Data Leakage Prevention

De uitdaging om bedrijfsgevoelige informatie binnen uw organisatie te houden

Ir. A.H.P. van Vliet
is junior adviseur bij KPMG IT Advisory. Zijn werkzaamheden zijn gericht op het gebied van informatiebeveiliging. Hij is in die hoedanigheid betrokken bij een breed scala van securitygerelateerde audit- en adviesopdrachten.

vanvliet.arjan@kpmg.nl

Ir. Arjan van Vliet

De hoeveelheid digitale informatie binnen bedrijven, die ook in toenemende mate gevoelige informatie bevat, neemt dagelijks toe. Aangezien het lekken van gevoelige informatie, een data leakage incident, een grote impact kan hebben op zowel het bedrijf als de getroffen personen, is het belangrijk de juiste preventieve en recessieve maatregelen te nemen. Het nemen van maatregelen wordt meer en meer vanuit wet- en regelgeving afgedwongen. Om een data leakage incident te voorkomen is het belangrijk organisatorische maatregelen te nemen zoals het opstellen en implementeren van een informatiebeveiligingsbeleid en het classificeren van informatie. Naast het uitvoeren van de organisatorische maatregelen kan een Data Leakage Prevention (DLP)-softwarepakket helpen het risico van lekken te verkleinen.

Inleiding

De steeds grotere hoeveelheden digitaal opgeslagen (gevoelige) informatie in combinatie met een transparantere manier van werken binnen organisaties brengt een verhoogd risico tot lekken van deze informatie met zich mee. Het is immers steeds gemakkelijker om allerlei informatie te raadplegen en moderne communicatiemiddelen maken ook het uitwisselen steeds eenvoudiger. De gevolgen van data leakage kunnen enorm zijn. Stel, de gevolgen voor zowel het bedrijf als de getroffen personen eens voor wanneer creditkaartgegevens op straat komen te liggen. Het lekken van informatie gaat gepaard met flinke imagoschade en er kunnen aanzienlijke financiële gevolgen mee gemoeid zijn. Onderzoek heeft uitgewezen dat niet alleen het aantal incidenten toeneemt, maar dat ook de financiële gevolgen steeds groter worden. Het is dan ook niet verrassend dat ander onderzoek uitwijst dat databescherming één van de belangrijkste drijfveren is voor informatiebeveiliging.

In dit artikel wordt eerst een overzicht gegeven van de risico's en gevolgen die gepaard gaan met het lekken van gevoelige informatie. Er zal onderscheid worden gemaakt tussen de oorzaken van het lekken en de gevolgen daarvan. Het belang om maatregelen te treffen zal worden geïllustreerd met gegevens uit relevant onderzoek en met praktijkvoorbeelden. In toenemende mate worden maatregelen ook afgedwongen vanuit wet- en regelgeving, en daarvan zal een kort overzicht worden gegeven. Daarna wordt ingegaan op de werking en het nut van Data Leakage Prevention (DLP)-softwarepakketten.

Risico's, gevolgen en oorzaken

De meeste data leakage incidenten worden pas opgemerkt wanneer negatieve gevolgen optreden. Dit is precies de reden waarom het onmogelijk is de exacte omvang van het aantal data leakage incidenten te bepalen. Uit recentelijk door KPMG uitgevoerd onderzoek ([Mars09]) bleek dat alleen al in de laatste drie maanden van 2008 de persoonlijke gegevens van 47,8 miljoen mensen op straat waren komen te liggen in een totaal van 404 waargenomen incidenten.

Bij de term data leakage wordt vaak ten onrechte alleen aan hackers gedacht die (digitaal) inbreken om zo toegang tot gevoelige informatie te verkrijgen. Een minstens even belangrijke oorzaak van data leakage zijn de eigen medewerkers en zakenpartners. Bij het lekken van gevoelige informatie kunnen we onderscheid maken tussen de volgende vormen:

- *Onbewust lekken.* Lekken als gevolg van een fout, bijvoorbeeld met e-mail waarbij de verkeerde bijlage of de verkeerde ontvanger wordt geselecteerd.
- *Bewust lekken.* Werknemers die de regels kennen maar deze toch overtreden zonder dat ze uit zijn op persoonlijk gewin, bijvoorbeeld door gevoelige informatie naar een privéaccount te mailen met het oog op thuis werken.
- *Kwaadaardig lekken.* Zowel een medewerker als een extern persoon kan hieraan ten grondslag liggen. Met voorbedachten rade informatie langs de beveiliging smokkelen met als doel persoonlijk gewin.

