Een checklist voor informatiebeveiliging en voorkomen datalekken

Versie maart 2017

Inleiding

Sla een krant of tijdschrift open en de kans is groot dat aandacht wordt besteed aan cyberrisico's of datalekken. Een actieve adviseur zal (zakelijke) relaties dan ook attenderen op deze risico's en de eventuele (financiële) gevolgen daarvan. De adviseur zal proberen met de klant mee te denken over het wegnemen, verminderen en eventueel verzekeren van cyberrisico's. Die markt is volop in ontwikkeling.

Maar hoe zit het met de financiële onderneming zelf? Denkt u dat uitsluitend andere bedrijven deze risico's lopen en bent u er van overtuigd dat u er in uw (digitale) verdediging geen bressen kunnen worden geslagen? Of bent u misschien toch een beetje de schilder bij wiens huis de verf van de kozijnen bladdert?

Veel cyberdreigingen kunt u pareren door binnen uw organisatie het bewustzijn te kweken resp. te vergroten, dat door het goed opzetten van beleid en procedures rondom de beveiliging van data, veel risico's tot behapbare proporties kunnen worden teruggebracht. Wat nog aan dreigingen resteert kunt u voor een groot deel met goed doordachte en proportionele technische maatregelen bestrijden. Het is van het grootste belang dat u deze zaken met uw ICT-leverancier bespreekt.

In deze checklist worden vragen gesteld die tot doel hebben u en uw medewerkers te laten nadenken over (voor het grootste deel niet-technische) procedures binnen uw onderneming die digitale dreigingen al een heel stuk kunnen voorkomen. Praat hier dan ook over met uw medewerkers. Probeer hen te laten inzien dat – wellicht onbewuste – handelingen of gewoontes van mensen de bescherming van informatie in gevaar kunnen brengen. Beschouw de checklist dan ook vooral als een praatstuk, en niet als een limitatieve afvinklijst van technische maatregelen die moeten worden genomen.

Veiligheid van data binnen uw onderneming begint bij bewustheid dat een kleine moeite (gedisciplineerd omgaan met informatie) kan bijdragen aan het behalen van de voor de onderneming gewenste resultaten, nl. het voorkomen van cyberincidenten of datalekken.

Beleid en organisatie van de informatiebeveiliging

Informatiestromen

- Zijn informatiestromen binnen de onderneming (incl. communicatie via website) in kaart gebracht? Is vastgelegd welke informatiestromen essentieel zijn voor het functioneren en voortbestaan van de onderneming? Is in kaart gebracht wat de mogelijke gevolgen voor de onderneming zijn wanneer een essentiële informatiestroom om wat voor reden dan ook uitvalt?
- Is per informatiestroom het gewenste resp. vereiste niveau van bescherming aanwezig?
- Hoe is de monitoring van de informatiestromen over het bedrijfsnetwerk geregeld? Kan bijv. de systeem- of netwerkbeheerder zien wie bepaalde mappen of documenten heeft geopend? Wordt vastgelegd welke medewerkers toegang hebben gehad tot een apparaat of applicatie (logging), inclusief het moment van aan- en uitloggen?

Denk bij informatiestromen aan het ontvangen van persoonlijke informatie van een klant ten behoeve van een voor de klant op te stellen advies, het versturen van offertes voor financiële producten, het versturen van schadeaangifteformulieren, het versturen van premienota's of nota's voor verleende diensten, de export van klantgegevens uit het administratiepakket naar advies- of vergelijkingssoftware, het doormailen van klantinformatie aan banken en verzekeraars, etc.

Ruimte voor aantekeningen

Beleid informatiebeveiliging

- Is het informatiebeveiligingsbeleid beschreven en is deze beschrijving bekend bij alle medewerkers binnen de organisatie?
- Wie is – zowel binnen als buiten de onderneming – verantwoordelijk voor de informatiebeveiliging door bijvoorbeeld risico's te signaleren of zich in andere mate bezig te houden met informatiebeveiliging? Hoe wordt georganiseerd dat de verantwoordelijke(n) altijd over actuele informatie beschikken over dreigingen en risico's op het gebied van informatiebeveiliging?

