AUXILIUM
adviesgroep

Cybercriminaliteit en de Europese Privacywetgeving

Sinds de komst van smartphones en tablets is het heel normaal dat medewerkers hun eigen apparaten gebruiken binnen een organisatie *(BYOD: bring your own device)*. Deze trend zorgt er voor dat er op steeds grotere schaal - via verschillende apparaten - data worden uitgewisseld. Deze groeiende connectiviteit tussen personen en bedrijven gaat onze maatschappij in de toekomst nog meer beïnvloeden.

ICT ondersteunt alle moderne bedrijfsprocessen en zorgt voor een gezonde infrastructuur. Het werken via internet, handel via webshops en internetbankieren is volledig geïntegreerd in onze huidige maatschappij. De digitale wereld brengt organisaties voordeel in de vorm van een tijdsbesparing in processen en dat leidt tot meer omzet.

Ook de 'criminele wereld' heeft ontdekt dat er in deze virtuele maatschappij geld te verdienen valt. Waar hackers voorheen nog alleen roem wilden behalen, zijn de motieven tegenwoordig gebaseerd op financieel gewin. Methoden van criminele hackers ontwikkelen sneller dan de techniek die hiertegen bescherming biedt. Zwakke plekken in de techniek zorgen ervoor dat hackers eenvoudig persoonsgegevens en andere vertrouwelijke data van een organisatie in kunnen zien. Daarnaast wordt een organisatie kwetsbaar als de processen en afspraken rondom het gebruik van technische middelen en verwerken van data niet duidelijk zijn. Zo is bijvoorbeeld de situatie waarin ontslagen werknemers - die nog beschikken over inloggegevens - bij vertrouwelijke gegevens kunnen, niet wenselijk.

Een vals gevoel van veiligheid

Organisaties zijn vaak van mening dat de beveiliging voldoende is. Er is immers flink geïnvesteerd in technische middelen zoals firewalls, systemen om hackpogingen te voorkomen en virusscanners. Echter, de virtuele risico's worden door ondernemers nog zwaar onderschat en er is veelal geen duidelijk beeld van de gevolgschade. Denk hierbij aan verlies van bedrijfsinformatie of personeelsgegevens, verzuimgegevens, het in verkeerde handen komen van mailcorrespondentie, schade aan het IT netwerk, aansprakelijkheid claims en reputatieschade.

Het is belangrijk het veiligheidsbeleid binnen uw organisatie vast te leggen en maatregelen te nemen om cyber/privacy incidenten te voorkomen. Daarnaast kan de impact van een incident worden verkleind door de juiste procedures te hanteren.

Strengere Privacy wetgeving: De AVG (Algemene Verordening Gegevensverwerking)

Bewustwording van de financiële risico's van een cyberincident is sinds het van kracht worden van nieuwe wettelijke regels nog urgenter geworden. Sinds 1 januari 2016 zijn aanpassingen van de WbP (Wet bescherming persoonsgegevens) van kracht. Een onderdeel van deze aanpassingen is de Meldplicht Datalekken. Organisaties moeten *onverwijld* melding doen als er een inbreuk plaatsvindt op de beveiliging die leidt tot een *aanzienlijke* kans op *ernstige nadelige gevolgen* voor de bescherming van persoonsgegevens. Per 25 mei 2018 worden ook de regels van de AVG (Algemene Verordening Gegevensverwerking), de Europese Privacyverordening, gehandhaafd. Deze verordening vervangt de huidige nationale wetgeving.

De Verwerkersovereenkomst

Het is belangrijk dat de onderneming in kaart brengt hoe binnen de organisatie, maar ook via welke externe bewerkers (ICT bedrijven/hosting/cloud/leveranciers), privacygevoelige informatie kan lekken. De organisatie moet nieuwe afspraken voor het signaleren en informeren van datalekken maken en hiervoor bestaande (service) contracten mogelijk openbreken. Nieuwe wetgeving vereist een dat afspraken duidelijk zijn vastgelegd in een zogenaamde verwerkingsovereenkomst.

