
De risico's van draagbare opslagmedia

Ongecontroleerd gebruik van iPods, USB-sticks, PDA's en andere apparatuur op uw netwerk kan leiden tot gegevensdiefstal, introductie van virussen, juridische problemen en meer

In een maatschappij waarin veel gebruik wordt gemaakt van draagbare opslagmedia wordt het risico dat het gebruik van dergelijke apparatuur met zich meebrengt veelal genegeerd. Dit white paper gaat in op de risico's van het gebruik van draagbare opslagmedia en de maatregelen die organisaties kunnen nemen om ze te vermijden.

Inleiding

In een samenleving waarin mensen eenvoudig toegang hebben tot draagbare muziekspelers, PDA's, mobiele telefoons en digitale camera's heeft de techniek ingespeeld op persoonlijke behoeften met de ontwikkeling van elektronische apparatuur waarop gegevens kunnen worden opgeslagen. Er kleeft echter een nadeel aan dit scenario – misbruik van dergelijke apparatuur kan voor een bedrijf de ondergang betekenen! De cijfers zijn niet erg bemoedigend: volgens onderzoek van CSI/FBI is de schade door diefstal van vertrouwelijke informatie toegenomen van \$168.529 in 2004 naar \$355.552 in 2005.

■ **2005 CSI/FBI computer crime and security survey**

“De schade door diefstal van vertrouwelijke informatie is toegenomen van \$168.529 in 2004 naar \$355.552 in 2005.”

Bedrijven die de ernst van dit probleem begrijpen, voeren beleid in om het gebruik van draagbare opslagmedia te reguleren. Maar is beleid alleen de beste manier om het probleem te bestrijden? En wat zijn nu precies de risico's van ongecontroleerd gebruik van draagbare opslagmedia?

Inleiding	2
De opkomst van draagbare opslagmedia	2
Waarom hebben bedrijven bescherming nodig?.....	3
Veelgebruikte tegenmaatregelen	6
Conclusie.....	6
Over GFI.....	7
Referenties	8

De opkomst van draagbare opslagmedia

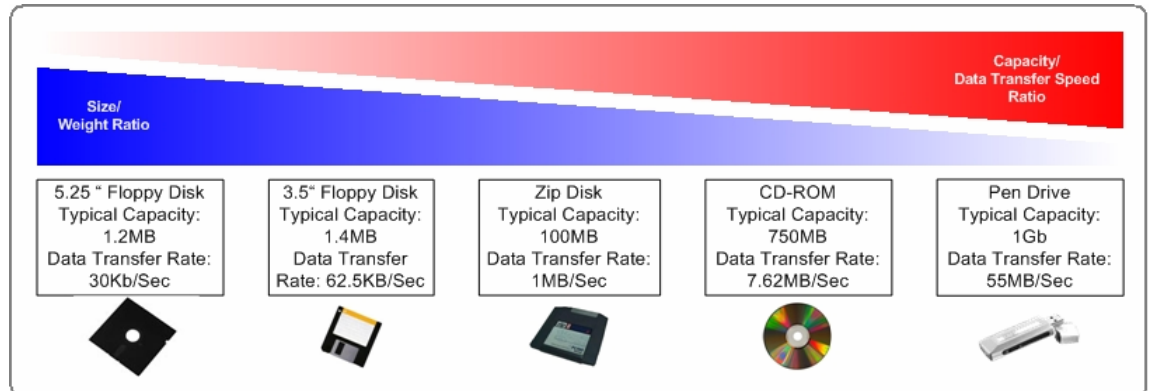
In de laatste tien jaar is de techniek zo ver vooruitgegaan dat men niet meer afhankelijk is van grote apparaten met beperkte opslagcapaciteit. Gevolgen van deze technische vooruitgang zijn:

- exponentiële toename van opslagcapaciteit en overdrachtsnelheid;
- apparaten zijn kleiner geworden en zijn dus makkelijker mee te nemen;
- door de komst van populaire, goedkope producten zijn er meer soorten apparaten beschikbaar;
- draagbare media kunnen nu gemakkelijker verbonden worden aan computersystemen.

