Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Risico's en maatregelen

Bescherming tegen onveilige USB-sticks

Inhoud

Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) – onderdeel van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) – bevordert de bescherming van staatsgeheimen en andere vertrouwelijke informatie. Het NVB ondersteunt de rijksoverheid met kennis en expertise van technische maatregelen die zijn gericht op het beschermen van bijzondere informatie. Het NBV keurt en ontwikkelt daartoe beveiligingsproducten.

Dit onderzoek naar de risico's van onveilige USB-sticks is primair verricht voor netwerkbeheerders van rijksoverheidsorganisaties. Gezien het belang van de materie is besloten dit rapport voor een bredere doelgroep ter beschikking te stellen.

Voor meer informatie over het NBV zie:
https://www.aivd.nl/organisatie/eenheden-en/nationaal-bureau

1 Inleiding

Met regelmaat maken media melding van beveiligingsincidenten waarin USB-sticks centraal staan. Meldingen van verlies van USB-sticks met gevoelige gegevens zijn algemeen bekend. Minder bekend zijn incidenten waarbij gemanipuleerde USB-sticks zijn gebruikt om systemen te besmetten en gegevens te stelen. Naast het verlies van (gevoelige) informatie of infectie met schadelijke virussen kunnen dergelijke incidenten ook imagoschade tot gevolg hebben.

Gemanipuleerde USB-sticks versturen data naar internet
Het actualiteitenprogramma NOVA liet op tv zien wat er gebeurde toen ze (als test) tachtig geprepareerde USB-sticks 'vergaten' bij bekende organisaties.[1] Het bleek dat minstens twintig USB-sticks door medewerkers in een bedrijfscomputer werden gestoken, waarna automatisch gegevens naar het internet werden verstuurd. De NOVA-test was niet kwaadaardig, maar maakte wel het risico zichtbaar. Bij een soortgelijke test zijn 35 van de 54 'verloren' USB-sticks in met internet verbonden computers gestoken.[2] Een vergelijkbare test is voor het eerst in 2006 uitgevoerd en toen werden 15 van de 20 'geplante' USB-sticks door medewerkers in de bedrijfscomputer gestoken.[3]

Voor de komst van het internet waren floppydisks het belangrijkste medium voor verspreiding van virussen. Daarna werden e-mail en downloads de belangrijkste dragers. Door het massale gebruik van USB-sticks wordt dit medium steeds geliefder bij cybercriminelen en is extra aandacht voor beveiliging gewenst.

Dit rapport analyseert de risico's van USB-sticks en geeft verschillende technische oplossingen om de risico's te beperken. De beschreven maatregelen geven op zich geen 100 procent veiligheid en hebben pas effect als zij worden ingebed in een sluitend stelsel van organisatorische, procedurele en technische beveiligingsmaatregelen.

Dit onderwerp is ook aan de orde gekomen in het GOVCERT rapport: *Beveiliging van mobiele apparatuur en datadragers* dat in 2006 is gepubliceerd.[4] Dit rapport sluit aan op de aanbevelingen van GOVCERT en werkt ze in meer detail uit.

2 Dreigingen via mobiele gegevensdragers

USB-sticks en mobiele gegevensdragers zijn een bekende verspreidingsbron van schadelijke software. Deze software zal proberen om zichzelf te kopiëren naar alle mobiele gegevensdragers op een besmet systeem. Hierbij wordt ook geprobeerd om de mobiele gegevensdragers zodanig te wijzigen dat schadelijke software wordt geactiveerd als de gegevensdrager in een systeem wordt gestoken. Op deze wijze kan schadelijke software zich van organisatie naar organisatie verspreiden. Dit risico is aanwezig voor alle soorten mobiele gegevensdragers, dus niet alleen USB-sticks maar ook mobiele harde schijven, SD-kaarten, cd's en dvd's, floppydisks en zelfs MP3-spelers, camera's en digitale fotolijstjes.