Kosten van een incident

Naast kosten van ICT moet de ondernemer bij een incident vooral rekening houden met hoge kosten (juridische/advocaatkosten), kosten van crisismanagement en kosten voor het beperken van imagoschade.

De Meldplicht Datalekken en toekomstige verordeningen luiden een nieuw tijdperk in rond de bewustwording van cyberrisico's. Organisaties zijn tot nu toe geneigd om bij ieder datalek vooral zo weinig mogelijk publiciteit hieraan te geven vanwege een reële reputatie/ imagoschade. Door de meldplicht en de hoge boetes is dit niet meer wenselijk.

Cyber Risico Analyse

Het is de verantwoordelijkheid van iedere organisatie om persoonsgegevens te verwerken in overeenstemming met de bepalingen in de AVG . In deze nieuwe Europese privacywetgeving worden deze verantwoordelijkheden van bestuurders aangescherpt en dient het ook inzichtelijk te worden welke maatregelen er genomen zijn. Stap één is overzicht en inzicht in welke persoonsgegevens de organisatie verwerkt, waar deze zijn opgeslagen en wie er toegang heeft. Stap twee is inzicht in de beveiliging van deze persoonsgegevens. Dit inzicht beperkt zich niet tot de interne processen, maar ook externe partijen die gegevens bewaren en bewerken (Cloud leverancier, ICT provider etc.) moeten hierin meegenomen worden. Voor deze data blijft de verantwoordelijke aansprakelijk in het kader van de AVG.

Multidisciplinair vraagstuk

De Cyber Risico Analyse van CYCO is multidisciplinair: de risico's van zowel Mens (het gedrag van medewerkers), Organisatie (de procedures en contracten) en Techniek (de beveiliging van de data) worden in kaart gebracht via een nulmeting. Meestal wordt het risico van een cyberincident vooral via de technische kant benaderd. Beter is om het cyberrisico te benaderen als een ondernemersvraagstuk: hoe kunnen we dit risico beheersbaar maken voor de onderneming? Wat staat ons te doen bij een cyberincident? Wat zijn de (nieuwe) wettelijke regels op het gebied van diefstal van privacy gevoelige gegevens? Hoe groot is mijn reputatieschade na een publicatie in de krant over een hack van mijn onderneming? Hebben mijn klanten en aandeelhouders nog het vertrouwen dat hun gegevens veilig zijn bij mijn organisatie?

Bewustzijn

In de praktijk blijkt dat technische maatregelen absoluut noodzakelijk zijn, maar dat deze slechts beperkt bescherming bieden tegen cybercriminelen. Technische oplossingen aanbrengen is niet voldoende, vooral niet als er wordt gewerkt met externe apparaten en cloudleveranciers. Beveiligingsmaatregelen zijn zo sterk als de zwakste schakel, dit geldt vooral bij digitale risico's De mens is vaak de zwakste schakel. Het is daarom noodzakelijk voor een organisatie, mede door invoering van de Meldplicht Datalekken, om interne protocollen op te stellen en bewustzijn te creëren bij medewerkers.

En nu?

Helaas is er geen kant-en-klaar pakket dat u kunt aanschaffen waarmee alle risico's afgedekt zijn. Belangrijk is om de risico's in kaart te brengen en bewustzijn te creëren binnen uw organisatie. Laat u daarom adviseren en begeleiden. Het gaat tenslotte om de bescherming van de aan u toevertrouwde persoonsgegevens en daarmee uw betrouwbaarheid als organisatie.

AUXILIUM adviesgroep

| Postadres Postbus 241, 3830 AE Leusden **| Bezoekadres** Philipsstraat 3, 3833 LC Leusden
| Telefoon 033 - 433 72 17 **| Fax** 033 - 433 76 65 **| E-mail** info@auxiliumadviesgroep.nl
| Website www.auxiliumadviesgroep.nl