De meeste data leakage incidenten worden pas opgemerkt wanneer er negatieve gevolgen optreden

Het is niet altijd duidelijk wat allemaal als gevoelige informatie beschouwd kan worden. Erg breed uitgezet kan hierbij gedacht worden aan alle informatie die door een andere partij misbruikt kan worden voor persoonlijk of bedrijfsmatig gewin of waardoor het betreffende bedrijf er nadeel van kan ondervinden. In tabel 1 wordt onderscheid gemaakt tussen een aantal verschillende vormen van gevoelige informatie ([Herm09]).

De gevolgen van een data leakage incident hangen af van het type data dat gelekt is, maar kan onderverdeeld worden tussen de gevolgen voor personen en de gevolgen voor bedrijven. Bij het lekken van persoonsgegevens kunnen de betreffende personen slachtoffer worden van identiteitsdiefstal. Bij identiteitsdiefstal is men uit op persoonlijk gewin door zich voor te doen als iemand anders. Het slachtoffer kan dan geassocieerd worden met acties welke hij of zij nooit heeft uitgevoerd. Voor bedrijven is het scala aan mogelijke gevolgen veel groter:

- verlies van uitstraling en reputatieschade;
- verlies van concurrentievoordeel;
- vertrouwensverlies bij huidige en toekomstige klanten;
- verlies in marktwaarde door verminderd aandeelhoudersvertrouwen;
- boetes van privacyregulerende instanties;
- compensatiekosten voor slachtoffers.

Informatietype	Beschrijving
Persoonlijk Identificeerbare Informatie (PII)	Alle informatie gerelateerd aan personen zoals NAW-gegevens en burgerservicenummers.
Medische/Patiëntgegevens	Alle informatie met betrekking tot de gezondheid van personen zoals medicijngebruik en medische dossiers.
Creditcard- of betaalpasgegevens	Creditcardnummers met eigenaar, vervaldatum en autorisatiecode, rekeningoverzichten en banksaldo's.
Inloggegevens	Data waarmee ingelogd kan worden als een andere persoon.
Financiële bedrijfsgegevens	Alle data gerelateerd aan financiën zoals gegevens over aandelenemissies, betaalverplichtingen / achterstanden en uitgekeerde of ontvangen sponsorbedragen.
Intellectueel eigendom	Binnen bedrijven ontwikkelde kennis over zaken als broncode, technische ontwerpen, productsamenstellingen en marketingstrategieën.

Tabel 1. **Verschillende vormen van gevoelige informatie.**

Buiten de directe gevolgen zijn er indirecte gevolgen. Door de opgelopen imagoschade hebben mensen minder vertrouwen in het bedrijf en zal het moeilijker zijn om nieuwe klanten te binden, hetgeen gepaard gaat met hogere marketingkosten. Het Ponemon Institute heeft in Amerika onderzoek gedaan naar de kosten per incident en kwam uit op een gemiddelde van $ 202 per gelekt record, waarvan $ 152 betrekking had op indirecte kosten ([Pone09b]).

Vanwege de wetgeving binnen de Verenigde Staten die het verplicht stelt om alle gevallen van data leakage waarmee persoonsgebonden informatie is gemoeid te melden, is het eenvoudig met voorbeelden uit Amerika te komen. Toch heeft ook een aantal incidenten in Nederland het nieuws weten te halen ([Spai08]).

