
Pod Slurping – Een eenvoudige techniek voor het stelen van data

Problemen met ongecontroleerd gebruik van iPods, USB sticks en flash drives op uw netwerk

Veel mensen denken onterecht dat firewalls en antivirussoftware een afdoende beveiliging vormen voor vertrouwelijke gegevens op het bedrijfsnetwerk. In dit white paper kunt u lezen hoe ongecontroleerd gebruik van draagbare opslagmedia zoals iPods, USB-sticks, flash drives en PDA's in combinatie met technieken als 'pod slurping' tot ernstige beveiligingsproblemen kan leiden.

Inleiding

We worden steeds afhankelijker van technologie. Draagbaarheid, gebruiksgemak, een mooi uiterlijk en een flinke dosis marketinghype vormen samen de perfecte mix om de massa te verleiden! De vraag naar draagbare elektronische consumentenproducten blijft toenemen. Zo is de iPod van Apple één van de meest succesvolle elektronische gadgets ter wereld. Sinds de introductie van de iPod in 2001 heeft Apple bijna 60 miljoen exemplaren verkocht (CNNMoney.com, 2006). De iPod is een universeel populair product geworden – het eponiem voor MP3 spelers. Volgens voorspellingen zal de vraag naar iPods en andere MP3 flash-memory muziekspelers blijven groeien naar bijna 124 miljoen in 2009 (Kevorkian, 2005).

■ IDC Market Analysis

“De verkoop van iPods en andere MP3 flash memory muziekspelers zal in 2009 toenemen tot bijna 124 miljoen exemplaren.”

De toenemende populariteit van iPods betekent dat een leger witte oordopjes langzaam de werkvloer aan het veroveren is. Deze MP3 spelers worden tegenwoordig even vaak op de werkvloer als in de trein gesignaleerd. Maar wat is er zo alarmerend aan iPods en MP3 spelers op het werk?

Inleiding	2
Pod slurping: hoe kunnen insiders uw data stelen?	2
Pod slurping: een eenvoudige techniek voor het stelen van data.....	3
Informatiediefstal door insiders is een groot probleem	4
Waarom zouden insiders informatie willen slurpen?	4
Hoe kunnen bedrijven gegevensdiefstal voorkomen?	5
Conclusie	6
Over GFI EndPointSecurity	6
Over GFI	7
Referenties	8

Pod slurping: hoe kunnen insiders uw data stelen?

De technische ontwikkelingen op het gebied van draagbare gegevensopslag gaan steeds sneller. De nieuwste versies van MP3 spelers en vergelijkbare apparaten kunnen enorme hoeveelheden data opslaan en zijn klein genoeg om ongemerkt het bedrijf binnen te worden gesmokkeld. Bovendien kunnen ze steeds gemakkelijker worden verbonden en kunnen ze met steeds grotere snelheid data overdragen. Men hoeft het apparaat slechts in een USB- of FireWire-poort in te pluggen en klaar is Kees: er zijn geen drivers nodig en er hoeft niets geconfigureerd te worden! In de praktijk betekent dit dat dieven vertrouwelijke data kunnen stelen en dat onzorgvuldige werknemers virussen op het bedrijfsnetwerk kunnen zetten, zelfs

als ze maar heel even met het netwerk verbonden zijn.

De iPod is slechts één voorbeeld van dergelijke draagbare instrumenten. Op het eerste gezicht lijkt het een onschuldige draagbare muzikspeler. Hij kan echter 60 GB aan gegevens opslaan: het equivalent van de hoeveelheid data op een gemiddeld werkstation. Dit betekent dat insiders met kwade bedoelingen iPods kunnen gebruiken om financiële gegevens, consumenteninformatie en andere vertrouwelijke informatie te stelen!

■ **2006 Identity Fraud Survey**

“In 2005 bedroeg de door identiteitsfraude veroorzaakte schade \$56,6 miljard.”

Contu en Girard (2004) waarschuwen voor de risico's die het ongecontroleerd gebruik van draagbare opslagmedia met zich meebrengt. De diefstal van informatie is een ware plaag geworden. Beveiligingsexperts spreken van lekken, dataversleuteling en *data disclosure incidents*. De meest originele term is echter 'pod slurping', bedacht door de Amerikaanse beveiligingsexpert Abe Usher (2005).

Pod slurping: een eenvoudige techniek voor het stelen van data

Usher gebruikt de term 'pod slurping' om te beschrijven hoe MP3 spelers zoals iPods en andere USB-apparaten gemakkelijk gebruikt kunnen worden om vertrouwelijke informatie te stelen. “Er zijn oneerlijke mensen op de wereld”, zegt Usher. “Velen van hen werken bij bedrijven – en deze USB-apparaten maken het stelen van gigantische hoeveelheden data heel eenvoudig” (Schick, 2006).

