeten hebben. Zo moet er bijvoorbeeld op alle werkplekken (mobiel en vast) nog altijd goede anti-virus applicaties zijn geïnstalleerd. Ook ontkomt hij er niet aan om een e-security-beleid uit te stippelen dat bij de medewerkers goed 'tussen de oren zit'. De bekende wachtwoorden die op een Post-It zijn genoteerd, kunnen immers nog steeds alle kostbare technologische e-security snufjes teniet doen.

Hoofdstuk 4

Hoe stel je een e-securitybeleid op?

Een goede voorbereiding is het halve werk. Dat geldt ook voor het opstellen van een e-securitybeleid. Het is een kwestie van een paar essentiële vragen beantwoorden én het gebruiken van het gezonde ondernemersverstand.

Het schrijven van het beleid is een klus voor de ondernemer zelf. Maar hier geven wij alvast de nodige handvatten zodat het e-securitybeleid uitstippelen bijna kinderspel wordt.

Ruwweg zijn er vier onderdelen bij het opstellen van een e-securitybeleid:

Inventariseer

Voordat er maatregelen worden genomen om de e-security afdoende te regelen, is het verstandig om in kaart te brengen wat er eigenlijk moet worden 'bewaakt'. Denk aan: de bedrijfsprocessen, de ICT-systemen waar gebruik van wordt gemaakt (inclusief mobiele hardware) en de bewaarde data (persoonsgegevens, klantinformatie en financiële data).

Kom met veiligheids-richtlijnen

De technische beveiliging kan nog zo goed op orde zijn, maar als medewerkers Post-It velletjes met wachtwoorden laten rondslingeren, dan staat de achter- en voordeur voor cybercriminelen – bij wijze van spreken – alsnog wagenwijd open. De menselijke factor blijft dan ook van cruciaal belang. Stel daarom richtlijnen op met betrekking tot de manier waarop er met wachtwoorden, bestanden en het gebruik van de bedrijfs-ICT en –internettoegang moet worden omgegaan. Idealiter wordt dit een onderdeel van de huisregels van het bedrijf.

Breng structuur aan

Als niemand zich verantwoordelijk voelt of verantwoordelijk wordt gemaakt voor een proces, dan is de kans groot dat het ook te weinig of geen aandacht krijgt. Dat is ook het geval bij e-security. Stel daarom een verantwoordelijke aan voor de e-security van het bedrijf en communiceer dat naar de rest van de onderneming. Die persoon is het primaire aanspreekpunt voor zowel calamiteiten als het cybersecuritybeleid. En overziet de implementatie of de eventuele contacten en contracten met toeleveranciers op dat gebied.

Regel de e-security

Ook niet onbelangrijk: de e-security zelf moet technisch op orde zijn. Doe het of zelf of besteedt het grotendeels uit door bijvoorbeeld over te stappen op ICT vanuit de cloud. Ondernemers die het in eigen hand willen houden, moeten rekening houden met het feit dat het grondige en actuele kennis van de ontwikkelingen op dat gebied vereist. Het loont daarom om de hulp in te roepen van een marktpartij die onder andere op het gebied van e-security zijn sporen heeft verdiend. Stel (al dan niet samen met de ICT-partij) een stappenplan op voor de implementatie van de ICT-beveiliging en vergeet daarbij niet om daarin ook op te nemen dat er continu wordt gekeken of er software updates (veelal uitgebracht omdat er 'beveiligingsgaten' zijn gevonden in de betreffende programma's) moeten worden doorgevoerd. Vaak wordt dat laatste vergeten.
En daar maken cybercriminelen dankbaar gebruik van.

Als laatste, maar zeker niet onbelangrijk: back-ups van data en applicaties vallen ook onder het kopje 'beveiliging'. Regel ook dit goed. Bijvoorbeeld door vast te leggen wanneer er (automatische) back-ups worden gemaakt en waar die fysiek worden opgeslagen. Plan op gezette tijden ook een zogenoemde 'restore-simulatie', waarbij wordt gecheckt of de back-up ook echt goed is verlopen. Mocht er iets misgaan, dan moet er immers binnen zeer korte tijd weer kunnen worden gewerkt met de bedrijfssoftware en -data. Ondernemers die hun applicaties en gegevens uit de cloud halen, hebben daar overigens zelf minder 'last' van: al deze back-up beslommeringen liggen namelijk op het bord van de gespecialiseerde cloud dienstverlener. Een kwestie van delegeren!

Nog makkelijker? Volg dit stappenplan!