Uit de voorbeelden in tabel 2 valt op dat veel incidenten te maken hebben met persoonsgegevens of dat personen last van het lekken hebben ondervonden. Tevens valt het op dat enorme

Datum	Beschrijving	Type lek
14-01-2008	Door een typefout heeft één van de systeembeheerders van Planet Internet per ongeluk een back-up van alle klantgegevens (2,5 miljoen) op de webruimte van een klant geplaatst. Het bestand bevatte gebruikersnamen, aliassen, IP-adressen, versleutelde wachtwoorden, afgenomen diensten van alle particuliere en zakelijke klanten. Nadat de gebruiker het incident bij Planet had gemeld, werd er geen actie ondernomen totdat het nieuws zich begon te verspreiden.	Typefout, onbewust lekken
22-09-2008	Door een configuratiefout ontving een lid van een politieke partij (SP) e-mail van iemand vanuit een andere partij (CDA) binnen de Provinciale Staten in Limburg. De ontvanger dacht dat een persoon binnen de CDA deze e-mails lekte vanwege de soms heftige inhoud. Na twee maanden is het CDA ingelicht over het incident.	Configuratie-fout, onbewust lekken
26-10-2008	Een militaire ambtenaar had een USB-stick verloren en werd vervolgens afgeperst door twee Hagenaren die dreigden het incident aan de pers te melden. Uiteindelijk heeft de militaire ambtenaar het incident gemeld bij de militaire politie, die de afpersers heeft gearresteerd.	Verloren USB-stick, onbewust lekken
23-03-2009	Op de website van OV-fiets, dat fietslokkers verhuurt op NS-stations, konden naam, adres, bankrekeningnummer, kaartnummer en deblokkeercode van 50.000 klanten worden achterhaald. Om persoonlijke informatie te achterhalen was alleen een persoonlijk nummer nodig. Door achtereenvolgende nummers in te voeren waren de gegevens van andere klanten te achterhalen.	Programmeer-fout, onbewust lekken
06-04-2009	De website van de geschillencommissie die geschillen tussen personen en bedrijven behandelt is gedurende één jaar slecht beveiligd geweest. Mensen met een zaaknummer en inloggegevens konden door het zaaknummer in de adresbalk te wijzigen toegang krijgen tot alle andere zaken teruggaand tot 2005. Onder de documenten bevonden zich gedetailleerde jaarafrekeningen, correspondentie van advocaten en rechtsbijstandsbureaus, facturen en bankafschriften.	Programmeer-fout, onbewust lekken

Tabel 2. **Enkele voorbeelden van onbewuste data leakage incidenten binnen Nederland.**

hoeveelheden gevoelige data onbewust worden gelekt en dat veel zaken aan het licht komen door goed oplettende burgers. In veel gevallen is het echter niet meer te achterhalen of er eerder al meer gegevens zijn gelekt.

Impact van de huidige economische crisis

Door het huidige economische klimaat waarbij meer mensen op straat komen te staan is de verwachting dat het aantal data leakage incidenten alleen maar verder zal toenemen. Onderzoek heeft uitgewezen dat ongeveer 59 procent van de vertrekkende werknemers bedrijfsdata steelt ([Ponec09a]). Uit hetzelfde in de Verenigde Staten uitgevoerde onderzoek is gebleken dat slechts vijftien procent van de bedrijven een controle uitvoert op meegenomen papieren en elektronische documenten. De e-mailgeschiedenis en hardcopybestanden zijn het meest populair. Tevens wordt het risico tot lekken vergroot door bezuiniging op IT-kosten en IT-personeel ([OEDL09]).

Wetgeving en regulering

Ook wet- en regelgeving proberen meer grip te krijgen op het alsmaar groeiende probleem van data leakage. Het meest volwassen is de wet- en regelgeving in de Verenigde Staten. De belangrijkste regelgeving is gericht op incidenten waar persoonsgegevens mee gemoeid zijn of op bedrijven die werken met financiële of medische gegevens.

Ongeveer 59% van de vertrekkende werknemers steelt bedrijfsdata

Hieronder is de belangrijkste wet- en regelgeving inclusief reguleringen vanuit de industrie zelf opgesomd.

- *Health Information Portability and Accountability Act (HIPAA).* Wetgeving voor alle bedrijven die met medische gegevens te maken hebben, en die ook eisen aan de beveiliging van Protected Health Information (PHI) beschrijft.
- *Gramm Leach Bliley Act (GLBA).* Wetgeving voor alle financiële organisaties inclusief bedrijven die financiële informatie ontvangen.
- *Data Breach Notification Laws.* Wetgeving die het melden van data leakage incidenten waar persoonsgegevens mee gemoeid zijn, verplicht stelt. Momenteel van toepassing in 38 Amerikaanse staten.