Onderzoeken naar onveilige USB-sticks

Sinds 2008 is het aantal virusbesmettingen via gegevensdragers en het 'autorun'-mechanisme toegenomen.[5] Een significant deel van alle recente virusbesmettingen vindt op deze wijze plaats en enkele onderzoeken geven aan dat 'autorun' virussen gevaarlijker zijn voor bedrijven dan voor particuliere gebruikers.[6, 7, 8]

Het risico van USB-sticks met schadelijke software is extra groot omdat al jarenlang handleidingen voor het maken van vijandige USB-sticks[9, 10] en kant-en-klare hack-pakketten[11] te downloaden zijn. Het risico wordt nog groter als men bedenkt dat schadelijke software niet altijd wordt ontdekt door virusscanners.[12, 13]

Genante en kostbare incidenten

- Eind 2008 werd het gebruik van USB-sticks in het Amerikaanse leger verboden vanwege een uitbraak van een 'worm' die zich verspreidde via verwijderbare gegevensdragers.[14] Pas sinds kort mogen USB-sticks weer gebruikt worden, en dan alleen USB-sticks die formeel zijn getest en goedgekeurd[15].
- In mei 2009 werd de infrastructuur van de Engelse gemeente Ealing geïnfecteerd met een USB-stick. Het bestrijden van de infectie kostte 2 weken en 80.000 euro.[16]
- In juli 2009 werd een deel van het netwerk van de Raad voor de Rechtspraak enkele dagen afgekoppeld. Dit vanwege een virusinfectie die waarschijnlijk via een USB-stick is verspreid. [17, 18]

3 Dreigingen van 'autorun' en autoplay'

Het besmettingsrisico via onveilige USB-sticks wordt vergroot door de 'autorun' en 'autoplay' functionaliteit van Windows.

De zogenaamde U3-USB-sticks leveren de grootste risico's op. Een U3-stick doet zich voor als een combinatie van een cd-rom en een USB-stick. Op de cd-rom staat een 'autorun.inf' bestand waarmee automatisch de U3-menu's worden gestart (de 'launchpad') waar vandaan weer nieuwe programma's kunnen starten.[19] Een gebruiker hoeft een USB-stick alleen maar in de computer te stoppen en de schadelijke software wordt automatisch opgestart. Er is geen speciale handeling van de gebruiker nodig, zoals het openen van bestanden.[20] De geprepareerde USB-sticks van de NOVA-documentaire waren van het U3-type. Een aanval met dit type USB-stick is eenvoudig omdat alleen de 'launchpad' door schadelijke software hoeft te worden vervangen.

Zelfs als geen U3-stick wordt gebruikt en de 'autorun' functie is uitgeschakeld, is het risico van besmetting nog steeds aanwezig. De aanvaller kan een gebruiker proberen te verleiden om een schadelijk programma te starten door een bekend klinkende of aantrekkelijke naamgeving zoals 'salarisadministratie.xls' of 'leuk-computerspel.exe'. De aanvaller maakt dan gebruik van 'social engineering' en speelt in op de nieuwsgierigheid van de gebruiker. Deze dreigingen en bijbehorende risico's worden hieronder gedemonstreerd en toegelicht.

1 Malware start automatisch bij insteken van 'gewone' USB-stick of 'U3' USB-stick

Het programma start automatisch, zonder tussenkomst van de gebruiker. Dit betekent dat het systeem kwetsbaar is voor onveilige USB-sticks. Schadelijke programma's kunnen worden gestart zonder tussenkomst van de gebruiker. Dit is een onacceptabel groot risico.

2 Malware start bij dubbelklik op schijficoon in 'Mijn computer'

In het menu 'My computer' zijn de naam en icoon van de USB-stick aangepast. Als de gebruiker op de icoon van de USB-stick dubbelklikt, wordt het programma automatisch gestart en wordt niet – zoals te verwachten was – de inhoud van de USB-stick weergegeven.

Door 'aantrekkelijke' bijschriften en iconen te kiezen kan een gebruiker verleid worden om het programma vanaf de USB-stick op te starten. Iconen

en bijschriften kunnen zodanig gekozen worden dat een gebruiker verwacht een map te openen en niet een programma op te starten.

Het risico is groot, zeker als gebruik wordt gemaakt van bovengenoemde ‘social engineering’ technieken. Bekende virussen zoals ‘Conficker’ gebruikten deze methode voor hun verspreiding.