Het ligt – zeker bij kleine ondernemingen – voor de hand dat de ICT-leverancier een grote verantwoordelijkheid heeft voor het realiseren van een adequate beveiliging van informatiesystemen en –netwerken binnen een financieel advieskantoor. Het mag echter niet zo zijn dat medewerkers niet op de hoogte zijn van de belangrijkste aspecten van het beleid.

Ruimte voor aantekeningen

Toegangsrechten op basis van functies/werkzaamheden medewerkers

- Wordt bij het vastleggen van functiebeschrijvingen van medewerkers rekening gehouden met gescheiden bevoegdheden en rechten?
- Wordt er op toegezien dat de rechten voor fysieke toegang worden gewijzigd zodra de functie van een medewerker verandert?

Aan een takenpakket of functiebeschrijving van een medewerker kunnen toegangsrechten tot mappen, documenten of applicaties worden gekoppeld. Ook binnen applicaties kunnen verschillende rechten worden toegekend. Wees terughoudend in het toekennen van toegangsrechten voor medewerkers die daar op grond van hun functie geen aanspraak op kunnen maken. Geef dus niet alle medewerkers de meest uitgebreide rechten.

Ruimte voor aantekeningen

Bewustheid en kennis medewerkers over oorzaken cyberrisico's

- Is er een 'clean desk' policy om te voorkomen dat informatie toegankelijk is voor onbevoegden?
- Hebben alle medewerkers een geheimhoudingsverklaring getekend, voordat zij hun werkzaamheden binnen uw onderneming aanvangen?
- Zijn alle medewerkers aantoonbaar gewezen op hun verantwoordelijkheden in het kader van informatiebeveiliging? Op welke wijze? Gelden de verplichtingen ook als buiten kantoor wordt gewerkt?
- Zijn er binnen de onderneming interne richtlijnen voor het gebruik van ICT, internet en social media? Maken deze richtlijnen deel uit van de huisregels of personeelsgids? Hoe wordt geborgd dat alle medewerkers de richtlijnen kennen?
- Is het privacybeleid van de onderneming beschreven? Zijn alle medewerkers hiervan op de hoogte?
- Zijn gebruikers bekend met en getraind in beveiligingsprocedures?
- Weten medewerkers wat ze moeten doen wanneer zij constateren dat er mogelijk sprake is (geweest) van een datalek?
- Zijn gebruikers zich bewust van risico's als:
  - Het slordig omgaan met gebruikerswachtwoorden?
  - Het klikken op linkjes of bijlagen bij mails van onbekende afzenders?
  - Het doorgeven van persoonlijke gegevens aan onbekenden die zich – per mail of telefoon – voordoen als leverancier?
  - Het slordig omgaan met vertrouwelijke documenten?
  - Het onbeheerd achterlaten van onbeveiligde PC's?
  - Het zichtbaar transporteren en het onbeheerd achterlaten van (onbeveiligde) laptops?
  - Het zonder toestemming installeren van software op laptop, PC of tablet?
- Is er een procedure hoe moet worden omgegaan met beveiligingsincidenten? Is bij alle medewerkers bekend hoe en waar dit soort incidenten moeten worden gemeld? Worden beveiligingsincidenten door gebruikers ook daadwerkelijk gemeld en zijn daar vervolgacties aan gekoppeld?

Verreweg het zwakste punt in de preventie van cyberincidenten en datalekken binnen een onderneming zijn de kennis en de discipline van medewerkers op dit punt. Zorg dat ze weten welke handelingen en gedrag risicoverhogend zijn met betrekking tot de kans dat er cyberincidenten of datalekken plaatsvinden.

