Modus Operandi van cybercriminelen evolueren snel en wetgeving is aangescherpt

Optimaal risico management onmisbaar bij inschatten van cyberrisico's

Wouter Parent en Robert van der Vossen

De digitale wereld brengt organisaties een groot goed op het gebied van efficiency en slagvaardigheid.
ICT ondersteunt alle moderne bedrijfsprocessen intern en zorgt voor een vitale infrastructuur. De ICT infrastructuur ontwikkelt zich snel. Het werken via internet en de handel via webshops is volledig geïntegreerd in onze moderne maatschappij. Organisaties kennen een hyperconnectiviteit; het nieuwe werken als BYOD (bring your own device) wordt standaard.
Ook de criminele wereld heeft ontdekt dat er in deze virtuele maatschappij veel geld te verdienen valt. Cybercriminelen zijn steeds meer financieel gemotiveerd geraakt en er is duidelijk sprake van een trend van 'hacking for fame' naar 'hacking for fortune' . Methoden van criminele hackers evolueren sneller dan security. Wat kunt u daar tegen doen?

De gevolgen van cybercrime voor de organisatie kunnen erg groot zijn

Een vals gevoel van veiligheid.

"Dat overkomt ons niet" is een veelgehoorde reactie op de vraag of een organisatie voldoende beschermd is tegen cyberaanvallen. Bestuurders en directieleden van organisaties zijn vaak van mening dat de ICT-beveiliging afdoende is. Er is immers flink geïnvesteerd in technische middelen zoals firewalls, intrusion detection, access-management, enzovoorts. Echter, de virtuele risico's worden door ondernemers nog zwaar onderschat en er is veelal geen duidelijk beeld van de gevolgschade.
De gevolgen van cybercrime voor de organisatie kunnen erg groot zijn. Denk maar aan verlies van zeer vertrouwelijke data, personeelsgegevens, verzuimgegevens, het in verkeerde handen komen van cijfergegevens, schade aan het IT netwerk, aansprakelijkheid, claims en reputatieschade.

De virtuele risico's worden door veel bestuurders nog zwaar onderschat

De virtuele risico's worden door veel bestuurders nog zwaar onderschat en er is veelal geen duidelijk beeld van het risico en de gevolgschade.

Meldplicht Datalekken

Een extra dimensie voor de bewustwording van de financiële risico's van een cyberincident is de komst van nieuwe wettelijke regels.
Op 1 januari 2016 zijn de nieuwe aanpassingen van de huidige WbP (Wet bescherming persoonsgegevens) van kracht. Een onderdeel van deze aanpassing is de nieuwe Meldplicht Datalekken. Organisaties (bedrijven en overheden) moeten op straffe van sancties en boetes onverwijld melding doen van datalekken van privacy gevoelige gegevens. Het College bescherming Persoonsgegevens (CBP) wordt een Autoriteit Persoonsgegevens en krijgt net als bijvoorbeeld de Autoriteit Financiële Markten (AFM) een zelfstandige bevoegdheid tot het opleggen van sancties en boetes. Deze boetes kunnen oplopen tot een maximum van € 820.000.

Boetes kunnen oplopen tot een maximum van € 820.000

Wat kost een cyberincident / een datalek?

De eerst logische reactie van de organisatie om het datalek intern te houden is dan dus niet meer mogelijk. Onverwijld, er wordt een termijn genoemd van 72 uur, moet de organisatie gekwantificeerd en gekwalificeerd, de Autoriteit en in sommige gevallen ook de betrokkenen informeren over welke data gelekt zijn en wat de organisatie hiervoor maatregelen treft.

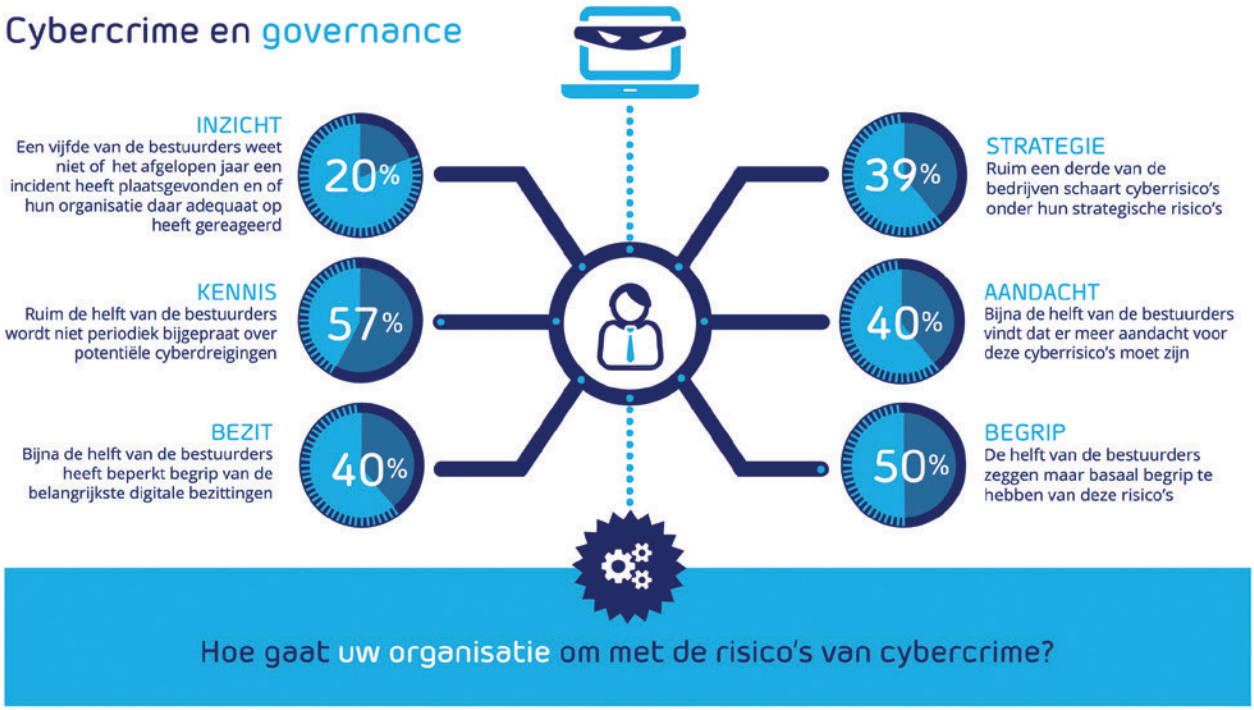
> De Meldplicht en verordeningen zullen een hele nieuwe fase inluiden in de bewustwording van cyberrisico's

