Ctrl+Alt+Delete: alle data op straat

Het beveiligen van informatie en data is een aspect dat over het algemeen weinig aandacht krijgt. Toch kan het grote implicaties hebben voor bedrijven die afhankelijk zijn van deze gegevens alsook voor hun klanten. Er zijn tegenwoordig nog maar weinig bedrijven te bedenken die op dit punt geen risico lopen. Adviseurs dienen dit aspect dan ook altijd mee te nemen in de inventarisatie van mogelijke risico's die klanten lopen.

Wouter Wissink:

'Feit is dat bij veel bedrijven het beveiligen van gegevens onderbelicht is en er nauwelijks beleid wordt gevoerd om gegevens effectief te beveiligen'

De afgelopen jaren zien wij het aantal incidenten op het gebied van falende informatiebeveiliging toenemen. Het blijkt dat veel ondernemers slechts beperkt aandacht schenken aan informatiebeveiliging en daardoor het risico lopen aansprakelijk te worden gesteld voor de gevolgen van diefstal of vernietiging van gegevens.

Eén van de meest bekende en meest omvangrijke incidenten is de TJX-affaire uit de Verenigde Staten. TJX is een retailketen in kleding en huishoudelijke artikelen. Gedurende een aantal jaren werden creditcardgegevens gestolen door online hackers. In totaal werden meer dan 45 miljoen records gestolen. Daarnaast verdwenen, volgens een verklaring van het bedrijf, meer dan 450.000 namen en persoonlijke ID-nummers (in de meeste gevallen het Social Security Number) van de servers. Door gedupeerde klanten is voor vele miljoenen dollars aan schadeclaims ingediend.

Maar ook in Nederland hebben incidenten plaatsgevonden. Een greep uit het nieuws van de afgelopen jaren. In 2006 werd de website van Taxatie 5punt20 gekraakt. De adressen van duizenden klanten werden als lead aan hypotheekverstrekkers te koop aangeboden. In 2009 bleek er een lek te zitten in de website van de Geschillencommissie waardoor documenten van klanten eenvoudig konden worden gedownload. Ook in 2009 werd Hostingbedrijf Intronic door een hacker verrast. Van een aantal klanten is alle data van zowel de primaire- als de back-upserver gewist.

In Nederland komen dit soort incidenten echter niet vaak in het nieuws. Over eventuele claims op dit gebied is daarom niet veel bekend. De reden hiervoor is dat, in tegenstelling tot bijvoorbeeld de Verenigde Staten, diefstal van data (nog) niet hoeft te worden gemeld aan gedupeerden. Er is echter geen twijfel over mogelijk dat ook in Nederland regelmatig diefstal van gegevens plaatsvindt. Vaak hebben bedrijven het niet eens opgemerkt. Immers, een kopie is zo gemaakt. De originele gegevens verdwijnen niet en controle vindt slechts sporadisch plaats.

Politiek

Feit is dat bij veel bedrijven het beveiligen van gegevens onderbelicht is en er nauwelijks beleid wordt gevoerd om gegevens effectief te beveiligen. Vanuit de politiek begint er langzaam bewustwording over dit onderwerp te komen. Officier van Justitie Spreijen, CBP-voorzitter Kohnstamm en D66-leider Pechtold riepen de politiek in november 2008 op een wettelijke meldingsplicht in te voeren bij diefstal van persoonsgegevens analoog aan de wetgeving in de Verenigde Staten. Vooralsnog geldt deze meldingsplicht alleen voor telecombedrijven, maar de verwachting is dat op termijn via de wetgever hierop een uitbreiding gaat komen.

Wetgeving

In de huidige wetgeving worden er overigens wel degelijk eisen gesteld aan de beveiliging van gegevens. Hierbij dient gedacht te worden aan de Wet Bescherming Persoonsgegevens of de eisen die de Inspectie voor de Gezondheidszorg bijvoorbeeld stelt aan de invoering van het burgerservicenummer in de zorg en het elektronisch patiëntendossier (NEN 7510). Andere voorbeelden zijn de Amerikaanse wetgeving met eisen op het gebied van corporate governance zoals Sarbanese-Oxley of de beveiligingseisen van de Payment Card Industrie (PCI standaard).