Ruimte voor aantekeningen

Apparatuur binnen netwerken

- Is vastgelegd of medewerkers eigen spullen (‘devices’) mogen of moeten gebruiken voor toegang tot het bedrijfsnetwerk? Is er een BYOD (Bring Your Own Device) beleid? Zijn met de betreffende medewerkers afspraken gemaakt en vastgelegd over veilig mobiel werken via eigen devices?
- Is er een autorisatiebeleid voor het installeren van nieuwe hardware? Wie geeft toestemming voor het installeren van nieuwe hardware? Geschiedt het installeren en verwijderen van hardware(componenten) altijd door een daartoe bevoegde medewerker?
- Is er een autorisatiebeleid voor het installeren van nieuwe software? Wie geeft toestemming voor het installeren van nieuwe software? Geschiedt het installeren en verwijderen van softwareapplicaties altijd door een daartoe bevoegde medewerker?
- Is vastgelegd wie bevoegd is om nieuwe software te installeren op apparatuur en/of het bedrijfsnetwerk? Wordt nieuwe software eerst stand alone getest alvorens deze te installeren op het bedrijfsnetwerk?

Het verkrijgen c.q. verschaffen van toegang tot het bedrijfsnetwerk via hardware die niet goed beveiligd is, of het installeren van software (waaronder ook apps) die mogelijk illegaal of schadelijk is, kan grote gevolgen hebben voor de beveiliging van informatiestromen binnen een onderneming. Stel regels op die strikt worden nageleefd.

Ruimte voor aantekeningen

Continuïteit dienstverlening

- Is er bewust voor gekozen bepaalde aspecten niet te beveiligen en zijn daarvoor continuïteitsmaatregelen getroffen?
- Hoe wordt omgegaan met de risico's van verlies, vernietiging en vervalsing van belangrijke bedrijfsdocumenten?
- Wordt ook rekening gehouden met infrastructurele verstoringen zoals brand, onderbreking van stroom of telecommunicatie, etc.?
- Worden continuïteitsmaatregelen regelmatig getest?
- Is de broncode van de voor de onderneming essentiële software beschikbaar wanneer de leverancier van die software door een calamiteit wordt getroffen? Is er een escrow overeenkomst gesloten?

Stel een plan op waardoor de voor de dienstverlening van de onderneming essentiële informatie altijd toegankelijk is, ook wanneer de onderneming zelf of een leverancier van een cruciale applicatie wordt getroffen door een calamiteit.

Ruimte voor aantekeningen

Beheer / procedures

Gebruik hardware en software binnen onderneming

- Is vastgelegd dat uitsluitend wordt gewerkt met originele hardware en software? Is dit bij alle medewerkers bekend? Zijn er maatregelen om het gebruik van illegale software/ kopieën van software tegen te gaan? Is bij de aanschaf van softwarepakketten voldoende zicht op het aantal gebruikers i.v.m. de licenties?
- Is vastgelegd wat het niveau van beveiliging moet zijn bij de aanschaf van nieuwe ICT (zowel hardware als software)? Wordt dit ook duidelijk in opdrachtbevestigingen richting leveranciers kenbaar gemaakt?
- Zijn er procedures voor correcte en veilige bediening van ICT-apparatuur? Zijn handleidingen beschikbaar?
- Zijn er procedures voor het correct en betrouwbaar gebruik maken van lokaal geïnstalleerde applicaties? Zijn handleidingen voor alle bevoegde medewerkers beschikbaar? Geldt hetzelfde voor online applicaties waarvan de onderneming gebruik maakt?
- Is vastgelegd dat updates of patches van softwarepakketten altijd direct moeten worden geïnstalleerd? Is er een overzicht van apparatuur en devices waarop de betreffende software is geïnstalleerd, zodat duidelijk is welke apparatuur in zulke situaties moet worden geüpdatet?
- Wordt de beveiliging van apparatuur en netwerk periodiek getest?

