

## Artikel Vertrouwelijke gegevens lopen gewoon de voordeur uit

Security.nl Door H. van der Heijden op donderdag 13 december 2007 12:30

Investerings in virusscanners, firewalls en antispam-software vormen een groot deel van het it-budget. Ondanks deze maatregelen is het lekken van gegevens nog altijd een veelvoorkomend probleem. Een probleem dat vaak onderschat wordt, omdat men vertrouwt op de technologie, terwijl de meeste gegevens verloren gaan door menselijke acties. Soms met opzet, maar vaak ook onbedoeld of zelfs onbewust. Hoe komt het dat datalekkage zo wordt onderschat, en welke acties moet men nemen om het de lekkage te verhelpen?

'Data leakage' wordt gedefinieerd als het verplaatsen van informatie naar ongeautoriseerde partijen. Het is een van de strategische bedreigingen voor elk bedrijf. Datalekkage kan directe gevolgen hebben voor een organisatie op financieel gebied of op de bedrijfsvoering en kan ernstige juridische problemen opleveren.

Het probleem van datalekkage wordt door veel bedrijven onderschat. Er zijn zelfs velen die het verschijnsel niet eens kennen. Dat is niet erg verrassend als je nagaat dat veel gegevensverlies onbewust gebeurt. Uiteraard zijn er kwaadwillenden die van buitenaf gegevens stelen, maar denk ook aan de veelgenoemde voorbeelden van weggegooide pc's met data of verloren usb-sticks. Er zijn dus drie bronnen van datalekkage: medewerkers die gegevens per ongeluk lekken, medewerkers die bewust gevoelige informatie naar buiten brengen en externe partijen die informatie stelen.

### Gevolgen niet duidelijk

Men denkt dat het probleem niet veel voorkomt. Ook worden de gevolgen van datalekkage lang niet altijd overzien.

Een van de redenen voor deze onderschatting is dat sommige gegevens moeilijk op waarde zijn te schatten. Wat heeft iemand aan een eenvoudig personeelsbestand, met daarin naam, adres, sofinummer en bankrekeningnummer? Op het eerste gezicht niet veel, totdat je beseft dat hiermee creditcard-accounts zijn aan te maken, verzekeringen zijn af te sluiten, inzicht in financiële situaties is te krijgen, etcetera. Geen direct gevaar voor de onderneming, zo lijkt het, maar wat als de werknemer het bedrijf aanklaagt wegens slordige administratie. Hij of zij maakt goede kans de zaak te winnen. En bedenk eens hoe hoog de publicitaire schade kan oplopen. Wie wil er nog werken bij een bedrijf dat zijn meest eenvoudige zaakjes niet op orde heeft?

### Huidige oplossingen vaak verouderd

Gegevensverlies treedt vooral op door de enorme hoeveelheid data. Traditionele oplossingen om datalekkage te voorkomen werken met contentfiltering. Hierbij worden uitgaande mails gescand op een aantal vooraf gedefinieerde kernwoorden. De verschillende data is tegenwoordig echter zo verspreid dat het nalopen van ervan lastig is en nauwelijks nog effect heeft. Bovendien vraagt het veel tijd om alle informatie van het juiste 'gevoeligheidslabel' te voorzien.

#### **Is er binnen mijn bedrijf voldoende aandacht voor datalekkage?**

*Veel bedrijven hebben geen tot weinig besef wat de gevaren zijn van datalekkage. Dit is meestal te wijten aan een gebrek aan kennis; men weet niet dat het probleem bestaat of het is niet bekend hoe men ermee om moet gaan. Om na te gaan of binnen een bedrijf voldoende aandacht is voor het probleem van datalekkage kunnen de volgende vragen als eenvoudige leidraad dienen.*

- *Waar binnen het bedrijf en waar op het netwerk is gevoelige informatie opgeslagen?*
- *Welke medewerkers zijn geautoriseerd om deze informatie te ontvangen en door te sturen?*
- *Welke mensen buiten de organisatie zijn geautoriseerd deze informatie te ontvangen?*