Een typisch voorbeeld is de Apple iPod die in oktober 2005 op de markt werd gebracht. Hierop kan 60 GB aan gegevens worden opgeslagen – even veel als op de harde schijf van de

gemiddelde computer. Dit zijn mogelijk miljoenen bestanden met vertrouwelijke informatie!

De overdracht van gegevens tussen computersystemen is tegenwoordig een heel eenvoudig en onopvallend proces. Dit betekent een risico aangezien misbruik van draagbare opslagmedia bedrijfsnetwerken kan blootstellen aan verscheidene gevaren die op diverse manieren schade kunnen berokkenen aan bedrijven.



Voorbeelden van draagbare opslagmedia

Waarom hebben bedrijven bescherming nodig?

Volgens de statistieken wordt 98% van de misdaden tegen bedrijven in het Verenigd Koninkrijk gepleegd door insiders. Als kwaadaardige insiders of onvoorzichtige werknemers misbruik maken van draagbare opslagmedia, kunnen bedrijven te maken krijgen met gegevensdiefstal, wettelijke aansprakelijkheid, productiviteitsverlies en inbraken op het netwerk.

■ Scotland Yard

"98% van alle misdaden tegen bedrijven in het Verenigd Koninkrijk wordt gepleegd door insiders."

Gegevensdiefstal

Het stelen van bedrijfsgegevens is vrij eenvoudig en tegenwoordig bestaat er software waarmee het hele proces geautomatiseerd kan worden. Men hoeft alleen het draagbare opslagmedium in een computer in te pluggen en alle data, inclusief vertrouwelijke gegevens, worden automatisch gekopieerd zonder dat de gebruiker iets hoeft te doen. Met behulp van dit proces (ook wel 'pod slurping' genoemd) kunnen complete databases en andere vertrouwelijke gegevens in enkele minuten op een draagbaar opslagmedium worden opgeslagen.

■ Serious Organized Crime Agency (SOCA) – U.K.

"...één van de grootste bedreigingen is nog steeds afkomstig van insiders: mensen in het bedrijf die het systeem aanvallen."

Niet alleen insiders kunnen uw gegevens stelen. Mensen van buiten het bedrijf kunnen met behulp van 'social engineering' nietsvermoedende werknemers overhalen om draagbare opslagmedia op het bedrijfsnetwerk te gebruiken. Met behulp van malware worden er dan zogenaamde backdoors geopend waarmee hackers gemakkelijk toegang tot bedrijfsgegevens kunnen verkrijgen. Een bekend voorbeeld hiervan is een experiment dat in 2006 is uitgevoerd door The Training Camp, een opleidingsinstituut in het Verenigd Koninkrijk (Sturgeon, 2006). The Training Camp verdeelde promotionele cd's onder de werknemers in een bedrijf. Behalve het op de verpakking vermelde materiaal bevatten deze cd's echter ook een script dat The Training Camp liet weten wanneer ze werden gebruikt. Ondanks het feit dat werd aangeraden de beveiligingsrichtlijnen van het bedrijf te controleren alvorens de cd te draaien, werden 75 van de 100 gedistribueerde cd's op het bedrijfsnetwerk gebruikt. Dit experiment onderstreept het feit dat in goed vertrouwen handelende werknemers de beste perimeterbeveiliging kunnen omzeilen en zo het bedrijf aan ernstige gevaren kunnen blootstellen.

De meeste bedrijven verzamelen vele gegevens die kunnen worden gestolen. Hieronder vallen onder andere:

- Blauwdrukken en ontwerptekeningen;
- Biedingen, budgets, klantenlijsten, e-mails en prijslijsten;
- Creditcardgegevens en andere financiële informatie;
- Broncode van software en database schema's;
- Medische informatie en andere persoonlijke gegevens;
- Geheime of persoonlijke informatie;
- Scripts, storyboards, gedrukt materiaal, foto's, video's of tekenfilms;
- Bladmuziek, songteksten, geluidsbestanden en andere vormen van geluidsmateriaal.

■ **U.S. Secret Service & CERT Coordination Centre**

"Respondenten beschouwen huidige of voormalige werknemers en contractwerkers als de op één na grootste bedreiging, alleen voorafgegaan door hackers."