3 Malware start bij klik op eerste menukeuze in autoplay menu

Na het insteken van de USB-stick wordt het ‘autoplay’ menu getoond. Hierin wordt een aangepast programma-icoon en bijschrift getoond. Als de gebruiker op het icoon klikt wordt het programma automatisch gestart.

Het risico is groot, zeker als gebruik wordt gemaakt van bovengenoemde ‘social engineering’ technieken.

4 Malware start bij rechtsklik op eerste menukeuze in context menu

In ‘My computer’ is het menu aangepast dat getoond wordt bij een rechter muisklik. Er worden nieuwe opties aan het menu toegevoegd en hun functie wordt gewijzigd. Menuopties en bijschriften worden zodanig gewijzigd dat een gebruiker verwacht een map te openen en niet een programma op te starten.

Als de gebruiker de rechter muisklik gebruikt om de mogelijkheden van de USB-stick te bekijken wordt automatisch het malware programma gestart.

Het risico is groot, omdat van de doorsnee gebruiker niet verwacht kan worden dat hij een dergelijke aanval herkent.

4 Uitschakelen van 'autorun' en 'autoplay'

Het is mogelijk om de riskante 'autorun' en 'autoplay' functionaliteiten uit te schakelen en hierdoor het automatisch opstarten van schadelijke software te voorkomen. Op dit moment zijn twee oplossingen populair: één oplossing die door de Microsoft wordt geadviseerd en één oplossing die door verschillende beveiligingsorganisaties wordt aanbevolen.

In de tests door het NBV en in tests van verschillende beveiligingsorganisaties, bleken beide oplossingen nagenoeg even effectief te zijn. De keuze voor één van de twee zal vooral afhangen van het verwachte beheergemak. De eerste oplossing, die Microsoft aanbeveelt, maakt gebruik van Group Policies, waardoor deze oplossing via Active Directory uitgerold kan worden. De tweede oplossing maakt gebruik van een registry wijziging en de uitrol hiervan vraagt waarschijnlijk grotere inspanning.

Waarschuwing
De onderstaande wijzigingen moeten eerst in een representatieve testomgeving worden uitgeprobeerd voordat zij in een productieomgeving worden toegepast. Het uitschakelen van de 'autorun' en 'autoplay' functies versterkt de beveiliging maar kan het gebruikersgemak verlagen, doordat bijvoorbeeld applicaties niet meer automatisch van de USB-stick starten.

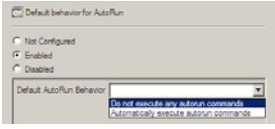
4.1 Uitschakelen functionaliteit met Group Policies

De maatregelen die Microsoft aanbeveelt werken alleen als een aantal specifieke updates op het systeem aanwezig zijn. Voor Windows Vista of Windows Server 2008 moet beveiligingsupdate 950582 zijn geïnstalleerd. Voor Windows XP, Windows Server 2003 of Windows 2000 moet beveiligingsupdate 967715 zijn geïnstalleerd.[21] Deze updates zijn door Microsoft eind 2008 en begin 2009 uitgebracht en zijn via Windows Update verspreid. Voor Windows 7 zijn geen aparte updates nodig.
Daarnaast heeft Microsoft in augustus 2009 update 971029 uitgebracht waarmee de 'autoplay' functie wordt uitgezet voor USB-sticks, maar niet voor optische media (CD-Rom / DVD).[22] Deze update wordt niet via Windows Update verspreid en moet handmatig worden geïnstalleerd.

Windows Vista, Windows Server 2008

- Zorg dat de vereiste updates aanwezig zijn.
- Start de editor voor Group Policies (gpedit.msc)

- Ga naar:
  Computerconfiguratie – Beheersjablonen – Windows onderdelen - Beleid voor automatisch afspelen (Turn off autoplay)
- Selecteer:
  Automatisch afspelen uitschakelen:Ingeschakeld
  Alle stations (All drives)



- Selecteer:
  Standaardgedrag voor Autorun: Ingeschakeld
  Geen Autorun-opdrachten uitvoeren (Do not execute any autorun commands)
- Herstart de computer

NB: In een centraal beheerde infrastructuur is het aan te bevelen deze policies via Active Directory uit te rollen.

