Pas op: **lekkagegevaar**

Hoe veilig zijn klantgegevens bij accountants? Als toonbeeld van vertrouwelijkheid bewaren ze hun databestanden achter slot en grendel. Maar dat is niet veilig genoeg. ‘Steeds weer zijn er incidenten die aanleiding zijn voor aanpassingen. Een kwestie van voortschrijdend inzicht.’

HENK VLAMING

Vorig jaar werd de auto van een accountant van Ernst & Young gekraakt. De buit bestond uit een laptop. Daarop stonden financiële gegevens van het beursgenoteerde bedrijf Rood Testhouse. Die zou de jaarcijfers binnen een paar weken rapporteren. Maar na de diefstal lag de informatie letterlijk op straat. In overleg met Euronext besloot Rood Testhouse de jaarcijfers dus maar eerder te publiceren. De koers van de aandelen zakte met tien procent. “Waarschijnlijk was de laptop gestolen door een junk”, zei bestuursvoorzitter Philip Nijenhuis. “Maar we hebben het zekere maar voor het onzekere genomen.”

Zestigduizend laptops

Een incident, zo lijkt het. Maar verlies van informatie is al veel meer dan dat. Accountantskantoren zijn vaker geplaagd door diefstal van gevoelige informatie. Zo ging het bij Ernst & Young vaker mis met laptops die in verkeerde handen vielen. Eén keer verdwenen daarbij gegevens van IBM-medewerkers, een andere keer waren creditcardgegevens van honderdduizenden mensen weg. In 2000 vervroegde KLM de presentatie van de jaarcijfers nadat cijfers hierover waren gestolen van KPMG. Toen waren het nog documenten. Al deze gevallen haalden de krant. Diefstal van informatie is eerder een trend dan een incident. Vorig jaar werden alleen al in Nederland zestigduizend laptops gestolen, 165 per dag. Met de data die daarop stonden, kunnen enorme archieven tot de nok worden gevuld. Het zijn niet alleen junks die toeslaan. Al in de jaren tachtig waren er publicaties over handel in voorkennis van een paar jongens die ’s nachts rondslingerende papieren stalen uit advocatenkantoren.

Kinderlijk eenvoudig

De beveiliging van elektronisch opgeslagen informatie is derhalve een topprioriteit, ook van accountantskantoren. Daarbij gaat het niet alleen om bescherming tegen dieven, maar ook tegen eigen slordigheden. Een paar jaar geleden lekte een reorganisatieplan van een groot bedrijf uit. Het lek was ontstaan bij het retourneren van de doorgerekende plannen door de accountant. Het dossier was per e-mail verstuurd, maar belandde in een verkeerd postvakje. “Volkomen onverantwoord”, zegt directeur Frank Jonker van bureau Creaim, dat zich vooral ten behoeve van accountants, fiscalisten en consultants toelegt op informatiebeveiliging. “Accountants gaan in hun elektronische communicatie nog te vaak lichtvaardig om met de vertrouwelijkheid van informatie. Een basisregel is dat je gevoelige gegevens nooit verstuurt per e-mail. Berichten die via e-mail worden verstuurd zijn kinderlijk eenvoudig te kraken.”

Armand Veltmeijer (KPMG):
‘Als er geen aanleiding is om bepaalde kennis te weten, hoeven mensen die ook niet te bezitten.’

Zesde plaats

Het probleem van de beveiliging van informatie is sterk toegenomen sinds gegevens digitaal worden opgeslagen en bewerkt. Hele bestanden passen op een handcomputer. Met een enkele druk op de knop flitsen documenten in seconden de wereld rond. Handig, maar ook gevaarlijk. E-mails worden gekraakt, systemen gehackt en spyware infiltreert in pc’s om daar