De experts van Nederland ICT – de brancheverenigingvan ICT-bedrijven in Nederland – hebben een stappenplan gemaakt voor ondernemers die een e-securitybeleid willen opstellen. Om de Belastingdienst te citeren: "Leuker kunnen wij het niet voor u maken. Wel makkelijker!"

Het e-security stappenplan van Nederland ICT is onderverdeeld in negen hoofdthema's:

Afhankelijkheid

- Breng in kaart wat de belangrijkste bedrijfsprocessen van uw bedrijf zijn en van welke informatie(systemen) deze afhankelijk zijn.

- Maak een overzicht van welke persoonsgegevens uw bedrijf bewaart.

- Breng in kaart welke risico's u loopt en zorg dat u actuele informatie hebt over dreigingen en risico's.

- Laat u informeren over de gevolgen die digitale dreigingen kunnen hebben op de reputatie en continuïteit van uw bedrijf. Bespreek dit eens met een speciaal ICT-beveiligingsbedrijf of met uw cloud aanbieder.

- Zet op een rijtje hoe uw bedrijf afhankelijk is van digitale informatie en wat de gevolgen zijn als er iets fout gaat.

- Zorg dat beveiliging bij nieuwe investeringsbesluiten een van de criteria is voor uw keuze.

- Laat u informeren over de wettelijke eisen die mogelijk voor uw bedrijf of uw sector gelden. Kijk hierbij in ieder geval naar de Wet Bescherming Persoonsgegevens.

Beveiligingsrichtlijnen

- Stel beveiligingsrichtlijnen voor uw bedrijf op. Beschrijf daarin welke informatie beschermd moet worden en hoe de organisatie (ook de medewerkers) met beveiliging om moeten gaan. Hierin beschrijft u ook wie verantwoordelijk is voor de naleving van deze richtlijnen.

- Zorg ervoor dat de richtlijnen over het gebruik van ICT en internet duidelijk zijn. Maak dit ook bekend bij medewerkers. Denk na over wat zij wel en niet mogen. En ook hoe u dat mag controleren als werkgever.

- Zorg ervoor dat medewerkers en leveranciers de richtlijnen kennen. Licht het bijvoorbeeld toe in introductiegesprekken met nieuwe medewerkers en leveranciers. En zet het in de huisregels.

- Stel een procedure op over hoe om te gaan met

(beveiligings)incidenten. Hierin staat bijvoorbeeld bij wie medewerkers incidenten kunnen melden en hoe klanten geïnformeerd worden.

- Bepaal of medewerkers eigen spullen ('devices') mogen meenemen op jouw netwerk. Maak met uw medewerkers afspraken over hoe ze veilig mobiel kunnen werken. Verwerk dit in de beveiligingsrichtlijnen en de huisregels.

- Zorg voor richtlijnen op het gebied van social media en leg het belang uit aan medewerkers. Dat voorkomt dat informatie onbedoeld openbaar wordt.

- Laat iedere medewerker en opdrachtnemer een geheimhoudingsverklaring ondertekenen. En leg dit vast in de beveiligingsrichtlijnen.

Organisatie

- Stel iemand aan binnen de organisatie die verantwoordelijk is voor de beveiligingsrichtlijnen. Dat betekent niet dat diegene ineens voor alle beveiliging verantwoordelijk is. Iedere medewerker is dat namelijk op zijn eigen manier.

- Maak duidelijk wie in de organisatie welke beveiligingstaken en –verantwoordelijkheden heeft en zorg dat iedereen ook weet bij wie ze moeten zijn voor vragen en opmerkingen. Leg dit bijvoorbeeld vast in de interne bedrijfsmap met andere praktische zaken.

- Zorg voor een procedure voor het goedkeuren van (nieuwe) ICT-voorzieningen en zorg dat dit bekend is binnen het bedrijf. Leg het bijvoorbeeld vast bij het personeelsbeleid of in de interne bedrijfsmap met andere praktische zaken.

- Wijs een medewerker aan die de werking van beveiligingsmaatregelen regelmatig controleert en die de directie informeert over de actuele status van de beveiliging.

- Maak altijd afspraken met dienstverleners over beveiliging. Wees kritisch bij de selectie van een ICT-partner en neem beveiliging altijd mee in de afspraken.

Bewustwording

- Bespreek het belang en de regels van informatiebeveiliging regelmatig. Zorg ook dat de beveiligingsrichtlijnen bij iedereen bekend zijn.

- Informeer medewerkers over het omgaan met gebruikersaccount en wachtwoorden en herinner ze regelmatig aan de afspraken.