Het gebruik van originele hard- en software levert aanmerkelijke verlaging op van cyberrisico's. Zorg dan ook dat alle hard- en software adequaat geïnstalleerd is door erkende leveranciers en dat updates of patches zo spoedig mogelijk worden geïnstalleerd.

Ruimte voor aantekeningen

Back-up beleid en procedure

- Van welke gegevens en volgens welk schema worden back-ups gemaakt (data en/of applicaties)? Zijn daar vaste procedures voor? Wordt vastgelegd of een back-up geslaagd is? Is bekend wat te doen wanneer een back-up niet succesvol is verlopen? Hoe en waar worden de gemaakte back-ups bewaard?
- Worden back-ups ook regelmatig teruggezet? Wordt hier een logboek van bijgehouden?
- Zijn er voldoende strenge procedures voor beperking van de toegang van onbevoegden tot back-up media en bestanden?

Een goed doordachte en goed werkende back-up procedure is essentieel voor het voorkomen van ongewenste gevolgen van een cyberincident.

Ruimte voor aantekeningen

Vernietiging en verwijdering hard- en software en data

- Is vastgelegd hoe digitale informatiedragers na gebruik moeten worden vernietigd? Zijn er voldoende strenge procedures voor het veilig vernietigen van geprinte en/of fysieke documenten?
- Zijn er voldoende strenge procedures voor het gebruik van verwijderbare magnetische media, zoals USB-sticks, externe harde schijven, etc.? Is ook vastgelegd wat er moet gebeuren bij verlies van dergelijke devices?
- Zijn er voldoende strenge procedures voor het veilig vernietigen of opschonen van geheugenmedia, wanneer ze niet meer worden gebruikt?
- Is geregeld dat, bij vervanging van hardware, de eventuele harde schijven – na overzetten van de data – worden vernietigd? Vindt controle plaats van definitieve verwijdering van data voordat de hardware daadwerkelijk wordt afgevoerd?
- Is geregeld dat bij overstappen naar een andere software applicatie de in de oude applicatie aanwezige data – na overzetten naar de nieuwe software – worden gewist?

Niet alleen het installeren van hard- en software, maar ook het veilig verwijderen van applicaties, apparatuur en data kan een grote rol spelen bij het voorkomen van cyberincidenten en datalekken.

Ruimte voor aantekeningen

Fysieke beveiliging van ruimtes en van apparatuur

Toegangsbeveiliging bedrijfsruimten

- Is de toegang tot het kantoor voldoende beveiligd? Hoe vindt de controle op de toegang tot het kantoor plaats op het moment dat de toegangsalarmering is uitgeschakeld (dus tijdens openingstijden van het kantoor)?
- Wat is er geregeld voor de toegang van externe dienstverleners die toegang (kunnen) hebben tot de bedrijfsruimten (bijv. interieurverzorgers, onderhoudsmonteurs)?
- Is de toegang tot beveiligingsvoorzieningen, zoals inbraakdetectiesystemen, beperkt tot daartoe bevoegde gebruikers? Wie kunnen het inbraakalarm aan- en uitzetten?
- Is de fysieke toegang tot essentiële ICT-apparatuur (servers, routers, poorten, etc.) voldoende beschermd? Is de serverruimte altijd afgesloten? Is de serverruimte alleen toegankelijk voor bevoegden? Is voor toegang tot de serverruimte toegangsverificatie vereist (bijv. een pasje)?
- Vinden er controles plaats wanneer leveranciers de serverruimte binnenkomen? Wordt alleen bevoegd personeel van de leverancier toegelaten? Worden rechten en middelen voor leveranciers gecontroleerd en zo nodig geblokkeerd of opgeheven wanneer de status van de medewerkers van de leverancier verandert?
- Vinden gesprekken met klanten en leveranciers altijd plaats in afgesloten spreekkamers? Zijn deze spreekkamers opgeruimd? Bevinden zich hierin geen fysieke ordners? Zijn eventuele in spreekkamers aanwezige PC's altijd voorzien van een toegangsbeveiliging?
- Zijn netwerktoegangspoorten die niet in gebruik zijn fysiek uitgeschakeld door middel van netwerkswitches? Zijn er fysieke barrières om toegang tot netwerktoegangspoorten door onbevoegden te voorkomen?
- Wanneer netwerkpoorten niet fysiek zijn uitgeschakeld, zijn er dan procedures voor de controle op onbevoegde toegang tot deze poorten? Is de fysieke toegang tot alle console- en hulppoorten op de routers beveiligd?
- Zijn kabels en/of kabelbehuizingen binnen de onderneming zo aangelegd dat fysieke toegang om transmissies te onderscheppen bemoeilijkt wordt? Is de locatie waar telefoon- en datakabels het gebouw binnenkomen fysiek beveiligd?
- Zijn kabelkasten altijd goed afgesloten? Zijn datacentra en kabelkasten voorzien van extra alarmering tegen inbraak?

