

HOE GAAT U OM MET GEVOELIGE DATA?

IT-MANAGERS ZIJN NIET VOORBEREID OP EUROPESE PRIVACYREGELS VOOR DATAWISSEN

81 procent van de IT-managers in Europa is nog niet op de hoogte van de nieuwe EU-verordening op het gebied van gegevensbescherming, de EU General Data Protection Regulation (GDPR). Dit blijkt uit onderzoek van Kroll Ontrack, specialist op het gebied van respectievelijk gegevensherstel en gegevensverwijdering. Op grond van de verordening kunnen bedrijven en instellingen worden verplicht om opgeslagen data in laptops, flash media, mobiele apparaten, servers en in de cloud, permanent te wissen. Maar hoe doe je dat op een veilige en gecontroleerde manier?



De GDPR heeft tot doel de wetgeving op het gebied van gegevensbescherming samen te voegen. Niet alleen om de uitdagingen van het digitale tijdperk het hoofd te kunnen bieden, maar ook om online opgeslagen persoonlijke gegevens beter te kunnen beschermen. Zo worden Europese bedrijven verplicht persoonlijke data op verzoek, of als deze niet meer wordt gebruikt, te wissen. De GDPR is een verordening en geen richtlijn, zoals de Richtlijn bescherming persoonsgegevens van 1995. De nieuwe Europese wet heeft extraterritoriale werking, waardoor Amerikaanse ondernemingen die naar Europa exporteren ook aan de regels moeten voldoen. Verder maakt in de grotere bedrijven de Data Protection Officer zijn opwachting. Hij of zij moet zorgen dat de onderneming of instelling compliant blijft.

In de pers kreeg het omstreden 'right to be forgotten' tot nog toe de meeste aandacht. Terecht, maar in het kader van de totale levenscyclus van bedrijfsgegevens zijn er meer aspecten die om aandacht vragen. Uit het bovengenoemde onderzoek blijkt namelijk dat 61 procent van de IT-managers geen maatregelen heeft getroffen voor het naleven van de op handen zijnde verordening. Daarvan heeft meer dan de helft (55 procent) het nagelaten het beleid voor gegevensvernietiging te herzien en aan te passen – en daarvan heeft weer een kwart toegegeven geen operationeel proces te hebben voor gegevensvernietiging. Opmerkelijk, omdat uit hetzelfde onderzoek blijkt dat 57 procent van de 660 ondervraagde IT-managers wel verwacht dat de nieuwe wetgeving gevolgen voor hen zal hebben. Wellicht dat de aangekondigde

sancties, 250.000 tot 100 miljoen euro boete, of een boete van respectievelijk 0,5 en 5 procent van de jaarlijkse wereldwijde omzet, managers alsnog aan het denken zet.

SPOOKDATA

Iedereen kent ze wel: verhalen over mensen die hun afgedankte computer bij het grof vuil zetten, maar die later geconfronteerd worden met gevoelige informatie die nog op de harde schijf van het apparaat stond. Het mag ondertussen ook bekend worden verondersteld dat DEL en SHIFT+DEL of het verwijderen uit de prullenbak niet afdoende is. Het DEL-commando haalt alleen een referentie weg uit de tabel. Hierdoor denkt het operating system dat het document verdwenen is, maar alle data staat nog op de harde schijf, totdat het bestand wordt overschreven. Het format-commando wijzigt slechts de tabel, zodat het lijkt dat alle bestanden en bibliotheken zijn gewist. Maar de onderliggende data staat nog steeds op de disk. Er zijn manieren om data écht voorgoed te wissen.

OVERSCHRIJVEN

Overschrijven van data is een goede methode om data te vernietigen. Het is daarbij belangrijk om zeker te weten dat alle gegevens daadwerkelijk zijn overschreven. Gebruikers zijn vaak niet op de hoogte waar en hoe op de harde schijf de data wordt opgeslagen. Zo worden er door verschillende programma's veel reservekopieën aangehouden op 'temporary sites', maar staan ook veel gegevens in allerlei log files. Maar ook zijn er gebieden waar je normaal niet bij komt, zoals bij SSD's. Het is met name van belang dat een onafhankelijke instantie de software heeft getest op werking.