Windows XP Pro, Windows Server 2003

- Start de editor voor Group Policies (gpedit.msc)

- Ga naar:
  Computerconfiguratie – Beheersjablonen –Systeem - Beleid voor automatisch afspelen (Turn off autoplay)
- Selecteer:
  Automatisch afspelen uitschakelen:Ingeschakeld
  Alle stations (All drives)
- Herstart de computer

4.2 Uitschakelen functionaliteit met een registry aanpassing

Enkele Windowsgebruikers hebben een effectieve manier ontdekt om de autorun en autoplay functies te blokkeren. Deze aanpak neutraliseert de risico's door Windows elk 'autorun.inf' bestand te laten negeren.[23] Hoewel deze oplossing neerkomt op een 'hack' die niet officieel door Microsoft wordt ondersteund, wordt deze oplossing wél door verschillende beveiligingsorganisaties aanbevolen als de meest effectieve oplossing.[24] De eenvoudigste manier om dit te doen is door de onderstaande instructies in een bestand met een '.reg' extensie op te slaan. Als dit bestand wordt uitgevoerd, wordt een wijziging in de Windows registry aangebracht.

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping\Autorun.inf]
@="@SYS:DoesNotExist"
```

5 Testen van het risico van USB-sticks

Het feitelijke risico van de 'autorun' en 'autoplay' functionaliteit van Windows wordt bepaald door de versie van het besturingssysteem, de geïnstalleerde service packs, updates en de aanwezige instellingen. De mogelijke combinaties en hun gevolgen zijn dan ook velerlei. Daarom is een test de beste manier om te bepalen welke risico's precies aanwezig zijn.

5.1 Test met standaard USB-stick

Een praktische en informatieve testaanpak wordt beschreven in een artikel in Computerworld.[25] Voor deze test wordt een test USB-stick gemaakt met daarop een 'autorun.inf' testbestand en een willekeurig uitvoerbaar programma (in dit geval een kopie van het Windows tekenprogramma 'mspaint.exe'). Het 'autorun.inf' testbestand krijgt de volgende inhoud.