Een sluitend systeem van fysieke toegangscontrole tot de bedrijfs- en serverruimte(n) is een belangrijk onderdeel van de beveiliging van data. Te allen tijde moet worden voorkomen dat onbevoegden toegang krijgen tot informatie die – wanneer ze in verkeerde handen terechtkomt – kan leiden tot een cyberincident of datalek.

Ruimte voor aantekeningen

Beheer apparatuur

- Is er een integraal overzicht van alle ICT-apparatuur, inclusief de fysieke locatie van de betreffende apparaten?
- Is elk apparaat voorzien van een barcode of ander middel voor eenvoudige herkenning?
- Is vastgelegd welke apparatuur vanuit de onderneming mag worden meegenomen, en welke toestemming daarvoor nodig is?
- Wordt bij plaatsing van ICT-apparatuur rekening gehouden met omgevingsfactoren zoals zichtbaarheid en bereikbaarheid van buitenaf?
- Vinden er (periodiek) controles plaats of ICT-apparatuur aanwezig is op de beschreven locatie?
- Zijn er fysieke veiligheidsbarrières om ICT-apparatuur te beschermen tegen diefstal of vernieling (bijv. verankering)?

Het beheer van ICT-apparatuur houdt in dat altijd bekend is welke apparatuur in gebruik is, waarvoor de apparatuur wordt gebruikt, en dat de kans dat de apparatuur wordt ontvreemd, zo klein mogelijk wordt gehouden.

Ruimte voor aantekeningen

Onderhoud apparatuur

- Is er klimaatregeling waarmee temperatuur en luchtvochtigheid in de serverruimte constant gehouden wordt?
- Is er klimaatregeling waardoor apparatuur in de serverruimte wordt beschermd tegen rook, stof, chemische dampen etc.?
- Wordt ICT-apparatuur volgens voorschrift van de leverancier onderhouden en worden onderhoudswerkzaamheden door deskundig personeel uitgevoerd?
- Worden technische verstoringen inclusief de genomen acties vastgelegd voor evaluatie en onderzoek achteraf?

Het beheer van ICT-apparatuur houdt tevens in dat de nodige voorzorgsmaatregelen en acties moeten worden genomen om er voor te zorgen dat de apparatuur altijd technisch naar behoren kan functioneren. Ook dit draagt bij aan het voorkomen van het verlies van data.

Ruimte voor aantekeningen

Toegang tot systemen en applicaties

Netwerken en verbindingen

- Is in kaart gebracht welke verbindingen de onderneming heeft met externe systemen en netwerken? Zijn alle verbindingen adequaat beveiligd?
- Zijn er systemen en applicaties die toegankelijk zijn voor derden (zoals bijvoorbeeld leveranciers van ICT-apparatuur i.v.m. onderhoud)? Wat is er geregeld om te voorkomen dat onbevoegden toegang krijgen tot netwerken, computers en applicaties?
- Zijn PC's, terminals en applicaties zodanig ingesteld dat gebruikers opnieuw moeten aanloggen na een periode van inactiviteit?