Om aan te tonen hoe kwetsbaar bedrijfsnetwerken zijn, heeft Usher een software-applicatie ontwikkeld die automatisch bedrijfsnetwerken kan doorzoeken en kritieke gegevens op een iPod kan zetten. Deze software-applicatie draait rechtstreeks vanaf een iPod en kan binnen enkele minuten grote hoeveelheden data van een computer 'slurpen'. En niet alleen iPods en MP3 spelers kunnen slurpen. Alle draagbare opslagmedia kunnen worden gebruikt om informatie op te slurpen. Voorbeelden zijn digitale camera's, PDA's, thumb drives, mobiele telefoons en andere plug-and-play apparaten.

Het slurpen van data is een heel eenvoudig, geautomatiseerd proces waarvoor geen enkele technische kennis nodig is. De gebruiker kan het draagbare apparaat in een werkstation inpluggen en alle vertrouwelijke gegevens op dat werkstation kopiëren in minder tijd dan nodig is voor het beluisteren van één MP3-bestand.

■ **Pod Slurping Blog**

“... in twee minuten kan men 100 MB downloaden aan Word-, Excel- of PDF-bestanden - eigenlijk alles wat bedrijfsgegevens kan bevatten...”

Informatiediefstal door insiders is een groot probleem

Informatiediefstal is voor iedere organisatie een steeds groter probleem en er wordt dus een steeds groter deel van het IT-budget gereserveerd voor de preventie ervan. Dit heeft twee oorzaken: de golf van aanvallen waarmee iedere industrie te maken heeft en de toename van wettelijke eisen op het gebied van beveiliging van klantgegevens en andere vertrouwelijke informatie. Organisaties worden door striktere controles and strengere straffen gedwongen om wetten en voorschriften serieuzer te nemen. In januari 2006 moest leverancier van identificatie- en verificatieservices ChoicePoint 15 miljoen dollar betalen voor het lekken van consumentgegevens en het schenden van het recht op de privacy (Federal Trade Commission, 2006).

In veel organisaties wordt ten onrechte gedacht dat de meeste gevaren van buiten afkomstig zijn. Elk jaar worden grote hoeveelheden geld uitgegeven aan firewalls en andere producten waarmee u uw netwerk tegen externe dreigingen kunt beveiligen. Volgens de statistieken nemen inbraken van binnenuit echter sneller toe dan aanvallen van buitenaf. Meer dan de helft van de inbraken vindt plaats van binnenuit. Helaas kunnen insiders de beveiliging gemakkelijk omzeilen. Het feit dat de eigen werknemers vertrouwd worden en continu aan gevoelige informatie worden blootgesteld betekent dat het niet gemakkelijk is om gegevensdiefstal te voorkomen – vooral in organisaties waar dergelijke informatie op grote schaal wordt verspreid!

■ Gartner Group

“70% van de ongeautoriseerde toegang tot informatiesystemen is het werk van de eigen werknemers.”

Waarom zouden insiders informatie willen slurpen?

Bedrijfsgegevens kunnen op diverse manieren winstgevend zijn. Denk maar aan ontwerptekeningen, biedingen, prijslijsten, broncode, databaseschema's, geluidsbestanden, songteksten, enzovoort. Al deze data zijn waardevol intellectueel eigendom en kunnen door individuen of bedrijven worden gebruikt om voordeel te behalen ten opzichte van concurrenten. Volgens onderzoek van CSI/FBI uit 2006 heeft diefstal van intellectueel eigendom het op drie na grootste economische effect op organisaties (Gordon et al., 2006). Kwaadwillenden kunnen ook gevoelige consumenteninformatie (zoals medische en financiële gegevens) van een bedrijf stelen en vervolgens openbaar maken. Dit heeft negatieve gevolgen voor de reputatie van het betreffende bedrijf. Bovendien kan het bedrijf aangeklaagd worden voor het schenden van het recht op de privacy.

De belangrijkste motieven voor gegevensdiefstal zijn waarschijnlijk kwade opzet, geldbejag en nieuwsgierigheid. Iedereen kan een vijand worden en er zijn dus vele verschillende soorten daders. Ontevreden werknemers die vinden dat ze uitgebuit worden of niet gerespecteerd

worden door hun werkgever kunnen misbruik maken van hun positie en bedrijfsplannen en andere gevoelige informatie verkopen aan concurrenten. Voormalige werknemers die vinden dat ze ten onrechte zijn ontslagen kunnen misbruik maken van hun kennis en hun connecties om consumentengegevens te stelen en openbaar te maken en zo het bedrijf schade te berokkenen. Insiders kunnen ook betaalde informanten worden en zich schuldig maken aan bedrijfsspionage, 'data warfare' en andere frauduleuze activiteiten zoals identiteitsfraude. De term 'identiteitsfraude' heeft betrekking op situaties waarin iemand de persoonlijke gegevens (bijvoorbeeld het sofi-nummer of creditcardnummer) van iemand anders gebruikt voor criminele