- Stel regels op en informeer medewerkers over de manier waarop zaken als usb-sticks, smartphones en tablets moeten worden beveiligd. En wat te doen bij verlies of diefstal.

- Stel regels op over de manier waarop met bedrijfsinformatie en persoonsgegevens moet worden omgegaan. En bespreek deze regels binnen het bedrijf.

- Denk eens na over een makkelijk te organiseren interne bewustwordingscampagne. Met het ophangen van posters of door er extra bij stil te staan tijdens een personeelsbijeenkomst.

- Geef een aantal keer per jaar aandacht aan beveiliging, zodat iedereen in het bedrijf zich bewust blijft van hoe hij zelf kan bijdragen aan veilig werken.

- Leg de verantwoordelijkheden van medewerkers in

het kader van informatiebeveiliging vast in het arbeidscontract. Deze gelden ook als er buiten kantoor wordt gewerkt.

- Vraag bij een incident om een evaluatie en neem het voortouw om dit te bespreken met medewerkers. Het doel is om ervan te leren, niet om te straffen.

Toegang en wachtwoorden

- Bedenk wie bij welke gegevens mag komen en doe dit op basis van 'need-to-know'. Leg duidelijk vast wie toegang heeft tot welke delen van het informatiesysteem. Dit kan in de beveiligingsrichtlijnen. Hierdoor houdt u het overzicht.

- Beperk speciale bevoegdheden op computers of het netwerk zoveel mogelijk. Zorg dat alleen door u aangewezen medewerkers extra bevoegdheden hebben, zoals administratorrechten.

- Laat regelmatig controleren of de toegangsrechten die medewerkers hebben, nog corresponderen met hun functie.

- Zorg dat op tijd toegangsrechten worden verwijderd wanneer medewerkers uit dienst gaan of van functie wijzigen. Het is hiervoor belangrijk dat niet iedere medewerker hetzelfde wachtwoord heeft.

- Maak voor elke medewerker een eigen gebruikersaccount aan met eigen wachtwoord.

- Stel medewerkers verplicht om persoonlijke wachtwoorden geheim te houden.

- Verplicht medewerkers periodiek hun wachtwoord te wijzigen (bijvoorbeeld een keer per vier maanden). Een oud wachtwoord mag dan niet worden gebruikt.

- Stel regels op voor de wachtwoorden en dwing deze technisch af.
- Stel computers zo in dat deze automatisch vergrendelen als ze een aantal minuten niet gebruikt zijn. En stel een wachtwoord verplicht voor ontgrendeling.

- Verplicht medewerkers het standaardwachtwoord direct te wijzigen in bijvoorbeeld nieuwe software, computers, smartphones of voicemaildiensten.

- Zorg voor een overzicht welke externe partijen toegang hebben met welk wachtwoord en pas dit aan als de situatie verandert.

Beveiligen data

- Maak een overzicht van het type gegevens dat op uw systemen staat opgeslagen. Neem daarbij ook de data mee die u in programma's gebruikt of online opslaat.

- Zorg dat uw bedrijf alleen die gegevens verzamelt die echt nodig zijn. Maak deze richtlijn bekend bij alle medewerkers.

- Zorg ervoor dat vertrouwelijke of geheime informatie beschermd is met encryptie (versleuteling). Dit geldt ook voor persoonsgegevens van bijvoorbeeld klanten.

- Zorg ervoor dat u ook afspraken hebt gemaakt over welke medewerker de 'sleutelbos' beheert. Als iedereen bij de digitale sleutel kan, heeft een slot geen zin.

- Zorg dat datatransport vertrouwelijk blijft door encryptie toe te passen en informatie te versleutelen. Bespreek dit ook met uw ICT-partner.

- Stel een meldprocedure op in het geval dat gegevens toegankelijk blijken te zijn voor derden of een ander beveiligingsincident is geweest.

- Classificeer uw bedrijfsgegevens en geef aan welk niveau van vertrouwelijkheid nodig is.

- Persoonsgegevens dienen volgens de wet adequaat beschermd te worden. Hier vindt u meer informatie.

Bijzondere persoonsgegevens mag u alleen onder bepaalde voorwaarden hebben en beheren. Aan de beveiliging hiervan worden strenge eisen gesteld.
Stel een procedure op voor het vernietigen of verwijderen van vertrouwelijke gegevens. Gegevens mogen namelijk maar een bepaalde termijn worden bewaard.

Beveiliging ICT

- Installeer een antivirusprogramma op de apparaten die met uw bedrijfsnetwerk verbonden zijn en zorg dat deze software up-to-date is.