Voorkomen moet worden dat onbevoegden online toegang krijgen tot externe verbindingen die de onderneming heeft. Denk hierbij aan niet alleen aan het gebruik van online administratie- en adviessoftware, maar ook aan het gebruik van extranetten van verzekeraars, banken en service providers.

Ruimte voor aantekeningen

Toegangsauthenticatie en wachtwoorden

- Worden systemen en applicaties beschermd door middel van toegangscontroles, zoals gebruikersnamen en wachtwoorden? Is vastgelegd dat alle medewerkers eigen gebruikersnamen en wachtwoorden moeten hebben? Is vastgelegd dat medewerkers de verplichting hebben om persoonlijke wachtwoorden geheim te houden?
- Is vastgelegd dat wachtwoorden moeten voldoen aan bepaalde eisen (minimaal aantal tekens, verplichte samenstelling van soorten karakters, etc.)? Is vastgelegd dat wachtwoorden periodiek moeten worden aangepast? Kunnen de aan wachtwoorden gestelde eisen technisch worden afgedwongen? Hoe vinden controles plaats dat wachtwoorden daadwerkelijk periodiek worden aangepast?
- Zijn medewerkers verplicht om standaardwachtwoorden direct na ontvangst van nieuwe software of hardware te wijzigen? Hoe wordt hierop toegezien?

Voor een goede beveiliging van toegang tot interne en externe applicaties en netwerken is het noodzakelijk dat alle medewerkers persoonlijke, sterke en wisselende wachtwoorden gebruiken. Deze uitgangspunten moeten zoveel mogelijk technisch worden afgedwongen.

Ruimte voor aantekeningen

Toegangsrechten en aanloggen

- Wordt de toegang van elke gebruiker tot applicaties op het systeem beperkt tot de applicaties die voor de werkzaamheden van de betreffende gebruiker nodig en geschikt zijn? Is duidelijk vastgelegd wie toegang heeft tot welke delen van het informatiesysteem? Wie geeft toestemming voor het verlenen van toegang tot bepaalde delen van het informatiesysteem? Wordt periodiek gecontroleerd of de rechten die medewerkers hebben, nog overeenstemmen met hun functie?
- Kunnen medewerkers door eenmalig aanloggen op het netwerk (single sign on) alle voor hen beschikbare applicaties gebruiken, of moeten ze voor iedere applicatie opnieuw aanloggen?
- Wordt er zorgvuldig omgegaan met extra bevoegdheden van medewerkers, met name als het gaat om zgn. administrator rechten?

Een goede organisatie, vastlegging en inregeling van toegangsrechten van medewerkers tot directories, bestanden en applicaties is essentieel voor het voorkomen van cyberincidenten en datalekken. Het verlenen van toegang aan medewerkers die hier op grond van hun functie niets in te zoeken hebben, verhoogt juist de risico's hierop.

Ruimte voor aantekeningen

Bescherming van gegevens

Beschermingssoftware, firewalls

- Is er antivirussoftware in gebruik? Zo ja, wordt regelmatig gecontroleerd of deze functioneert en of er patches of updates zijn die moeten worden geïnstalleerd?
- Is voor alle gebruikers duidelijk hoe te handelen in geval van besmetting?
- Zijn er firewalls in gebruik? Zo ja, wordt regelmatig gecontroleerd of deze functioneren en of er patches of updates zijn die moeten worden geïnstalleerd?
- Wie regelt het beheer van antivirussoftware en firewall die op uw systemen zijn geïnstalleerd? Is geregeld dat uitsluitend bevoegden toegang hebben tot beschermings-software en firewalls?