Beheer uitbesteden

De toename in incidenten en vraag naar striktere wetgeving gaat gelijk op met de ontwikkeling dat steeds meer ondernemingen het beheer van hun informatie en databases uitbesteden. Hiervoor worden service level agreements (SLA) afgesloten met ICT-bedrijven, al dan niet inclusief de verantwoordelijkheid voor de beveiliging van data. Voor deze bedrijven die hun databeheer uitbesteden, is het belangrijk om de verantwoordelijkheid voor de beveiliging van de gegevens zo veel mogelijk contractueel over te dragen aan de ICT-onderneming. De aansprakelijkheid voor de gevolgen van het verlies van data komt dan bij de ICT-onderneming te liggen. Voor deze laatste is het dan wel van essentieel belang om een goede beroepsaansprakelijkheidsverzekering te hebben ter dekking van dit risico en ter bescherming van de continuïteit van de bedrijfsvoering.

Informatiebeveiliging

Het is vanzelfsprekend en van groot belang dat de betreffende ICT-ondernemer op een betrouwbare en veilige manier met gegevens van derden omgaat. Hierbij zijn drie principes van belang, namelijk vertrouwelijkheid, integriteit en beschikbaarheid van gegevens. Dit zijn ook de drie pijlers van de meeste (inter)nationale normen met betrekking tot informatiebeveiliging, waaronder de ISO/IEC 27000-reeks.

De tussenpersoon dient in dit verband een aantal vragen aan zijn klant te stellen. Allereerst moet hij weten of de ondernemer beschikt over 'gevoelige' gegevens van derden. Gevoelige gegevens zijn tot personen herleidbare informatie zoals bankrekening- en creditcardnummers, het burgerservicenummer, medische informatie, maar ook koersgevoelige informatie, marketinginformatie en dergelijke. En indien de ondernemer beschikt over gevoelige gegevens, weet hij dan ook waar deze gegevens worden bewaard of zijn opgeslagen?

Daarnaast moet de onderneming zich ervan bewust zijn wat de impact is als deze gegevens worden gestolen. Verder dient onderzocht te worden of duidelijk (contractueel) is vastgelegd wie de verantwoordelijkheid heeft over deze gegevens en of deze gegevens afdoende beveiligd zijn in overeenstemming met internationale normen, wetgeving en private contracten. Wat gebeurt er met de gegevens als ze niet meer gebruikt worden en waar vindt er opslag van gegevens plaats? Vanzelfsprekend dient dit proces binnen de organisatie regelmatig doorlopen en geborgd te worden. Hiermee kunnen mogelijke aanspraken en financiële schade worden voorkomen.

Verzekeringsoplossingen

Hoewel er gezien de wetgeving en het aantal incidenten wel risico's voor bedrijven verbonden zijn aan het opslaan en gebruik van persoonlijke informatie is het aantal verzekeringsoplossingen echter relatief beperkt.

Aanspraken voor verlies van persoonlijke gegevens vallen niet standaard onder de dekking van een aansprakelijkheidsverzekering voor bedrijven, omdat het hierbij niet om letsel- of zaakschade gaat. Medeverzekering als een aparte rubriek voor vermogensschade kan een mogelijke oplossing bieden.

Daarnaast bestaat voor ICT-bedrijven die zich specifiek met het beheer van informatie en data bezighouden, de mogelijkheid om een beroepsaansprakelijkheidsverzekering te sluiten. Ook bestaan er nog beperkte mogelijkheden voor het verzekeren van de financiële gevolgen van het verlies van persoonlijke informatie veroorzaakt door hackers onder een zogenaamde Cyberpolis. Deze laatste verzekering wordt in de markt echter slechts door een beperkt aantal aanbieders aangeboden. Het credo voor dit soort risico's is dan ook: Voorkomen is beter dan genezen!

Door: ing. Wouter Wissink, Loss Control Manager, Chubb Insurance Company of Europe SE