De gestolen gegevens kunnen verkocht worden aan concurrenten of gebruikt worden door de insiders, hun criminele vrienden of hackers om een keur aan misdaden te plegen variërend van identiteitsfraude tot afpersing en chantage. Bovendien kunnen werknemers die het bedrijf verlaten om voor een concurrent te gaan werken de verkregen gegevens gebruiken om een voorsprong op hun voormalige werkgever te krijgen of diens imago te beschadigen. Uit onderzoek van de Amerikaanse geheime dienst en het CERT Co-ordination centre is gebleken dat "respondenten huidige of voormalige werknemers en contractwerkers beschouwen als de op één na grootste bedreiging, alleen voorafgegaan door hackers" (Keeney et al., 2005). Dit wordt bevestigd door de CSI/FBI enquête waarin 68% van de respondenten aangeeft verliezen

■ **2006 CSI/FBI Computer crime and security survey**

"68% van de respondenten geeft aan verliezen te hebben geleden door inbraken op het netwerk door insiders."

te hebben geleden door acties van insiders (Gordon et al., 2006).

Wettelijke aansprakelijkheid

Als vertrouwelijke informatie 'zoek' raakt of er door middel van draagbare opslagmedia illegale/bezwaarlijke gegevens op uw bedrijfsnetwerk worden geïntroduceerd, kan uw bedrijf wettelijk aansprakelijk worden gesteld voor gestolen of op illegale wijze geïntroduceerde informatie. Afhankelijk van plaatselijke wetgeving kan dit een flinke impact hebben op de activa van uw bedrijf. Zo staat er onder HIPAA (in de Verenigde Staten) een boete van maximaal \$250.000 en 10 jaar gevangenisstraf op het onterecht openbaar maken van persoonlijke medische informatie. In de onderstaande tabel kunt u zien welke wetten in welk land van toepassing zijn.

Land:	Wetten
VS	Sarbanes Oxley Act , Gramm-Leach-Bliley Act , USA PATRIOT Act , Title 21 of the Federal Regulations Part 11 (21 CFR Part 11) , Federal Information Security Management Act , HIPAA
EU	Data Protection Directive , Privacy and Electronic Communication Regulations ; EU Annex 11 , Computerized Systems
Verenigd Koninkrijk	Turnbull Guidance Act [1999] , Companies Act , Data Protection Act , Freedom of Information Act , Money Laundering Regulations 2003
Japan	Personal Information Protection Act 2003
Canada	Personal Information Protection and Electronic Document Act (PIPEDA)
Australië	The Federal Privacy Act (Privacy Act 1988)

Productiviteitsverlies

Het bedrijfsnetwerk kan worden misbruikt door onbetrouwbare werknemers die draagbare opslagmedia gebruiken om de perimeterbeveiliging te omzeilen om persoonlijke bestanden te kunnen gebruiken. Voorbeelden hiervan zijn werk voor een part-time baan of materialen voor een hobby waaraan onder werktijd tijd wordt besteed. Het probleem wordt nog groter wanneer iemand videospelletjes mee naar kantoor neemt. Deze zijn verslavend en eisen veel aandacht op. Spelletjes voor twee of meer spelers kunnen zelfs meer dan één werknemer tegelijk van het werk afleiden.

Inbraken op het bedrijfsnetwerk

Het gebruik van draagbare apparatuur op het werk kan ook de veiligheid van het bedrijfsnetwerk in gevaar brengen door de al dan niet doelbewuste introductie van virussen, malware of crimeware waardoor het netwerk onbeschikbaar wordt en het werk wordt onderbroken. Wetshandhavende instanties erkennen tegenwoordig dat "...één van de grootste dreigingen nog steeds van insiders afkomstig is, dus mensen in het bedrijf die het systeem

■ U.S. Federal Trade Commission

"Misnoegde werknemers die toegang weten te verkrijgen tot klantenlijsten en andere informatie vormen een toenemend gevaar."

aanvallen" (Ilett, 2006).