FOTO: CORBIS

Veiligheidsrisico's

- **Huisvesting**. Het gaat hierbij om de veiligheid van kantoren, dossiers en bestanden. Onbevoegden mogen niet zo maar toegang kunnen krijgen tot ruimten waarin gevoelige informatie bereikbaar is.
- **Opslag**. Laptops, usb-sticks, pda's en andere mobiele informatiedragers zijn afraders als opslag van klantgegevens. Ze zijn over het algemeen te kwetsbaar.
- **Internet**. Via websites en het gewone e-mailverkeer kunnen virussen of spyware binnenkomen. Spyware is software die informatie verzamelt en doorgeeft aan de afzender. Virussen kunnen databestanden aantasten.
- **Hackers**. Via internet proberen hackers voortdurend toegang te krijgen tot alle systemen die ze maar kunnen kraken. Niet altijd met intenties om schade aan te richten of informatie te ontvreemden, maar de risico's zijn er.
- **Autorisatie**. Ook binnen het accountantskantoor is niet iedereen bevoegd voor toegang tot klantgegevens. Onbevoegde toegang tot informatie kan ook per ongeluk leiden tot verkeerd gebruik van gegevens.
- **Bewerking**. Ook al is het maar een kat die op een onbewaakt moment over een toetsenbord loopt, het risico dat digitale informatie een ongewenste bewerking ondergaat is aanwezig op het moment dat gegevens zijn opgevraagd.
- **Transport**. Gewoon e-mailverkeer of gewone verzending per post zijn taboe. Alleen beveiligde communicatie en aangetekende postverzending zijn acceptabel.

Guno Pocorni (Jefferson Wells):
'Beveiliging is vooral ontmoedigingsbeleid. Je probeert de drempel zo hoog mogelijk op te werpen.'

naar informatie te speuren. Onderzoek van Symantec laat zien dat de accountancy de zesde plaats inneemt op een ranglijst van aangevallen sectoren. Over omvang van de schade die voortvloeit uit dataverlies is nauwelijks iets bekend. Wel berekende bureau Gartner dat particulieren in Amerika vorig jaar voor vijftien miljard dollar waren gedupeerd als gevolg van datadiefstal, vooral creditcardfraude.

FOTO: SIMONE VAN ES

Guno Pocorni (Jefferson Wells): 'In de interfaces, de koppeling tussen verschillende IT-systemen, zitten veel risico's, omdat systemen daar toegankelijk zijn.'

Vluchtig medium

Genoeg redenen voor accountantskantoren om de spreekwoordelijke deuren dubbel te vergrendelen. "Bedreigingen van accountantskantoren zijn legio en kunnen uit elke hoek komen", zegt voorzitter Hans Donkers van NOREA, de beroepsorganisatie van IT-auditors. "Niet alleen de georganiseerde misdaad en bedrijfsspionage vormen een risico. Ook personeel kan informatie verspreiden door slordig om te gaan met gegevens. Daardoor kan informatie terechtkomen bij onbevoegden die er onbedoeld misbruik van maken."
Waar moeten we dan aan denken? Aan handelingen die elke accountant dagelijks verricht, zegt Jonker van Creaim. "Fouten in verzending via berichten per e-mail komen veel voor. E-mail is een heel vluchtig medium. Je klikt met de muis en weg is het bericht, je kunt het niet meer terughalen. Daarnaast komt het vaak voor dat je digitale post verstuurt zonder dat die aankomt. Waar het blijft, weet je niet."

Voorbeeldfunctie

Uiteraard hebben accountantskantoren niet stilgezeten. De meeste hebben inmiddels een veiligheidsbeleid opgetuigd. "Vanuit de NOREA zien we dat informatiebeveiliging hoog op de agenda staat van accountantskantoren", zegt Donkers. "We zien dat een aantal kantoren al veel maatregelen heeft getroffen. Een generiek beleid dat voor alle kantoren zou gelden, is er niet. Het is altijd maatwerk. Je kunt denken aan technische maatregelen, zoals encryptie van verstuurde bestanden en beveiligde USB-sticks. Maar veel van die maatregelen steunen op procedures en die vragen voortdurende aandacht van de betrokken mensen."
Beveiliging is voor accountants niet alleen belangrijk vanuit het oogpunt van bedrijfsvoering, maar heeft ook te maken met de aard van het vak. Integriteit en vertrouwelijkheid zijn zo'n beetje het handelsmerk van de accountant.
"Ze hebben een voorbeeldfunctie", zegt engagementmanager Guno Pocorni van Jefferson Wells. Pocorni licht regelmatig organisaties door op veiligheid, waarbij hij vooral kijkt naar de inrichting van systemen en modellen. "Accountants bezitten heel veel vertrouwelijke informatie van klanten, die moeten ze wel goed beschermen. Maar het ontbreekt aan wettelijke voorschriften en richtlijnen voor deze doelgroep over hoe om te gaan met veiligheid. Elk kantoor moet daarom veiligheidsmaatregelen treffen op basis van een eigen veiligheidsbeleid."

Frank Jonker (Creaim): 'Volgens onderzoek neemt accountancy de zesde plaats in op een ranglijst van aangevallen sectoren.'