*Als er geen duidelijk antwoord is te formuleren op één van de vragen, is de beveiliging van gegevens nog niet voldoende.*

Gegevens, en dan met name de gevoelige, moeten geïdentificeerd kunnen worden op basis van hun locatie in het netwerk. Er is inmiddels een aantal toepassingen dat hierin goed presteert. Er wordt dan een waardeoordeel aan de gegevens gekoppeld, dat aangeeft in hoeverre die informatie verplaatst mag worden. Er zijn echter nog weinig bedrijven die effectief gebruikmaken van deze oplossingen.

In de praktijk zijn met betrekking tot datalekkage vier verschillende soorten organisaties te onderscheiden. Ten eerste het bedrijf dat helemaal niets tegen lekkage doet. Vervolgens zijn er bedrijven die hun data fysiek beveiligen, door bijvoorbeeld draagbare opslagmedia niet toe te staan. Weer een stap hoger staan de organisaties die een infrastructurele oplossing hebben ingevoerd, zoals e-mail filtering of het monitoren van het netwerk. En als laatste zijn er de bedrijven die systemen hebben geïmplementeerd die gevoelige informatie identificeren en blokkeren.

### **Combinatie van techniek en bewustwording**

Gevoelige gegevens op straat verminderen het concurrerende vermogen, maar kunnen ook directe financiële schade opleveren. Het probleem is alleen dat de meeste bedrijven de bedreigingen van buitenaf in de gaten houden, terwijl een groot gedeelte van het gevaar van binnenuit de organisatie komt.

Externe gevaren worden met behulp van technologische oplossingen geprobeerd tegen te houden. Dit lukt gelukkig ook steeds beter. Beveiliging staat hoog op de agenda en er komt steeds meer budget vrij om de meest uitgebreide technologische hoogstandjes aan te schaffen. Techniek alleen is echter niet voldoende. En alleen naar buiten kijken is niet voldoende.

Het is hoog tijd voor een nieuwe aanpak. Niet alleen op technologisch gebied, maar vooral ook qua organisatie. Management én werknemers moeten bewust worden van de gevaren en bijvoorbeeld eerst drie keer nadenken, voordat de usb-stick met klantgegevens in de tas wordt gegooid.

### **Aanpak in stappen**

Een aantal stappen is vereist om datalekkage tegen te gaan. Als eerste moet duidelijk worden wat precies gevoelige informatie is. Hoewel er overeenkomsten zijn, zoals de eerder genoemde personeelsbestanden, moet elk bedrijf voor zichzelf zijn vertrouwelijke gegevens identificeren.

Vervolgens moet helder worden gemaakt welke bedrijfseenheden met gevoelige informatie omgaan. Een strengere scheiding maken in gebruikersgroepen is van belang om het gevaar van lekkage te verkleinen. Hoewel veel werknemers het zullen ontkennen, zijn er slechts weinig mensen die alle informatie nodig hebben om goed te kunnen functioneren. De taakomschrijving van een functie moet worden uitgebreid met een bepaald toegangsniveau tot informatie. Dit moet gebeuren op afdelingsniveau. Hiervoor moet dus niet alleen bedrijfsbreed, maar ook per specifieke afdeling geïdentificeerd worden welke informatie aanwezig is, en wat daarvan een vertrouwelijk karakter heeft.

Daarna moet er concreet worden gekeken naar mogelijke lekken door de gangbare procedures na te lopen. Juist in de dagelijkse activiteiten kunnen slordigheden opduiken die een potentieel gevaar opleveren.

Wanneer dit alles in kaart is gebracht, kun je pas verschillende technologische oplossingen met elkaar vergelijken. Een passende toepassing vraagt uiteraard ook een nauwkeurige implementatie die de juiste werking verzekert.