■ **2005 Identity Theft Summit**

"In Sacramento is iemand erin geslaagd om voor \$17.000 aankopen te doen met gebruik van de naam en het sofi-nummer van de beroemde golfer Tiger Woods!"

activiteiten. In de Verenigde Staten is dit het snelst groeiende misdrijf. Naar schatting zijn in 2005 negen miljoen volwassenen in de VS het slachtoffer geworden van identiteitsfraude (Johannes, 2006).

Hoe kunnen bedrijven gegevensdiefstal voorkomen?

Het belangrijkste voordeel van iPods en vergelijkbare producten is de eenvoudige toegang. In theorie kan dit voor bedrijven een groot voordeel zijn. Het is echter bekend dat toegang en beveiliging niet goed samengaan. U weet namelijk nooit wat gebruikers precies met hun draagbare apparatuur doen. Het kan wel lijken alsof een werknemer naar muziek op zijn iPod zit te luisteren, maar misschien zit hij wel schadelijke bestanden te uploaden of waardevolle gegevens te slurpen.

Een van de manieren om informatiediefstal te voorkomen is het implementeren van regels om het gebruik van draagbare opslagmedia te controleren. Sommige experts en onderzoekers adviseren conventionele methodes zoals het blokkeren van poorten, strenge supervisie en zelfs een algeheel verbod op iPods en vergelijkbare apparaten. Dit is echter niet de meest praktische benadering. Draagbare opslagmedia kunnen erg nuttig zijn en een algeheel verbod is dus contraproductief. Bovendien moet u er nooit vanuit gaan dat iedereen vrijwillig zal meewerken.

■ **Pod Slurping Blog**

"Op incidenten reageren kost meer dan proactief zijn!"

De beste manier om zeker te zijn van volledige controle over draagbare opslagmedia is door introductie van technologische barrières zoals GFI EndPointSecurity. GFI EndPointSecurity biedt volledige controle over gegevensoverdracht van en naar draagbare opslagmedia per gebruiker op het netwerk.

Conclusie

Bedrijven lopen altijd het risico vertrouwelijke informatie te verliezen. In dit white paper hebben we laten zien hoe ongecontroleerd gebruik van draagbare opslagmedia in bedrijven een groot risico vormt. Dit komt vooral doordat de meeste bedrijven perimeterbeveiliging prioriteit geven en de 'vijand in hun midden' negeren en het dus gemakkelijk maken voor insiders om waardevolle informatie te stelen.

Om bedrijfsgegevens te kunnen beveiligen en het slurpen van data te kunnen voorkomen moeten netwerkbeheerders het gebruik van draagbare opslagmedia kunnen controleren. Producten als GFI EndPointSecurity stellen beheerders in staat om controle uit te oefenen op het gebruik van draagbare opslagmedia op hun netwerk.

Over GFI EndPointSecurity

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/>.

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

CNNMoney.com (2006) *iPod, Mac Sales Boost Apple Profit Almost 48%* available from: http://money.cnn.com/services/tickerheadlines/for5/200607191714DOWJONESDJONLINE001233_FORTUNE5.htm (last cited 27 July 2006).

Contu R. and Girard J. (2004) *Put Security Policies in Place for Portable Storage Devices*, Gartner.

Federal Trade Commission (2006) *ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress* available from <http://www.ftc.gov/opa/2006/01/choicepoint.htm> (last cited 27 July 2006).

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

Hunter R. (2003) *Enterprises and Employees: The Growth of Distrust*, Gartner available from: <http://www.csoonline.com/analyst/report3317.html> (last cited 27 July 2006).

Johannes R. (2006) *2006 Identity Fraud Survey Report*, Javelin Strategy & Research.

Kevorkian S. (2005) *Worldwide and U.S. Compressed Audio Player 2005-2009 Forecast and Analysis: MP3 All Over the Place*, IDC.

Schick S. (2006) *Be afraid of the file-slurping iPod*, globeandmail.com available from: <http://www.theglobeandmail.com/servlet/story/RTGAM.20060209.wpodslurping09/BNStory/> (last cited 27 July 2006).

Scully J. (2005) *Summit on Identity Theft Solutions: Locking Up the Evil Twin* available from: <http://www.da.saccounty.net/main/idtheft2005.htm> (last cited 27 July 2006).

Usher A. (2005) *Pod slurping*, Sharp Ideas LLC available from: http://www.sharp-ideas.net/pod_slurping.php (last cited 27 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.