Eenvoudige maatregelen

Accountants moeten ook wel. De beroepsregels schrijven voor dat informatie van cliënten geheim gehouden moet worden. Daarnaast is de Wet op de bescherming persoonsgegevens van toepassing. Maar die vertelt organisaties niet hoe ze hun systemen en dossiers moeten beveiligen. Een veiligheidsbeleid gaat over het ontwikkelen van procedures en protocollen en het toezien op de naleving daarvan. Dat gaat van het classificeren van informatie naar risicoprofiel, tot het beveiligen van IT-systemen. Dat klinkt ingewikkeld, maar veel maatregelen zijn eenvoudig van aard.
Geen laptops mee naar de klant met gevoelige informatie erop bijvoorbeeld. Beperkte autorisatie voor toegang tot centrale bestanden.
"Maar denk ook eens aan de bezoekersregeling", zegt Pocorni. "Wordt een bezoeker het pand doorgeleid en weer terug naar de uitgang? Of wordt een bezoeker slechts tot de lift begeleid?"

Versleutelen

Beveiliging van informatie wordt al iets ingewikkelder als de bestanden bewerkt of getransporteerd moeten worden. Dat vraagt om

Veiligheidsmentaliteit

Hoe is het gesteld met het veiligheidsbesef? Die zit nog niet helemaal tussen de oren, zo blijkt uit onderzoek dat vooral in Amerika plaatsvindt. Dat gaat niet specifiek over accountantskantoren maar over het bedrijfsleven in het algemeen, waaronder ook financiële en zakelijke dienstverleners. Uit een dit jaar gepubliceerd onderzoek van PricewaterhouseCoopers in vijftig landen naar de veiligheid van informatie, kwam naar voren dat slechts een derde van de ondervraagde bedrijven er een gedegen strategie op na houdt voor wat betreft de veiligheid van informatie. Bijna tachtig procent heeft geen speciale verantwoordelijken die expliciet zorgen voor veiligheid van informatie. In de helft van de gevallen is er geen rampenplan voor als er iets ernstig mis gaat met bedrijfsgeheimen. Minder dan een derde informeert leveranciers en andere partners over veiligheidsmaatregelen die genomen worden. Minder dan de helft van de bedrijven versleutelt informatie zodat die voor buitenstaanders ontoegankelijk is. Beter omkijken naar de eigen informatie is er evenmin bij. Zestig procent van de bedrijven voert nooit een inventarisatie naar klantenbestanden uit aldus onderzoek van het Amerikaanse Ponemon-instituut. Bijna de helft van de ondervraagde bedrijven voert nooit een check uit op belangrijke gegevens.

Veiligheidsgaranties

Accountantskantoren kunnen desgewenst de norm BS 7799 (British Standard - een internationaal keurmerk) toepassen, die specifiek over informatiebeveiliging gaat. Hiervan bestaat inmiddels ook een ISO-normering: ISO 17799. De standaard bestaat uit twee delen. Het eerste splitst het vakgebied informatiebeveiliging op in *best practices*. Die zijn beschreven in tien hoofdstukken, 36 doelstellingen, 127 *controls* en meer dan 1.400 aanbevolen beveiligingsmaatregelen. In deel twee wordt de managementcyclus in de vorm van een procesplan beschreven (*plan-do-check*).

FOTO: MARJA BROUWER

Hans Donkers (NOREA):
'Een generiek beleid dat voor alle kantoren zou gelden, is er niet. Het is altijd maatwerk.'

veilige procedures, die echter ook niet zo moeilijk zijn om in te voeren. "De eerste basisregel is dat je nooit vertrouwelijke gegevens met de gewone e-mail mag versturen", doceert Jonkers. "Je mag daarvoor ook niet de gewone post gebruiken. Je moet het aangetekend versturen. Dan kan het ook nog zoek raken, maar het afgelegde parcours is altijd te traceren."
Veilig gebruik van technologie is verder ook een voorwaarde. "Stel eisen aan de interfaces", zegt Pocorni. Een interface is de koppeling tussen verschillende IT-systemen. "Daar zitten veel risico's, omdat systemen daar toegankelijk zijn. Afhankelijk van de gevoeligheid van de informatie, stel je eisen aan de beveiliging van de interfaces. Je moet weten hoe groot het risico is dat iemand iets op een lijn zet. Versleutel gevoelige informatie, zodat die niet leesbaar is. Daarnaast geldt dat je zo veel mogelijk gebruik moet maken van geanonimiseerde databestanden, zodat de informatie niet te herleiden is naar organisaties."