Veelgebruikte tegenmaatregelen

Bedrijven die ongeautoriseerd gebruik van draagbare apparatuur willen voorkomen hebben slechts enkele methoden tot hun beschikking. Wat vaak gebeurt is dat het meebrengen van draagbare opslagmedia wordt verboden en toegangspoorten geblokkeerd worden. Ook worden Windows Group Policies ingezet. Deze tegenmaatregelen hebben echter diverse tekortkomingen:

- De meeste draagbare opslagmedia zijn klein en gemakkelijk te verbergen. Het is dus moeilijk om ervoor te zorgen dat niemand een verboden apparaat meebrengt.
- Met bovenstaande methoden is het niet mogelijk om onderscheid te maken tussen legitieme en verboden apparaten.
- Het kost tijd en geld om deze tegenmaatregelen te implementeren.

De enige echt effectieve methode is het gebruik van software waarmee het bedrijfsnetwerk wordt beschermd tegen ongeautoriseerd gebruik van apparatuur. Op deze manier kunt u onderscheid maken tussen legitiem en verboden gebruik van apparatuur, in overeenstemming met het beveiligingsbeleid van uw bedrijf.

GFI Software biedt een permanente oplossing om uw bedrijf te beschermen tegen de gevaren van draagbare opslagmedia: GFI EndPointSecurity. Dit is dé manier om dreigingen van binnenuit tegen te gaan! Met GFI EndPointSecurity heeft u controle over data die via draagbare opslagmedia het netwerk binnenkomen of verlaten. U kunt dus voorkomen dat gebruikers vertrouwelijke gegevens meenemen of virussen en trojans op uw netwerk zetten. Met GFI EndPointSecurity kunt u bepalen wie gebruik mag maken van media players (zoals iPod en Creative Zen), USB-sticks, CompactFlash, geheugenkaarten, PDA's, Blackberry's, mobiele telefoons, cd's, diskettes, en meer. Kijk voor meer informatie en een trialversie op <http://www.gfi.nl/nl/endpointsecurity/>.

Conclusie

Ongecontroleerd gebruik van draagbare opslagmedia door werknemers vormt een grote bedreiging voor de veiligheid en stabiliteit van ieder bedrijf. Kwaadwillende insiders en onvoorzichtige werknemers vormen de zwakste schakel in uw beveiliging. Het is niet verstandig om erop te vertrouwen dat gebruikers zich vrijwillig aan de regels zullen houden – u moet software gebruiken om dit risico af te weren. Met GFI EndPointSecurity kunt u ernstige problemen voorkomen. De continuïteit van uw bedrijf is verzekerd en uw bedrijf is beschermd tegen ongeautoriseerde gegevensoverdracht van en naar draagbare opslagmedia. Met GFI EndPointSecurity zijn bedrijven permanent beschermd!

Over GFI

GFI is een toonaangevende ontwikkelaar van software voor netwerkbeveiliging, inhoudsbeveiliging en messaging. Dankzij bekroonde technologie, een agressieve prijsstrategie en een sterke focus op MKB-bedrijven helpt GFI bedrijven over de hele wereld om maximale continuïteit en productiviteit te bewerkstelligen. GFI is opgericht in 1992 en heeft kantoren in Malta, Londen, Raleigh, Hong Kong, Adelaide en Hamburg die wereldwijd meer dan 200.000 installaties ondersteunen. GFI is een kanaalgericht bedrijf met meer dan 10.000 partners over de hele wereld. GFI is ook een Microsoft Gold Certified Partner. Meer informatie over GFI is te vinden op <http://www.gfi.nl>.

Referenties

Canadian Parliament (2000) *Personal Information Protection and Electronic Documents Act* available from: http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp (last cited 28 July 2006).

Commission of the European Communities (2000) *Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector* available from: http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/com2000-385en.pdf (last cited 28 July 2006).

Computer Crime Research Center (2005) *Security issues: find the enemy within* available from: <http://www.crime-research.org/analytics/security-insider/> (last cited 28 July 2006).

European Parliament and the Council of the European Union (2002) *Directive on privacy and electronic communications* available from: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML> (last cited 28 July 2006).

European Parliament and the Council of the European Union (2003) *Annex 11 Computerised systems*, Labcompliance available from: <http://www.labcompliance.com/documents/europe/h-213-eu-gmp-annex11.pdf> (last cited 28 July 2006).