```
[autorun]
action=Testing autoplay: Run paint from usbdrive
open=mspaint.exe
shell\FromFlash=Testing context: run paint from usbdrive
shell\FromFlash\command=mspaint.exe
shell=FromFlash
icon=mspaint.exe
label=Testing AutoRun
```

Als de USB-stick met deze bestanden in een Windows computer wordt gestoken kan worden nagegaan of de dreigingen uit paragraaf 3 aanwezig zijn.

5.2 Test met U3-USB-stick

Een test met een standaard U3-stick laat direct zien of risico's aanwezig zijn. Hiervoor is elke stick met U3-functionaliteit geschikt, speciale bestanden hoeven niet op de stick te worden gezet. Als het U3-menu automatisch start bij het insteken van de stick is het systeem kwetsbaar.

5.3 Voorbeelden van testresultaten

Als een USB-stick met schadelijke bestanden in een Windows computer wordt gestoken levert dit een aantal dreigingen op, zoals beschreven in paragraaf 3. Met de tests uit paragrafen 5.1 en 5.2 kan men eenvoudig nagaan of deze dreigingen op een systeem aanwezig zijn en of de in paragraaf 4 voorgestelde oplossingen correct werken. Voorbeelden van testresultaten vóór en na het aanbrengen van updates en beveiligingsinstellingen zijn hieronder gegeven. Deze resultaten gelden voor een 'out of the box' geïnstalleerd systeem waarvan de instellingen niet zijn gewijzigd en waarop geen verdere applicaties zijn geïnstalleerd. Bij uitvoering van de test op eigen systemen kunnen de resultaten afwijken.

Testresultaat voor systeem met alle automatisch geïnstalleerde Windows Updates, zonder extra beveiligingsmaatregelen

Type medium	Dreiging	Windows OS versie		
		Windows XP	Windows Vista	Windows 7
USB-stick SD-kaart (Alle niet-optische verwisselbare media)	1 Malware start automatisch bij insteken stick.	nee	nee	nee
	2 Malware start bij dubbelklik op schijf icoon in 'Mijn computer'.	ja	ja	nee
	3 Malware start bij klik op eerste menukeuze in autoplay menu.	ja	ja	nee
	4 Malware start bij rechtsklik op eerste menukeuze in context menu.	ja	ja	nee
CD-Rom / DVD (Alle optische verwisselbare media) Gesimuleerde CD-Rom van U3-stick	1 Malware start automatisch bij insteken stick.	ja	nee	nee
	2 Malware start bij dubbelklik op schijf icoon in 'Mijn computer'.	ja	ja	ja
	3 Malware start bij klik op eerste menukeuze in autoplay menu.	ja	ja	ja
	4 Malware start bij rechtsklik op eerste menukeuze in context menu.	ja	ja	ja

NB: Update 971029 van Microsoft schakelt de 'autoplay' functie uit voor USB-sticks, maar dat geldt niet voor optische media (CD-Rom / DVD). Na installatie van deze update reageren Windows XP en Windows Vista hetzelfde als Windows 7 (zie bovenstaande tabel). Het installeren van deze update verhoogt de beveiliging, ook zonder dat aanpassing van andere instellingen nodig is. Deze update wordt niet via Windows update verspreid en moet handmatig worden geïnstalleerd.

Testresultaat voor systeem beveiligd met Group Policies of registry aanpassing

Type medium	Dreiging	Windows OS versie		
		Windows XP	Windows Vista	Windows 7
USB-stick SD-kaart (Alle niet-optische verwisselbare media)	1 Malware start automatisch bij insteken stick.	nee	nee	nee
	2 Malware start bij dubbelklik op schijf icoon in 'Mijn computer'.	nee	nee	nee
	3 Malware start bij klik op eerste menukeuze in autoplay menu.	nee	nee	nee
	4 Malware start bij rechtsklik op eerste menukeuze in context menu.	nee	nee	nee
CD-Rom / DVD (Alle optische verwisselbare media) Gesimuleerde CD-Rom van U3-stick	1 Malware start automatisch bij insteken stick.	nee	nee	nee
	2 Malware start bij dubbelklik op schijf icoon in 'Mijn computer'.	nee	nee	nee
	3 Malware start bij klik op eerste menukeuze in autoplay menu.	nee	nee	nee
	4 Malware start bij rechtsklik op eerste menukeuze in context menu.	nee	nee	nee

NB: Als de Group Policy oplossing wordt gekozen, wordt de schijf icoon nog wél aangepast (dreiging 2), maar dubbelklikken start geen software meer op. Dit is mogelijk verwarrend voor de gebruiker, maar het levert geen beveiligingsproblemen op. Als de registry aanpassing wordt gekozen wordt ook het icoon niet meer aangepast.