Hackers vinden steeds nieuwe manieren om online toegang te krijgen tot netwerken en systemen. Daarom is het van het grootste belang dat antivirus- en aanverwante beschermingssoftware en firewalls altijd zijn 'bijgewerkt'. Zorg dat op dagbasis wordt gecontroleerd of er updates of patches zijn.

Ruimte voor aantekeningen

Bescherming persoonsgegevens

- Is vastgelegd welke persoonsgegevens door de onderneming worden verwerkt? Is duidelijk wat de Wbp-term 'verwerken' inhoudt? Is per soort persoonsgegeven vastgelegd waarom het noodzakelijk is om deze gegevens vast te leggen?
- Is vastgelegd welke overige gegevens binnen de onderneming worden vastgelegd? Is per soort gegeven vastgelegd waarom het noodzakelijk is om deze gegevens vast te leggen?
- Is vertrouwelijke of geheime informatie beschermd door middel van encryptie (versleuteling)? Is de toegang tot de sleutel voor het raadplegen van versleutelde informatie beperkt tot uitsluitend daartoe bevoegde medewerkers? Wie is beslissingsbevoegd om toegang te verlenen tot die sleutel(s)?
- Zijn er termijnen bepaald voor het bewaren van persoonsgegevens? Worden de persoonsgegevens na verloop van deze termijn(en) adequaat vernietigd of verwijderd?
- Zijn persoonsgegevens minimaal op het niveau van Wbp-eisen beschermd? Geldt dit ook voor de vereiste extra bescherming van zgn. bijzondere persoonsgegevens?

De Wbp eist dat u als onderneming zorgvuldig omgaat met persoonsgegevens en dat u de vereiste maatregelen neemt om deze gegevens te beschermen.

Ruimte voor aantekeningen

Bewerkers

- Doet de organisatie aan outsourcing (bijv. externe salarisverwerking)? Hoe wordt in dergelijke situaties rekening gehouden met de informatiebeveiliging?
- Maakt de onderneming gebruik van cloud diensten? Heeft de cloud leverancier beschreven hoe de in de cloud aanwezige data worden beschermd? Biedt de cloud leverancier de mogelijkheid om, eventueel door derden, controles uit te laten voeren? Levert de cloud leverancier statusrapporten over intern uitgevoerde controles?
- Maakt de onderneming gebruik van online advies-, vergelijkings-, administratie- of planningssoftware? Hoe heeft de aanbieder van die software geregeld dat de persoonsgegevens die u of uw medewerkers hierin vastleggen, voldoende worden beschermd?
- Wanneer uw onderneming gebruik maakt van online back-up faciliteiten, hoe is dan geregeld dat de aanbieder van deze faciliteiten zorgvuldig met persoonsgegevens omgaat?
- Zijn er met eventuele bewerkers van persoonsgegevens harde afspraken gemaakt over het niveau van beveiliging van persoonsgegevens? Is er per bewerker een zgn. bewerkersovereenkomst opgesteld?

Wanneer externe bedrijven toegang hebben tot de binnen uw onderneming verwerkte persoonsgegevens (zgn. bewerkers), moet u er voor zorgen dat die externe bedrijven zich met betrekking tot die persoonsgegevens ook aan de Wbp houden.

Ruimte voor aantekeningen

Wifi netwerken

- Kunnen bezoekers of klanten gebruik maken van wifi faciliteiten binnen uw onderneming? Is hiervoor een apart bezoekersnetwerk aangelegd? Zo nee, is er dan een bezoekersprofiel ingesteld? Is geregeld dat essentiële delen van uw bedrijfsnetwerk niet toegankelijk zijn via deze wifi faciliteiten?
- Maken de mobiele devices binnen uw netwerk automatisch verbinding met openbare wifi hotspots? Wordt bij het gebruik maken van externe wifi netwerken altijd gecontroleerd of het netwerk daadwerkelijk bestaat en of de verbinding beveiligd is? Wordt gebruik gemaakt van encryptie bij de uitwisseling van data via een extern wifi netwerk?
- Zijn documenten met gevoelige informatie beveiligd tegen printen wanneer dat niet noodzakelijk is?