Federal Trade Commission (1999) *Gramm-Leach Bliley Act* available from: <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html> (last cited 28 July 2006).

Financial Reporting Council (2005) *Internal Control: Guidance for Directors on the Combined Code* available from: <http://www.frc.org.uk/documents/pagemanager/frc/Revised%20Turnbull%20Guidance%20October%202005.pdf> (last cited 28 July 2006).

Gordon L.A., Loeb M.P., Lucyshyn W. and Richardson R. (2005) *2005 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute.

Gordon L.A., Loeb M.P., Lucyshyn W. and Richardson R. (2006) *2006 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute.

Ilett D. (2006) "Trusted insiders" a threat to corporate security, silicon.com available from: <http://www.silicon.com/research/specialreports/idmanagement/0,3800011361,39158361,00.htm> (last cited 28 July 2006).

Japanese Government (2003) *Personal Information Protection Act 2003* available from: <http://www.privacyexchange.org/japan/PIPA-offtrans.pdf> (last cited 28 July 2006).

Keeney M., Kowalski E., Cappelli D., Moore A., Shimeall T. and Rogers S. (2005) *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, U.S Secret Service and CERT Coordination Center/SEI.

Leahy P. (2001) *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, H.R. 3162 Section-by-section Analysis* available from: <http://leahy.senate.gov/press/200110/102401a.html> (last cited 28 July 2006).

NIST Computer Security Division (2002) *Federal Information Security Management Act of 2002* available from: <http://csrc.nist.gov/policies/FISMA-final.pdf> (last cited 28 July 2006).

Office of Legislative Drafting and Publishing (2006) *Privacy Act 1988* available from: http://www.privacy.gov.au/publications/privacy88_030706.pdf (last cited 28 July 2006).

Sarbanes-Oxley (2002) *Sarbanes-Oxley Act of 2002* available from: http://www.sarbanes-oxley.com/section.php?level=1&pub_id=Sarbanes-Oxley (last cited 28 July 2006).

Sturgeon W. (2006) *Proof: Employees don't care about security, silicon.com* available from: <http://software.silicon.com/security/0,39024655,39156503,00.htm> (last cited 28 July 2006).

United Kingdom Parliament (1989) *Companies Act 1989* available from: http://www.opsi.gov.uk/acts/acts1989/Ukpga_19890040_en_1.htm (last cited 28 July 2006).

United Kingdom Parliament (1998) *Data Protection Act 1998* available from: <http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm> (last cited 28 July 2006).

United Kingdom Parliament (2000) *Freedom of Information Act 2000* available from: <http://www.opsi.gov.uk/ACTS/acts2000/20000036.htm> (last cited 28 July 2006).

United Kingdom Parliament (2003) *The Money Laundering Regulations 2003* available from: <http://www.opsi.gov.uk/si/si2003/20033075.htm> (last cited 28 July 2006).

U.S. Food and Drug Administration (2000) *Title 21 Code of Federal Regulations (21 CFR Part 11): Electronic Records; Electronic Signatures* available from: http://www.fda.gov/ora/compliance_ref/part11/ (last cited 28 July 2006).

U.S. Department of Health & Human Services (1996) *Health Insurance Portability and Accountability Act of 1996* available from: <http://aspe.hhs.gov/admsimp/pl104191.htm> (last cited 28 July 2006).

© 2007 GFI Software Ltd. Alle rechten voorbehouden. De informatie in dit document geeft het standpunt van GFI weer betreffende de besproken onderwerpen op de datum van publicatie. Aangezien GFI moet reageren op veranderende marktomstandigheden, moet dit document niet als een toezegging van GFI worden geïnterpreteerd. Na de publicatiedatum kan de correctheid van de informatie niet worden gegarandeerd. Dit white paper dient puur ter informatie. GFI GEEFT IN DIT DOCUMENT GEEN ENKELE GARANTIE, EXPLICIET NOCH IMPLICIET. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor en de bijbehorende logo's zijn ofwel geregistreerde handelsmerken of handelsmerken van GFI Software Ltd. in de Verenigde Staten en/of andere landen. Alle product- en bedrijfsnamen in dit persbericht zijn mogelijk handelsmerken van hun respectievelijke eigenaren.