6 Beveiliging met end-point security software

Een andere methode om de infrastructuur te beveiligen tegen ongewenste gevolgen van het gebruik van USB-sticks is om extra beveiligingssoftware op de werkstations te installeren. Bepaalde applicaties kunnen bijvoorbeeld het gebruik van randapparatuur en interfaces zoals USB-sticks of Wifi blokkeren. Andere applicaties blokkeren bijvoorbeeld het starten van programma's vanaf USB-sticks.
Deze functionaliteit is echter ook als onderdeel van integrale pakketten verkrijgbaar, die volledig geïntegreerd worden in de infrastructuur. Deze pakketten bevatten veel meer functionaliteit, zoals bijvoorbeeld anti-virus, anti-malware en firewallfuncties. Software met een dergelijke combinatie van functies wordt end-point security software genoemd. Voor meer informatie hierover kan onder andere verwezen worden naar het onderzoek van onderzoeksbureau Gartner[26] en andere publicaties.[27]

End-point security software kan dus beveiligen tegen verschillende soorten dreigingen. Een overzicht van de beveiligingsfunctionaliteit en hun effectiviteit tegen onveilige USB-sticks is in de volgende tabel weergegeven.

Beveiligingsfunctionaliteit	Effectief tegen onbetrouwbare USB-sticks
Blokkering en beveiliging van interfaces voor USB, Firewire, cd/dvd, floppydisks, parallelle poorten, infrarood interfaces, Wifi en Bluetooth	ja
Detectie, blokkering en verwijdering van 'malware' (virus, spyware, rootkit, Trojaans paard, worm)	ja: als de op de USB-stick gebruikte malware door de beveiligingssoftware herkend wordt
Alleen bekende en veilige applicaties opstarten ('whitelisting')	ja, hoewel dit extra beheerinspanning kan opleveren
Blokkering van 'verdacht gedrag' op het systeem (Host Based Intrusion Prevention System - HIPS)	ja, hoewel deze technologie pas sinds kort als 'volwassen' kan worden beschouwd
Filtering van netwerkverkeer door een 'personal firewall'	beperkt: als bij uitgaand netwerkverkeer wordt nagegaan of het van een 'vertrouwde' applicatie afkomstig is
Encryptie van harddisks en verwijderbare media	indirect
Blokkering van pogingen om gevoelige gegevens uit het systeem te exporteren (Data Loss Prevention - DLP)	indirect
Systeem wordt alleen op het bedrijfsnetwerk toegelaten als de beveiliging van het systeem afdoende is (Network Access Control - NAC)	indirect
Inventarisatie van aanwezige systemen en hierop aangesloten randapparatuur	indirect
Logging, monitoring en centrale rapportage over gebeurtenissen op de systemen en het aansluiten van randapparatuur	indirect
Gebruikers die op het internet surfen doen dit vanuit een geïsoleerde omgeving zodat onbetrouwbare websites geen aanvallen kunnen uitvoeren ('sandboxing')	nee

7 Beveiligingsmaatregelen in samenhang

Bij de keuze van beveiligingsmaatregelen is het goed om het principe van 'defense in depth' te gebruiken. Dit betekent dat elk risico door meerdere maatregelen moet worden beheerst, zodat de beveiliging in stand blijft als één maatregel faalt of uitvalt. In het geval van mobiele gegevensdragers levert dit een stelsel van maatregelen op dat bestaat uit:

- de gangbare standaard beveiligingsmaatregelen die in elke organisatie aanwezig dienen te zijn,
- aanvullende maatregelen specifiek voor de 'autorun' functie,
- indien nodig: inzet van specifieke hard- en software voor een extra hoog beveiligingsniveau.

7.1 Standaardmaatregelen

De volgende standaardmaatregelen verhogen het algemene beveiligingsniveau en verminderen tegelijk het risico van onbekende USB-sticks.

Standaardbeveiligingsmaatregelen		
	Maatregel	**Effect**
1	Stel een duidelijk informatie-beveiligingsbeleid op en kweek bewustzijn binnen de organisatie.	Elke medewerker kent de risico's van USB-sticks en steekt alleen 'vertrouwde' USB-sticks in zijn computer. Elke medewerker start alleen 'vertrouwde' software.