Afgesloten ruimte

Dit soort lessen is inmiddels doorgedrongen tot accountantskantoren. "Wij hebben interne richtlijnen voor de beveiliging van onze informatie", zegt Arnold Wisselink van Accountanskantoor K. den Haring in Dordrecht. "Jaarcijfers moeten altijd langs accountants. Bestanden zijn uitsluitend toegankelijk via wachtwoorden. Informatie zetten we wel op laptops, maar de richtlijn is dat die er niet langer dan een dag opstaat. We zorgen voor een dubbele backup van alle gegevens, zodat we ze nog hebben als er iets mis mocht gaan. De server staat in een afgesloten ruimte die alleen voor de directeur toegankelijk is. Zo zijn we constant bezig de veiligheid te aan te passen en te vernieuwen."

Digitale bunker

Betekent dit dat accountantskantoren hun informatie met wat logische aanpassingen afdoende hebben beveiligd? Was het maar waar. Volledige veiligheid vereist een dermate zware beveiliging dat een kantoor bijna op een digitale bunker lijkt. Zeker de grote kantoren waar veel informatie is en veel mensen rondlopen. "Voor het gebruik van laptops hebben onze accountants strikte richtlijnen voor wat wel en niet mag", vertelt Amand Veltmeijer, die als IT-security officer van KPMG verantwoordelijk is voor de beveiliging van informatie daar. "Zo moeten alle laptops een disk-encryptie hebben, waardoor de harde schijven afdoende beveiligd zijn. De toevallige dief kan er onmogelijk bij komen. Honderd procent zeker weet je dat nooit, maar

Hans Donkers (NOREA):
'Je kunt adequaat beveiligen. Maar de laatste procenten vragen vaak een enorme extra investering.'

Veilig Internet Diagnose-Instrument

Voor kleinere accountantskantoren en andere kleine intermediairs heeft het NIVRA in samenwerking met de branchevereniging Nederlandse Internet Providers (NLIP) een Veilig Internet Diagnose-Instrument ontwikkeld. Dit instrument dient als hulpmiddel om snel de beveiligingsrisico's in kaart te kunnen brengen en ontbrekende maatregelen te kunnen identificeren. De praktijkhandreiking biedt een praktische tweestappenaanpak. In het eerste deel worden de veiligheidsrisico's beschreven waaruit de specifieke beveiligingsbehoefte van een bedrijf blijkt. Ook worden enkele beveiligingsmaatregelen voorgesteld. Het tweede deel bevat een checklist en een diagnose-instrument die de bestaande beveiligingssituatie schetst.

Arnold Wisselink (Accountantskantoor K. den Haring): 'Informatie zetten we wel op laptops, maar de richtlijn is dat die er niet langer dan een dag opstaat.'

we houden goed bij wat de mogelijkheden zijn op dit gebied. We passen deze beveiligingen voortdurend aan. Alleen door ons goedgekeurde usb-sticks mogen worden gebruikt door de accountants. Antivirusprogramma's, firewalls en anti-spyware hebben wij zowel op de werkplek als op de servers. Het aantal beheerders dat toegang heeft tot servers en centrale bestanden houden we zo klein mogelijk. Als er geen aanleiding is om bepaalde kennis te weten, hoeven mensen die ook niet te bezitten. Verder hebben we onze beheersprocessen geregeld. Voor elke nieuwe softwareapplicatie is de juiste goedkeuring vereist voordat deze in bedrijf genomen kunnen worden. Die onderwerpen we aan allerlei checklists om er zeker van te zijn dat alles er in moeten zitten dat nodig is om veilig te werken."

Incident gedreven

Maar zelfs de meest extreme maatregelen kunnen diefstal of misbruik niet volledig uitsluiten. "Accountantskantoren moeten er mee leven en vooral heel alert blijven", zegt Pocorni. "Alles is te kraken. Beveiliging is vooral ontmoedigingsbeleid. Je probeert de drempel zo hoog mogelijk op te werpen."
Dat is ook de mening van Hans Donkers van NOREA. "Je kunt adequaat beveiligen. Maar de laatste procenten vragen vaak een enorme extra investering, want die hebben betrekking op personele handelingen en perfectie van technische beveiligingsoplossingen. Hoever accountantskantoren hierin kunnen en willen gaan, hangt mede af van hun volwassenheid. Helemaal veilig zal het accountantskantoor niet worden. Altijd zullen er weer incidenten plaatsvinden die noodzaken tot aanvullende maatregelen. Net als bij alle organisaties is er ook bij de accountantskantoren in dit verband sprake van incidentgedreven voortschrijdende beveiliging." ■