SHREDDING EN FYSIEKE VERNIETIGING

Fysiek beschadigen of harde schijf shred-den, ook wel de sledgehammer-methode genoemd. Kan effectief zijn, zeker omdat de kosten voor het terughalen van zwaar beschadigde schijven heel erg hoog zijn en in sommige gevallen onmogelijk. Op een klein stukje van 5 bij 5 millimeter kunnen nog meer dan 750.000 A4'tjes met data staan, een stapel van wel 75 meter hoog. De European Association for Data Media Security publiceert de DMS 2008 Standaard voor fysieke HDD-vernietiging.

DEGAUSSEN OF DEMAGNETISEREN

Een degausser vernietigt alle magnetisch geregistreerde gegevens, zoals op tape drives of harde schijven, met behulp van een sterk magnetisch veld. Degaussen is snel, effectief en milieuvriendelijk. Belangrijk is wel om na te gaan of het gebruikte magnetisch veld sterk genoeg is en hoe lang een specifieke hard disk daaraan moet worden blootgesteld. De hoeveelheid energie die nodig is om een opgenomen signaal volledig te wissen noemen we coërciviteit. Met de huidige schijven bedraagt deze $\geq 10K$ Gauss.

SOFTWAREMATIC

Uit onderzoek blijkt dat 54 procent van de tweedehands mobiele telefoons nog persoonlijke gegevens bevat, denk aan vertrouwelijke rapporten, e-mails en bankdetails. Zogenaemde 'wipe-standaarden' zijn er in overvloed. Wat te denken van Air Force System Security Instructions 5020, Bruce Schneier's algorithm, The National Computer Security Centre (NCSC-TG-025), de German Standard BSI enzovoorts. Meestal wordt echter gebruikgemaakt van gecertificeerde software die de hele schijf overschrijft volgens de zogenaemde Amerikaanse DoD5220.22-M-standaard. Volgens deze norm wordt de harde schijf drie maal overschreven en geverifieerd. Momenteel is speciale verwijderingssoftware beschikbaar voor servers, laptops en pc's. Daarnaast is er voor smartphones en tablets een aparte oplossing en komen specifieke bestanden en LUN's voor selectieve dataverwijdering in aanmerking.

AUDIT

Dataverwijdering is moeilijk aan te tonen, zeker als er geen bewijs kan worden overlegd, zoals wel vereist is volgens de EU-regelgeving. Verwijdering van data is belangrijk, maar het bewijs van de verwijdering is nóg belangrijker. Idealiter kan het proces centraal worden beheerd via een management console. Hierdoor ontstaat een compleet, controleerbaar gegevensverwijderingsproces (data erasure). Gecertificeerde dienstverleners op het terrein van verwijderingssoftware verstrekken gedetailleerde rapporten aan het einde van elk verwijderingsproces. Daarmee kunnen managers met het volste vertrouwen een volledige audit tegevoet zien. Digitaal ondertekende rapportages geven cruciale informatie over



wanneer, hoe en door wie de gegevens zijn verwijderd, evenals het serienummer van het apparaat en de conditie van de hardware.

CONCLUSIE

Datawissen is een vak apart. Het is een klus voor specialisten. Schakel daarom een aanbieder in met gecertificeerde methodes voor gegevensvernietiging. Deze specialisten bieden de benodigde tools, diensten en certificaten om data veilig te verwijderen van servers en andere apparaten, zoals mobiele telefoons en tablets. Hiermee voorkomt u dat data in verkeerde handen valt en uw bedrijf reputatie- en financiële schade lijdt door torenhoge boetes.

Jaap-Jan Visser is country manager van Kroll Ontrack Nederland

KROLL ONTRACK NEDERLAND
KRUISWEG 825C
2132 NG HOOFFDORP
T 023 - 56 73 030
E INFO@KROLLONTRACK.NL
I WWW.ONTRACKDATARECOVERY.NL