Het is mooi wanneer u uit service-overwegingen een wifi verbinding aan klanten of bezoekers ter beschikking stelt. Maar zorg er wel voor dat er op deze manier niet kan worden ingebroken in uw bedrijfsnetwerk.

Ruimte voor aantekeningen

Vertrek personeel

- Worden bij vertrek van een medewerker direct alle accounts en inlogmogelijkheden met wachtwoorden van de betreffende medewerker op het interne systeem geblokkeerd?
- Wordt nadien binnenkomende e-mail voor de betreffende vertrokken medewerker doorgestuurd naar een ander zakelijk emailadres?
- Worden de e-mailbox(en) waartoe de vertrokken medewerker toegang had, afgesloten? Geldt dit ook voor eventuele webmail-account van de betreffende persoon?
- Zijn eventuele badge(s)/pasje(s) door de vertrokken medewerker ingeleverd en zijn deze direct geblokkeerd?
- Heeft de vertrokken medewerker eventueel hardware van de zaak (mobiele telefoon, tablet, laptop) ingeleverd?
- Is de receptie/portier ingelicht dat de betreffende persoon niet langer bij uw organisatie werkzaam is?
- Is het telefoonnummer van de betreffende persoon doorgeschakeld naar de juiste vervanger?
- Wanneer met een vertrekkende medewerker wordt overeengekomen dat deze de aan hem/haar ter beschikking gestelde zakelijke device(s) in privé mag behouden of overnemen, wordt dan alle zakelijk verkregen informatie/data/software gewist door een bevoegde en ter zake kundige medewerker?
- Controleer tot slot ook de website van uw bedrijf waar vaak ook contactgegevens op staan vermeld. Controleer de gehele site op namen, telefoonnummers en e-mail adressen van personeelsleden die uw organisatie verlaten hebben en verwijder of verander de betreffende gegevens.

Het gebeurt niet zelden dat medewerkers die niet meer werkzaam zijn binnen uw onderneming, nog wel toegang hebben tot netwerken of systemen. Zorg dat hun accounts tijdig worden verwijderd, en dat elke link met uw onderneming wordt doorgehaald.

Ruimte voor aantekeningen

Website

- Kunnen klanten persoonlijke gegevens achterlaten op uw website? Waar komen deze gegevens terecht? Is de beveiliging van deze gegevens adequaat? Bevat uw website formulieren waarop (potentiële) klanten gegevens kunnen invullen? Zijn deze formulieren afdoende beveiligd?
- Kunnen klanten via de website online financiële producten afsluiten? Is de veiligheid van deze faciliteit altijd geborgd? Wordt deze veiligheid periodiek getest?
- Kan via uw website een verbinding worden opgebouwd met een of meer externe partijen, zoals een verzekeraar of een service provider? Is deze verbinding adequaat beveiligd c.q. versleuteld?
- Bevat uw website een voor klanten toegankelijk, afgeschermd gedeelte, waarin zij de door hen afgesloten financiële producten kunnen raadplegen? Is dit afgeschermde gedeelte adequaat beveiligd?
- Kunnen klanten via het afgeschermde gedeelte van uw website bepaalde persoonlijke gegevens wijzigen? Hoe vindt controle en verificatie van deze mutaties plaats? Worden deze mutaties rechtstreeks in de klantendatabase aangebracht, of worden deze eerst in een ‘schaduwbestand’ vastgelegd?

Hoe interactiever uw website is, hoe groter de mogelijkheid is dat kwaadwillenden via uw website pogingen doen om uw bedrijfsnetwerk binnen te dringen. Zorg daarom voor een niveau van beveiliging dat overeenstemt met de functie van uw website binnen uw onderneming.

Ruimte voor aantekeningen