Een DLP-softwarepakket kan aanzienlijke meerwaarde bieden op het gebied van kostenbesparing en het voldoen aan wet- en regelgeving

- *Payment Card Industry Data Security Standard (PCI DSS).* Wetgeving voor alle bedrijven die met creditcardgegevens werken of deze verwerken.

Op het gebied van de integriteit speelt ook de Sarbanes Oxley (SOx)-wetgeving, die deugdelijk bestuur van beursgenoteerde ondernemingen vereist, een rol. De SOx-wetgeving vereist onder andere een verantwoordelijke voor alle beschikbare informatie.

In Nederland is momenteel alleen de Wet bescherming persoonsgegevens (Wbp) ingevoerd, die omschrijft hoe organisaties moeten omgaan met persoonsgegevens en welke rechten de burgers hebben. Deze wet voorziet echter niet in het verplicht melden na het lekken van persoonsgegevens.

Onlangs is in de Europese Unie een voorstel gedaan om het melden van data leakage incidenten te verplichten. Dit voorstel, bekend onder de naam 'the ePrivacy Directive', is echter alleen van toepassing op elektronische communicatiediensten in publieke netwerken. Om deze reden heeft de Europese databeschermingstoezichthouder (EDPS) in een reactie laten weten de voorstellen niet ver genoeg te vinden gaan.

Hoe voorkom ik een data leakage incident?

Om het risico van het optreden van een data leakage incident te verkleinen dienen in eerste instantie organisatorische aanpassingen te worden gemaakt. De eerste stappen zijn het inventariseren welke data beschermd moeten worden, te bepalen hoe strikt het beleid moet worden en het beleggen van verantwoordelijkheden. Tevens is het van belang het beleid naar werknemers uit te dragen en werknemers te trainen om zo het informatiebeveiligingsbewustzijn te verhogen.

Naast het nemen van de juiste organisatorische maatregelen kunnen technische maatregelen zoals het aanschaffen en implementeren van een DLP-softwarepakket helpen bij het verkleinen van het risico tot het lekken van informatie.

De werking van een DLP-softwarepakket

Om het lekken van gevoelige informatie tegen te gaan richten DLP-softwarepakketten zich op data in drie verschillende stadia:

- *Data 'in motion'.* Alle data die zich over het netwerk verplaatsen, die 'in beweging zijn' zoals webverkeer, e-mail en Instant Messaging (IM)-berichten. De focus ligt hierbij op data die het bedrijfsnetwerk verlaten.
- *Data 'at rest'.* Alle data binnen het bedrijfsnetwerk die zijn opgeslagen op eindpunten, zoals op laptops, servers en databases.
- *Data 'in use'.* Alle data die in gebruik zijn, zoals het bewerken van een document of het kopiëren van een bestand naar een USB-stick.

De geanalyseerde data kunnen grofweg in twee categorieën worden ingedeeld. In het ideale geval betreft het 'structured data', data in een vooraf bekend formaat, zoals geboortedatum, creditkaartnummers en burgerservicenummers. Deze informatie kan met eenvoudige patroonherkenningstechnieken worden gedetecteerd. De meeste data zijn echter ongestructureerd, 'unstructured data', en zorgen voor een grotere uitdaging. Voor een stuk tekst in bijvoorbeeld een e-mail worden geavanceerdere technieken gebruikt, zoals conceptuele en taalanalyses, om de strekking van de tekst te achterhalen.

De meerwaarde van een DLP-softwarepakket

Er kunnen verschillende motieven ten grondslag liggen aan het besluit een DLP-softwarepakket aan te schaffen. De meest voor de hand liggende is het verlagen van het risico tot het openbaren van gevoelige informatie, maar ook op het gebied van kostenbesparing en het voldoen aan wet- en regelgeving kan een DLP-softwarepakket aanzienlijke meerwaarde leveren. Tevens kan het helpen bij meer zijdelingse aspecten zoals het 'opvoeden' van werknemers in het gebruik van en de omgang met (gevoelige) informatie. De belangrijkste gebieden waarop een DLP-softwarepakket meerwaarde aan een organisatie kan leveren zijn:

- *Compliancy met wet- en regelgeving.* De meeste DLP-softwarepakketten bieden standaard de mogelijkheid templates (een set regels) te activeren die in lijn zijn met verschillende vanuit wet- en regelgeving gestelde eisen. Tevens kunnen er rapporten worden gegenereerd om de compliancy met de betreffende wet- of regelgeving aan te tonen.
- *Verhogen van het beveiligingsbewustzijn (trainen van medewerkers).* Wanneer medewerkers het beveiligingsbeleid overtreden of dreigen te overtreden wordt de actie geblokkeerd en krijgt de medewerker hier melding van met uitleg van reden. Ook is het mogelijk een keuzemelding te genereren; medewerkers krijgen dan een waarschuwing waarna ze de betreffende actie kunnen annuleren of een keuze kunnen maken voor een

Producent	Kenmerken
Fidelis Security Systems	Fidelis Security Systems biedt een sterke netwerkanalyse, maar beschikt niet over een 'end point agent'.
McAfee	Een bekende speler op het gebied van informatiebeveiliging. McAfee heeft de markt betreden door de overname van Reconnex.
RSA (Tablus)	Een bekende speler op het gebied van databescherming. RSA heeft de markt betreden door overname van Tablus. Opvallende eigenschap is de aanwezigheid van 'content discovery agents'.
Symantec (Vontu)	Symantec is een bekende speler uit de computerbeveiligingsmarkt en heeft de DLP-markt betreden door de overname van Vontu, waardoor zij is uitgegroeid tot één van de grootste spelers.
Trend Micro (LeakProof)	LeakProof heeft een sterke 'end point agent', maar heeft minder sterke netwerkanalysemogelijkheden.
Vericept	Vericept focust zich alleen op DLP en biedt een volledige DLP-oplossing.
Websense	Websense richt zich op webfiltering en webbeveiliging en biedt een complete DLP-oplossing.

Tabel 3. **Overzicht van enkele DLP-softwarepakketproducenten.**

vervolgactie zoals het versleutelen van het e-mailbericht of de bijlage. Op deze manier wordt het beveiligingsbeleid afgedwongen, leren werknemers van hun fouten en wordt beveiligingsbewustzijn onder werknemers verhoogd.

- *Kostenbesparing.* Door de centrale managementinterface waar alle informatie wordt verzameld, is het veel gemakkelijker om het beleid af te dwingen en eventuele incidenten te analyseren. Tevens wordt het eenvoudiger om compliancy met wet- en regelgeving aan te tonen doordat compliancyrapporten eenvoudig gegenereerd kunnen worden.

DLP-softwarepakketten kunnen aanzienlijke meerwaarde bieden voor de informatiebeveiliging, maar kunnen niet alle incidenten voorkomen. Dergelijke softwarepakketten richten zich over het algemeen niet op aanvallen van hackers en bieden alleen bescherming tegen lekken van elektronische informatie.

Het implementeren van een DLP-softwarepakket

Het implementeren van een DLP-softwarepakket kan alleen succesvol worden wanneer eerst de noodzakelijke organisatorische aanpassingen worden doorgevoerd en wanneer realistische doelstellingen aan het DLP-product worden gesteld.

Op organisatorisch gebied dient begonnen te worden met het opstellen van een breed informatiebeveiligingsbeleid om dat vervolgens binnen de organisatie door te voeren. Bij het doorvoeren van het informatiebeveiligingsbeleid is het belangrijk de werknemers op de hoogte te brengen van het beleid, en nut en noodzaak om bewust met (gevoelige) informatie om te gaan kenbaar te maken. Binnen het informatiebeveiligingsbeleid dient te worden nagedacht over de waarde van verschillende typen informatie voor het bedrijf. Aan de hand van deze analyse kan dataclassificatie worden uitgevoerd en kunnen verschillende classificatieniveaus en overeenkomstige beveiligingsniveaus worden gedefinieerd. Per classificatie en beveiligingsniveau dienen autorisaties te worden gedefinieerd en autorisatietabellen te worden opgesteld. Belangrijk aspect hierbij is om niet alleen generieke autorisaties op te stellen; zo zullen de autorisaties op het bekijken en versturen (e-mailen) van contracten van werknemers binnen de afdeling Personeelszaken anders zijn dan op andere afdelingen. Na het in kaart brengen van het volledige informatiebeveiligingsbeleid en het definiëren van alle autorisaties kan worden begonnen met de implementatiefase.

