USB Stick beveiligen

Juli 2006

Henk Jongedijk, maandag 23 oktober 2006 - 00:00:00

Iedereen kent de vervanger van de floppy disk inmiddels wel: de USB stick. Heel veel computer gebruikers bezitten er tenminste Ã © Ã ©n. Het gadget gehalte is hoog; ze worden vaak ook als relatiegeschenk weggegeven. Recente nieuwsberichten over gestolen of verloren USB memory sticks met gevoelige informatie erop staan volop in de belangstelling. De gevallen die het nieuws halen bevatten veelal staats- of militaire geheimen, maar veel mensen hebben informatie die ze niet met iedereen willen delen. Het midden- en klein bedrijf (MKB) wil natuurlijk ook bedrijfsinformatie veilig behandelen. Wellicht heeft u zelf wat persoonlijke documenten op een USB stick staan die u niet zomaar te grabbel wil gooien. Verlies of diefstal kan veroorzaken dat vertrouwelijke informatie op straat komt te liggen. Nu USB-sticks gemeengoed zijn geworden neemt daarbij ook het gevaar ook toe dat belangrijke informatie terecht komt bij mensen waarvoor die niet bedoeld is.

Eigenlijk zou u uw USB stick moeten zien als een open kast: iedereen die de kastdeur opent kan zien wat er in ligt. Bedrijfsmatig gaat mijn voorkeur echter uit naar een soort kluis waarin je bestanden kunt zetten. Op het moment van openen van de kluis wordt er om je wachtwoord gevraagd.

Risico's

Steeds vaker worden USB keys gebruikt om data van de ene computer naar de andere te transporteren.
Vaak gaat het om vertrouwelijke (klant-) gegevens van bijvoorbeeld accountants en financieel adviseurs. En wat te denken van verschillende soorten onderzoeksrapporten, interne kostprijs berekeningen of juridische stukken. Het risico is behoorlijk groot dat een USB key verloren raakt of vergeten wordt en zo per ongeluk in handen van onbevoegden terecht komt.

Beveiliging

De beveiliging van data op USB keys is dan ook een hot item. Hardware leveranciers spelen op deze behoefte in; er zijn USB sticks verkrijgbaar met ingebouwde beveiliging (bijvoorbeeld NEC Microsafe USB keys). Buzz-words die bij dergelijke producten genoemd worden zijn steevast: security, encryptie, databeveiliging, versleutelen, PGP.

Korte risico analyse

Mijn simplistische risico analyse: ga uit van het slechts denkbare scenario (ook wel worst case scenario genaamd) en bedenk vervolgens wat het je waard is om de gevolgen te beperken. Business case: een USB stick waarop een aantal documenten staan met installatie instructies en wachtwoorden. Geen ultra geheime informatie, maar toch erg vervelend als je de stick kwijtraakt en iemand krijgt de wachtwoorden in handen. Dit worst case scenario heeft dus de definitie: "Ik raak mijn USB stick kwijt." Dit is zelfs een realistisch scenario, een USB stick is niet al te groot en kan snel zoekraken. Wat is het je waard om de gevolgen te beperken? Ik wil graag met enige investering hier wat aan doen. Het liefst in korte tijd en zonder al te veel geld uit te geven, zoals alle business requirements.

Gadgets

USB sticks zijn natuurlijk een ware rage; ze zijn verkrijgbaar in fraai design, als balpen, inclusief zakmes, ultralicht, in credit card formaat en als polsbandje. Sommige USB sticks hebben een extra knop waarmee de encryptiesoftware gestart wordt. Door de knop wat langer ingedrukt te houden start het automatisch synchroniseren van mappen en folders en kan de PC of notebook vergrendeld en ontgrendeld worden. Andere zijn voorzien van vingerafdruk herkenning. Deze laatste uitvoering is een zeer effectieve methode om informatie op de USB stick te beveiligen, maar is tevens een kostbare oplossing. Er van uitgaande dat we al een bestaande USB memory card hebben, zoek ik zelf niet naar nieuwe hardware, maar wil ik liever een software oplossing toepassen. Data versleuteling is dan het toverwoord.