2	Installeer een goede virusscanner en houd deze 'up-to-date'.	Als bekende vijandige software op een USB-stick aanwezig is dan wordt deze verwijderd voordat hij kan worden uitgevoerd.
3	Zorg voor een goed werkend patchingmechanisme en zorg voor een veilige instelling van alle systemen (bijvoorbeeld door: 'hardening', beperking van toegangsrechten en beperking van het gebruik van 'administrator' accounts).	Vijandige software vindt minder 'zwakke plekken' om misbruik van te maken.

7.2 Beperking van de ‘autorun’ functionaliteit

De volgende maatregelen richten zich direct op het risico van onbekende USB-sticks en de achterliggende ‘autorun’ (en ‘autoplay’) functionaliteit.

Maatregelen tegen ‘autorun’ en ‘autoplay’		
	Maatregel	**Effect**
4	Test of de systemen kwetsbaar zijn voor vijandige USB-sticks. Zie paragraaf 5 voor enkele eenvoudige tests.	Als systemen kwetsbaar zijn dan wordt dit direct zichtbaar, zodat de noodzaak van beveiligingsmaatregelen goed onderbouwd kan worden.
5	Schakel de ‘autorun’ en ‘autoplay’ opties van Windows uit en test dit op alle typen systemen. Zie paragraaf 4 voor enkele mogelijke instellingen.	Als vijandige software op een USB-stick aanwezig is dan wordt deze automatisch gestart.

7.3 Overige maatregelen voor een extra hoog beveiligingsniveau

Daarnaast zijn voor een hoger en meer controleerbaar niveau van beveiliging de volgende maatregelen denkbaar.

Aanvullende maatregelen voor extra hoog beveiligingsniveau		
	Maatregel	**Effect**
6	Maak gebruik van systemen voor 'End Point Security en/of 'Host-based Intrusion Prevention Systems'.[28, 29] Zie paragraaf 6 voor een introductie tot deze systemen.	Dergelijke systemen verhogen de beveiliging van aanwezige computers doordat zij een of meer van de volgende beveiligingsmaatregelen voor hun rekening nemen: • blokkeren van software (.exe bestanden) op verwijderbare media; • blokkeren van 'verdacht gedrag' van software; • blokkeren van USB-poorten en CD- en dvd-spelers; • blokkeren van verdacht netwerkverkeer dat wijst op 'lekkage' van informatie.
7	Maak gebruik van versleutelde USB-sticks en zorg dat de aanwezige computers géén andere USB-sticks accepteren. Vanaf Windows Vista is dit ook mogelijk via Group Policies.	Dit zorgt er voor dat alleen veilige en geautoriseerde opslagmedia op de systemen kunnen worden aangesloten.
8	Zet de USB- (en eventueel CD/DVD-) functionaliteit volledig uit. Dit is mogelijk via registry-instellingen of Group Policies.	Vijandige software op gegevensdragers krijgt geen kans om systemen te besmetten.
9	Schakel de mogelijkheid uit om systemen op te starten vanaf een USB-stick of CD/DVD. Dit kan in de BIOS worden ingesteld.	Als een onbetrouwbare USB-stick aanwezig is terwijl het systeem wordt opgestart dan kan geen 'vijandig' operating system worden gestart en kan de normale toegangsbeveiliging niet worden omzeild.
10	Overweeg om systemen voor 'Data Loss Prevention' toe te passen.[29, 30]	Als een systeem besmet is met vijandige software wordt het risico van gevoelig dataverlies verder beperkt.

8 Samenvatting

Bedrijfssystemen kunnen met behulp van onveilige USB-sticks eenvoudig worden besmet en gegevens kunnen vervolgens worden gestolen. Het risico is het grootst voor Windows systemen waarop de 'autorun' en 'autoplay' functies standaard actief zijn. Bij dergelijke systemen is de dreiging aanwezig dat onbedoeld schadelijke software wordt gestart. Een USB-stick is een populair medium voor cybercriminelen, omdat het op eenvoudige wijze toegang verschaft tot systemen en netwerken:

- een nietsvermoedende gebruiker steekt een onveilige USB-stick in het systeem waarna schadelijke programma's direct en ongemerkt worden uitgevoerd, of
- een gebruiker wordt verleid schadelijke programma's van de stick te starten zonder dat hij zich hiervan bewust is.

Om deze specifieke dreiging weg te nemen adviseert het NBV om de 'autorun' en 'autoplay' functionaliteit uit te schakelen. Afhankelijk van de aanwezige infrastructuur en aanwezige beveiligingsapplicaties zijn hiervoor de volgende oplossingen mogelijk:

1. gebruik veilige registerinstellingen of group-policies voor Windows systemen
2. gebruik beveiligingsfuncties van reeds aanwezige beveiligingsprogrammatuur ('end point protection')
3. gebruik specifieke beveiligingsprogrammatuur gericht op mobiele gegevensdragers.

Het NBV heeft de eerstgenoemde oplossing getest en vastgesteld dat deze effectief is tegen het onbedoeld starten van schadelijke software. Dit rapport presenteert de oplossing van gebruik van veilige registerinstellingen of group-policies voor Windows systemen, inclusief de testresultaten. Verder wordt de effectiviteit van de oplossing 2 en 3 besproken.

9 Referenties

1 Belastingdienst doet 'dom' met USB-stick, 24-06-2009, Nova, Uitzending op Nederland 2
2 The Honey Stick Project, Measuring risk decisions, Scott Wright, www.streetwise-security-zone.com, 24 juli 2009
3 Social Engineering, the USB Way, Steve Stasiukonis, www.darkreading.com, 7 juni 2006
4 Beveiliging van mobiele apparatuur en datadragers, GOVCERT.NL, Versie 1.2, Den Haag, 31 juli 2006
5 Symantec Global Internet Security Threat Report, Trends for 2008, Volume XIV, p. 61, April 2009, Symantec enterprise security
6 McAfee Threats Report:, First Quarter 2009, p.13, McAfee Avert Labs, 2009 McAfee, Inc.
7 Microsoft Security Intelligence Report, Volume 6, July through December 2008, p. 21: Worms and Social Engineering, Win32/Autorun, Win32/Conficker, 2009, Microsoft Corporation.
8 Microsoft Security Intelligence Report, Volume 7, January through June 2009, p.64: Win32/Conficker, Win32/Hamweq, Win32/Taterf, Win32/Autorun, 2009, Microsoft Corporation
9 How to: Quick intro to hacking autorun for USB flash drives, www.usbhacks.com/2006/10/25
10 Hacking U3 USB drives Updates, www.mcgrewsecurity.com/pub/hackingu3/, 27 oktober 2006
11 USB Hacksaw, Hak.5, Episode 2x03, wiki.hak5.org, 14 september 2008
12 Measuring the in-the-wild effectiveness of Antivirus against Zeus, Trusteer, September 14, 2009
13 Average binary Antivirus detection rate, Zeus Tracker, zeustracker.abuse.ch
14 Under Worm Assault, Military Bans Disks, USB Drives, Noah Shachtman, 19 november 2008, Wired Magazine
15 SANS NewsBites, Volume: XI, Issue: 76, DOD to Lift USB Ban With Restrictions
16 Computer Virus Impact, Council, Business and Community Partnerships Scrutiny Panel, Ealing, 3 september 2009
17 Virus binnen Rechtspraak, Den Haag, 31 juli 2009, www.rechtspraak.nl
18 Netwerk Rechtspraak volledig hersteld, Den Haag, 4 augustus 2009, www.rechtspraak.nl
19 Island hopping: the infectious allure of vendor swag, Jesper M Johansson, Maart 2008, Microsoft TechNet Magazine
20 TR08-004 Disabling Autorun, 22 december 2008, Canadian Cyber Incident Response Centre

21 De Autorun-functionaliteit in Windows uitschakelen, support.microsoft.com, Artikel ID: 967715, 11 augustus 2009, versie 4.0
22 Update to the AutoPlay functionality in Windows, support.microsoft.com, Article ID: 971029, 25 augustus 2009, versie 1.1
23 The best way to disable Autorun for protection from infected USB flash drives, Michael Horowitz, 30 januari 2009, Computerworld Blogs
24 Microsoft Windows Does Not Disable AutoRun Properly, Technical Cyber Security Alert TA09-020A, US-CERT, 20 januari 2009
25 Test your defenses against malicious USB flash drives, Michael Horowitz, 24 januari 2009, Computerworld Blogs
26 Magic Quadrant for Endpoint Protection Platforms, Note G00166218, Gartner RAS Core Research, 28 mei 2009
27 Zware beveiligingspakketten voor het bedrijf, 26 februari 2009, Keith Schultz, techworld.nl/technologie
28 Secure USB Flash Drives, European Network and Information Security Agency (ENISA), juni 2008
29 Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines, versie 2.1, 10 augustus 2009, SANS
30 Magic Quadrant for Content Aware Data Loss Prevention, Gartner RAS Core Research, 22 juni 2009

Colofon

Deze brochure is een uitgave van:

Algemene Inlichtingen- en Veiligheidsdienst
www.aivd.nl

Postbus 20010 | 2500 EA Den Haag

December 2009