- Zorg dat informatie die over uw interne bedrijfsnetwerk gaat, versleuteld is. Zorg daarnaast voor monitoring op de bedrijfsnetwerken. Dit is met speciale software automatisch te regelen.

- Stel encryptie in op het bedrijfsnetwerk (bijvoorbeeld WPA2) en kies een sterk wachtwoord. Als u bezoekers of klanten ook toegang tot het internet wilt geven, leg dan een apart bezoekersnetwerk aan of stel een speciaal bezoekersprofiel in.

- Installeer een firewall en zorg ervoor dat deze altijd up-to-date is. Stel op de firewall ook een zelf gekozen wachtwoord in.

- Loop na welke soort verbindingen u heeft met de buitenwereld en zorg dat deze goed beveiligd zijn. Maak hierbij gebruik van experts om dit te controleren.

- Laat de veiligheid van de website en/of webshop ook eens testen door een gespecialiseerd bureau.

- Leg bij de aankoop van nieuwe ICT vast wat de beveiligingseisen zijn. Zorg dat dit ook in de opdracht aan de leverancier staat.

- Schaf alleen software en hardware aan bij originele leveranciers en hun officiële verkoopkanalen. Zorg dat uw medewerkers weten welke software ze op internet (in de 'cloud') mogen gebruiken. Leg dit ook vast in de beveiligingsrichtlijnen.

- Test de werking van nieuwe software eerst voordat deze voor de hele organisatie beschikbaar komt.

- Stel het direct updaten van software verplicht. Veel inbraken of lekken ontstaan door software die niet geüpdatet is.
Gebruik de lijst die u hebt gemaakt voor uw hard- en software als overzicht. Let ook op upgrades van bijvoorbeeld firewalls, smartphones, tablets.
Als u online software (in de 'cloud') gebruikt, worden updates voor u geïnstalleerd door de cloud aanbieder.

- Zorg ervoor dat uw medewerkers software, documentatie en wachtwoorden op een zorgvuldige plaats bewaren. En zorg dat u hier ook als directie bij kunt.

Breng in kaart welke ICT-voorzieningen er zijn en waar deze staan.

- Test de beveiliging regelmatig en betrek daarbij ook eens een extern bureau.

Back-up

- Zorg voor een procedure voor het updaten van software die bekend is bij medewerkers en systeembeheer. Leg dit vast in de beveiligingsrichtlijnen.

- Stel een procedure op voor het maken van back-ups, onderhoud van soft- en hardware en het beheer en beveiliging van computerruimten. Als u gebruik maakt van een online back-up dienst (in de 'cloud'), dan wordt dit door de cloud aanbieder voor u gedaan.

- Maak regelmatig een (online) back-up van alle belangrijke gegevens. Hoe vaak hangt af van hoe snel de gegevens veranderen. Denk er ook hier aan gevoelige gegevens te versleutelen. Als u gebruik maakt van een online back-up dienst (in de 'cloud'), dan wordt dit door de cloud aanbieder voor u gedaan.

- Bewaar back-ups op een veilige afstand. Als u gebruik maakt van een online back-up dienst (in de 'cloud'), dan wordt dit door de cloud aanbieder voor u gedaan.

- Test iedere back-up of deze goed is uitgevoerd om verrassingen in geval van nood te voorkomen. Als u gebruik maakt van een online back-up dienst (in de 'cloud'), dan wordt dit door de cloud aanbieder voor u gedaan.

Fysieke beveiliging

- Zet de servers in een aparte ruimte en beveilig deze ruimte(s). Een alternatief is om de servers in een goed beveiligd datacenter te zetten. Of om gebruik te maken van ICT vanuit de cloud. In dat geval wordt dat al door de cloud aanbieder voor u gedaan.

- Wijs medewerkers aan die onderhouds- en schoonmaak personeel begeleiden in beveiligde ruimtes in uw pand.

- Tref maatregelen tegen: brand, inbraak, overstroming, stroomuitval en blikseminslag, zodat uw bedrijf ook fysiek goed is beveiligd. Kijk ook welke maatregelen uw verzekeraar hiervoor eist.

- Zet noodprocedures op over wat te doen als informatie niet toegankelijk is. Test welke bedrijfsprocessen kunnen doordraaien op een alternatieve procedure.

Trends ICT Amsterdam
Hessenbergweg 73
1101 CX Amsterdam
T 020 599 599 5
E info@trends.nl

Trends ICT Rotterdam
Hoofdweg 20
3067 GH Rotterdam
T 010 281 22 22
E info@trends.nl

www.trends.nl