Contracten en Privacy Management

Het is dus zaak dat de onderneming in kaart brengt hoe binnen de organisatie privacy gevoelige data kunnen lekken en via welke externe bewerkers (ICT bedrijven / hosting / cloud / leveranciers) dit kan gebeuren. De organisatie zal nieuwe afspraken voor het signaleren en informeren van datalekken moeten maken en bestaande contracten / service level agreements moeten herinrichten. Naast kosten van ICT zal de ondernemer vooral rekening te houden met hoge verweerkosten (juridische / advocaatkosten), kosten van crisismanagement en kosten voor beperken van imago schade.
Deze Meldplicht en verordeningen zullen een hele nieuwe fase inluiden in de bewustwording van cyberrisico's. Organisaties zijn immers tot nu toe geneigd om bij iedere datalek vooral zo weinig mogelijk publiciteit hieraan te geven vanwege een reële reputatie en imagoschade. Door de meldplicht zal aan veel meer incidenten ruchtbaarheid moeten worden gegeven.

> Het is de verantwoordelijkheid van iedere organisatie om persoonsgegevens te verwerken overeenkomstig de bepalingen in de Wet Bescherming Persoonsgegevens

Accountantskantoren hebben hierin een bijzondere positie: zelf zijn zij immers bewerker van de vertrouwelijke data van haar cliënten. Het is verstandig om hierover afspraken op te nemen in de Algemene Voorwaarden. Ook kunnen partijen waarmee wordt samengewerkt mogelijk data inzien. Het verdient aanbeveling om met deze partijen een non-disclosure (geheimhoudingsverklaring) te ondertekenen. Maakt het kantoor gebruik van een clouddienst of een hostingprovider die persoonsgegevens voor de organisatie verwerkt dan bent u verplicht om een bewerkersovereenkomst met deze partij te sluiten. Krijgt u deze overeenkomst niet van uw provider of clouddienst, dan bent u verplicht om deze zelf op te stellen en voor te leggen aan de provider of clouddienst.



Cyber Risico Analyse

Het is de verantwoordelijkheid van iedere organisatie om persoonsgegevens te verwerken overeenkomstig de bepalingen in de Wet Bescherming Persoonsgegevens (WbP). In de nieuwe wet Meldplicht Datalekken wordt de verantwoordelijkheid van bestuurders op dit punt aangescherpt. De tijd van "Trust me" is voorbij. Het worden tijden van "Show me". Dit betekent dat u als verantwoordelijke meer behoefte heeft aan overzicht en inzicht in de adequate beveiliging van persoonsgegevens die een organisatie heeft genomen. Dit inzicht beperkt zich niet tot de interne processen. De bestuurder is ook aansprakelijk voor een datalek bij de bewerkers (de externe ICT leverancier en de hostingpartij).

Wat staat ons te doen bij een cyberincident?

Verantwoordelijken zijn geneigd het risico van een cyberincident vooral via de technische kant te benaderen. Wij adviseren de verantwoordelijke partijen om het cyberrisico te benaderen als een strategisch vraagstuk. Dit kunnen onder meer de volgende vraagstukken zijn; hoe kunnen we dit risico beheersbaar maken voor de onderneming? Wat zijn onze kritische bedrijfsprocessen? 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 stakeholders nog het vertrouwen dat hun gegevens veilig zijn bij mijn organisatie? Wat is onze worst case scenario?

Bewustzijn

Organisaties leggen bij ICT beveiliging vaak sterk de nadruk op de techniek. In de praktijk blijkt dat technische maatregelen noodzakelijk zijn, maar organisaties zich slechts beperkt beschermen tegen cybercriminelen. Technische oplossingen in het netwerk aanbrengen is niet afdoende als de medewerkers van een organisatie onveilig gedrag vertonen.
Beveiligingsmaatregelen tegen cybercrime risico's zijn zo sterk als de zwakste schakel. De mens is vaak de zwakste schakel. Organisaties zullen, mede door invoering van de eerdergenoemde Meldplicht, zelf interne protocollen moeten opstellen om te voldoen aan vergelijkbare kwaliteitseisen.

De auteurs Wouter Parent en Robert van der Vossen zijn beiden werkzaam bij CYCO Cybercrime Cover.