Gedurende de implementatiefase van het DLP-product is de eerste stap het product te configureren aan de hand van het gedefinieerde beleid en de opgestelde autorisaties. Nadat het product enige tijd heeft gedraaid moet de werking worden geëvalueerd en waar nodig de configuratie worden bijgesteld. Dit proces wordt herhaald totdat het DLP-product naar wens werkt. Tevens is belangrijk ook bij de implementatiefase de medewerkers die mogelijk met meldingen van het DLP-product geconfronteerd worden, hiervan op de hoogte te stellen.

Conclusie

De alsmaar groeiende hoeveelheid digitale informatie binnen bedrijven en tegelijkertijd de toename van (moderne) digitale communicatiemedia stelt bedrijven voor een grote uitdaging gevoelige informatie binnen hun grenzen te houden. Het nemen van maatregelen wordt enerzijds afgedwongen door de afschrikkende werking van de enorme (financiële) gevolgen die data leakage incidenten met zich mee kunnen brengen en anderzijds door toenemende wet- en regelgeving op het gebied van data retention en privacy.

Het huidige economische klimaat heeft de noodzaak tot het nemen van effectieve maatregelen alleen maar vergroot. Veel medewerkers die bedrijven verlaten nemen gevoelige informatie mee, en nu door de economische crisis meer medewerkers bedrijven verlaten is het risico tot het lekken van gevoelige informatie groter geworden. Tevens drukt de economische crisis op de beschikbare IT-budgetten en het IT-personeel.

De aanschaf van een DLP-softwarepakket kan een effectief middel zijn ter voorkoming van een data leakage incident. Deze softwarepakketten bieden bescherming door zich te richten op data die zich verplaatsen, opgeslagen zijn of in gebruik zijn. Deze data worden vervolgens met geavanceerde technieken geanalyseerd op overeenstemming met de vooraf ingestelde regels. Buiten het beschermen tegen data leakage incidenten bieden DLP-softwarepakketten tevens voordelen bij het voldoen aan wet- en regelgeving, het aantonen van compliancy en het verhogen van het informatiebeveiligingsbewustzijn onder de werknemers.

Ondanks alle voordelen dient men zich te realiseren dat ook DLP-softwarepakketten hun beperkingen hebben. Zij richten zich niet op kwaadaardige aanvallen van hackers en bieden alleen bescherming tegen het lekken van elektronische informatie. Desondanks kan een DLP-softwarepakket een effectief middel zijn tegen het ongewenst naar buiten komen van gevoelige informatie.

Literatuur

[EGDL09] *The Executive Guide to Data Loss Prevention*, Securosis LLC, March 2009.

[Herm09] Ing. J.A.M. Hermans en drs. J.W. de Jong, *Information Leakage Prevention – Putting your information first*, KPMG IT Advisory, 2009.

[Mars08] M. Marshall, M. Martindale, R. Leaning en D. Das, *Data Loss Barometer*, KPMG, September 2008.

[Mars09] M. Marshall, M. Martindale en R. Leaning, *Data Loss Barometer; Review of 2008 and Predictions for 2009*, KPMG, 2009.

[OEDL09] *Outbound Email and Data Loss Prevention in Today's Enterprise*, Proofpoint, 2009.

[Oule09] E. Ouellet en P.E. Proctor, *Magic Quadrant for Content-Aware Data Loss Prevention*, Gartner, 2009.

[Pone09a] Dr. L. Ponemon, *Data Loss Risks During Downsizing; As Employees Exit, so does Corporate Data*, Ponemon Institute LLC, 2009.

[Pone09b] Dr. L. Ponemon, *Fourth Annual US Cost of Data Breach Study; Benchmark Study of Companies*, Ponemon Institute LLC, 2009.

[Spai08] K. Spaink, *Dutch Data Breaches*, http://www.spaink.net/dutch-data-breaches/, 2009.

[Vlie08] A.H.P. van Vliet, *Data Leakage and It's Prevention*, TU Delft, September 2008.