Wanneer de identificatie van informatie en de invoering van technologische bescherming is afgerond, moet ervoor worden gezorgd dat dit binnen het bedrijf navolging vindt. Door bedrijfsprocessen vast te leggen die regels opleggen voor het gebruik van informatie, wordt iedere werknemer actief betrokken bij het tegengaan van datalekkage. Op die manier komt stap voor stap vast te liggen hoe een financiële rapportage wordt gemaakt, of een marketingplan wordt opgesteld. De beveiliging van de betreffende gegevens speelt dan uiteraard een belangrijke rol, of is zelfs het uitgangspunt.

De laatste stap is het concreet trainen van medewerkers. Hierbij volgen het topmanagement en geselecteerde werknemers workshops over hoe men om moet gaan met gevoelige informatie. Deze trainingen tonen dan ook direct hoe de nieuwe bedrijfsprocessen hun weerslag hebben op de dagelijkse gang van zaken.

### **Investeren in veiligheid**

Het hierboven beschreven proces is niet eenvoudig of snel door te voeren. Er wordt al jaren gesproken over informatiebeveiliging, maar de cijfers over dataverlies geven aan dat de combinatie van oplossingen nog in de kinderschoenen staat. Naast technische toepassingen die steeds meer voor handen zijn, is een groeiende bewustwording van groot belang. Er moet worden beseft dat bepaalde data van onschatbare waarde is. En medewerkers moeten inzien hoe ze met dit soort gegevens om moeten gaan.

Wanneer bewustwording van datalekkage een feit is en we handelen zoals veiligheidsprocessen aangeven, kunnen we ons volledig richten op de bedrijfsvoering en het product of de dienst waarmee we geld verdienen. Dit vraagt investering in geld, maar vooral in tijd. Het tegengaan van datalekkage van binnenuit eist een gedragsverandering en dat gebeurt nu eenmaal niet van de ene op de andere dag. Tot die tijd moeten we dus niet alleen de gevaren van buitenaf blijven controleren, maar ook onszelf en onze eigen collega's aansporen na te denken hoe om te gaan met bedrijfsinformatie.

Door Henk van der Heijden, managing director Comsec Consultancy.

*UBM Global is het met deze zienswijze eens, en heeft daarvoor de volgende DriveLock edities:*

- *DriveLock Basic. Poort- en randapparaatcontrole en autorisatie plus netwerkprofielen.*
- *DriveLock Encryption. Versleutelen van informatie op verwijderbare drives.*
- *DriveLock Security Reporting Center. Verzamelen en rapporteren van DriveLock events.*
- *DriveLock Application Filter. Applicatiecontrole en -autorisatie.*
- *DriveLock Terminal Services. DriveLock functionaliteiten voor Terminal Server sessies.*

*UBM Global: organisaties met medewerkers die nog geen encryptie discipline en mentaliteit hebben, kunnen worden geholpen met DriveLock software voor beveiliging van CD's, USB-sticks en overige externe drives die – optioneel als standaard door de organisatie te configureren - geen wachtwoord, code of biometrie*

*gebruiken om informatie te beveiligen, maar alleen op bepaalde computers of bij bepaalde medewerkers functioneren.*

*DriveLock Encryptie versleutelt – na eerst de gebruiker te waarschuwen - niet-encrypte CD's, USB-sticks automatisch. DriveLock herkent de gebruiker, waardoor de gebruiker geen wachtwoord hoeft te verzinnen en te onthouden. Bovendien kan een teamgenoot, die in dezelfde gebruikersgroep zit, ook deze CD en USB-stick gebruiken. De onderlinge uitwisselbaarheid is erg handig bij een (tijdelijke) taakgroep die werkt aan een vertrouwelijke zaak of voor dezelfde patiënt of cliënt. Deze onderlinge uitwisselbaarheid is mogelijk bij alle soorten verwijderbare drives.*

#### *Alternatief*

*DriveLock Encryptie versleutelt – na eerst de gebruiker de mogelijkheid op vrijwillige basis aan te bieden – CD's, USB-sticks en alle overige externe drives.*