Freeware?

Op Internet is veel software te vinden waarmee je data kunt versleutelen. Veel Windows software kost geld maar als je goed zoekt kun je ook wel gratis software vinden zoals bijvoorbeeld de tegenhanger van PGP, GnuPG. Met GnuPG kun je bestanden versleutelen echter het is niet mogelijk een complete USB stick te encrypten en deze weer aan een driveletter te koppelen onder Windows.
Ik ben een voorstander van open source en freeware. Legaal en gratis te gebruiken. De Truecrupt Foundation (www.truecrypt.org) biedt het freeware programma TrueCrypt aan. Je kunt het zo instellen dat het automatisch opstart wanneer je de USB-stick in je (Windows of Linux) PC stopt. TrueCrypt 'draait' dan ook vanaf je USB-stick. Op de site is documentatie en een beginners tutorial aanwezig.

Mijn ervaring

Na installeren op mijn USB stick van 250 MB draaide ik de standaard wizzard waarmee ik in enkele minuten een volume cre Ã «erde van 200 MB. Zo houd ik voldoende ruimte over om het programma erop te runnen Ã ©n ook om even mijn stick aan een collega te lenen. Stick erin, start truecrypt programma, mount volume, wachtwoord ingeven en vanaf dan is het beschermde volume onder een driveletter beschikbaar.

Conclusie

Het aanmaken van een beveiligde USB stick is niet zoveel werk als je wellicht eerst zou denken. Onbeveiligde USB sticks, zelfs voor ambtenaren en defensiepersoneel, zouden toch echt tot het verleden moeten behoren. Natuurlijk zijn er ook talloze andere alternatieven beschikbaar, maar de open source community biedt een aantal versleutelingsprogramma's die alles bieden wat je van encryptie software mag verwachten en nog gratis ook.

Relevante links

Algemeen:

http://en.wikipedia.org/wiki/USB_flash_drive
Werking van Truecrypt uitgelegd: http://www.security.nl/article/13114/1

Gadgets:

USB met mes: http://www.dedigitalerevolutie.nl/toontext.asp?id=5006
USB als balpen: http://www.dedigitalerevolutie.nl/toontext.asp?id=7459
USB met vingerafdruk herkenning: http://www.bioslimdisk.com/bioslimdisk.htm
USB in creditcard formaat: http://www.dedigitalerevolutie.nl/toontext.asp?id=12427
USB van 1 gram: http://www.dedigitalerevolutie.nl/toontext.asp?id=12369
USB als polsbandje: http://www.dedigitalerevolutie.nl/toontext.asp?id=12702
USB met display: http://www.dedigitalerevolutie.nl/toontext.asp?id=13958

Freeware:

http://www.truecrypt.org/downloads
http://www.powerarchiver.org
http://www.cypherix.com/nld/index.html
http://www.gnupg.org/

Betaald:

http://www.protect-me.com/index.htm

Nieuws:

Politie krijgt extra beveiligde USB stick
Politie tevreden met vingerafdruk
Weer geheimen Defensie op straat
Vinder usb stick met staatsgeheimen krijgt vvv bon

Memorystick met geheim defensiemateriaal zoek
Geheime informatie Defensie weer op straat
Memorysticks nauwelijks beveiligd
Werknemers gaan slordig om met geheugensticks
Defensie ontraadt gebruik usb-sticks

NASCHRIFT AUTEUR:

Alleen toen ik mijn TrueCrypt USB in een Dell pc met Windows XP Professional stopte kreeg ik om de haverklap de volgende melding (op mijn priv Ã © pc geen enkele last):

"Disk free space has dropped below the minimum threshold. Free up space on your hard disk drive by:

1. Backing up your data to a tape backup, ZIP or network drive.
2. Delete unused files.

If you are unsure which files are safe to move or delete, contact your Help Desk or consult your software manuals."

Er is genoeg leesvoer te vinden hierover in Google nieuwsgroepen.