

German
Data
Security



G Data Whitepaper 2009

Systemveiligheid van Windows 7

Marc-Aurél Ester & Ralf Benz Müller
G Data Security Labs



Go safe. Go safer. G Data.



Inhoud

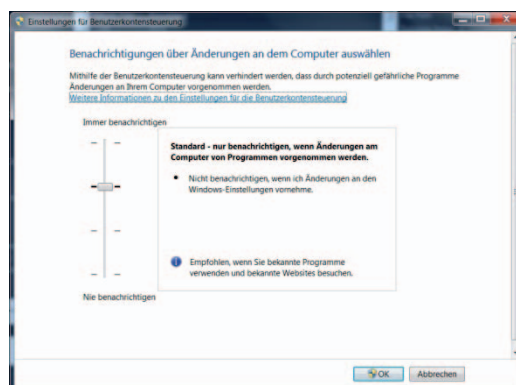
1. Windows 7 in de startblokken.....	2
2. Gebruikersaccountbeheer.....	2
3. Firewall	3
4. Bestandsextensieweergave	3
5. AppLocker	4
6. Windows Defender	4
7. Bitlocker	5
8. Bitlocker to go	5
9. Conclusie	6

1. Windows 7 in de startblokken

Windows 7 is de directe opvolger van Windows Vista, het besturingssysteem dat vooral door zakelijke klanten maar aarzelend werd overgenomen. Het marktaandeel van Windows Vista bedraagt ca. 30%, Windows XP heeft nog steeds een aandeel van 58%. Met Windows 7 probeert Microsoft veel punten van kritiek uit de weg te ruimen die bij de release van Windows Vista zowel bij thuisgebruikers als bij zakelijke klanten voor ontevredenheid en discussies zorgden. Zo heeft Windows 7 in vergelijking met Vista minder resources nodig. Bovendien zal er snel een speciale editie voor netbooks en soortgelijke apparatuur worden uitgebracht. Met Windows 7 wordt tevens de nieuwe grafische interface DirectX-11 geïntroduceerd. Het systeem werd ook voor het gebruik van Solide State Disks geoptimaliseerd. Dit leidt tot een kortere opstarttijd. Ook de bediening is gemoderniseerd. En last but not least zou Windows 7 veiliger zijn dan zijn voorgangers. Hieronder zullen de belangrijkste nieuwe functies en wijzigingen van Windows 7 met betrekking tot veiligheid worden toegelicht. Wij tonen u de effectiviteit van de veiligheidsmechanismen, laten zien waar nog ruimte voor verbetering bestaat en wat in vergelijking met Windows Vista minder goed is. Bovendien zullen we zien dat ook de nieuwste Windows-versie het gebruik van een krachtige antivirusoplossing noodzakelijk maakt.

2. Gebruikersaccountbeheer

Helaas zorgt veiligheid niet altijd voor gebruiksvriendelijkheid. Het beste bewijs hiervoor is het gebruikersaccountbeheer van Vista. Veel gebruikers klaagden erover dat de dialoogvensters van het gebruikersaccountbeheer te vaak het werkproces afremden. Daarom hebben veel gebruikers het probleem zelf opgelost edoor de irritante waarschuwingmeldingen resoluut uit te schakelen. Hierdoor wordt een effectief middel in de strijd tegen schadelijke programma's uitgeschakeld, omdat de malware zich automatisch de nodige rechten kan verschaffen voor de installatie.



Om dit tegen te gaan, is het in Windows 7 nu mogelijk om de weergave van de UAC-waarschuwingmeldingen op vier verschillende gevoeligheidsniveaus in te stellen.

1. Altijd melden als een programma of gebruiker het systeem wil wijzigen;
2. Alleen een melding weergeven wanneer een programma systeemwijzigingen probeert uit te voeren;
3. Alleen een melding weergeven wanneer een programma systeemwijzigingen probeert uit te voeren; Het bureaublad wordt in deze modus niet gedimd;
4. Geen meldingen weergeven.

Het is te verwachten dat veel gebruikers de eerste twee modi links laten liggen. Hierdoor wordt echter ook het beveiligingseffect verminderd.

Maar ook als UAC is ingeschakeld, kan malware in het systeem terechtkomen. Tijdens de betafase van Windows 7 was er al sprake van succesvolle aanvallen die het systeem infecteerden en UAC volledig uitschakelden.

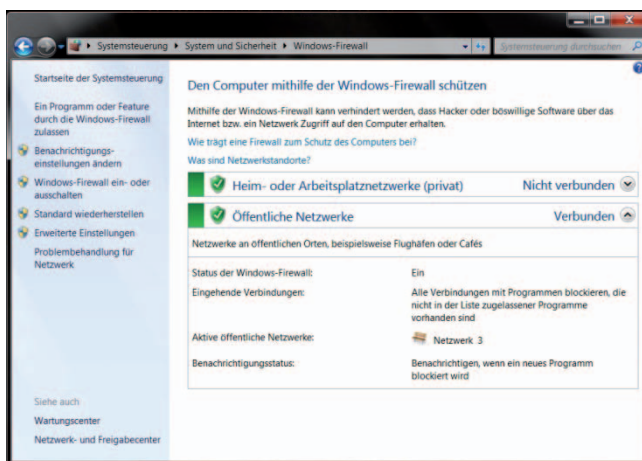
Ongecontroleerde taken

Ondanks de permanente bewaking bestaan er enkele automatische processen in Windows die buiten het gebruikersaccountbeheer vallen. Zo is het mogelijk om met de taakplanner programma's met beheerdersrechten te starten bij het opstarten van het systeem, zonder dat een melding voor de gebruiker verschijnt. Zo kan malware in een systeem terechtkomen.

Microsoft heeft met het nieuwe gebruikersaccountbeheer iets meer gebruiksvriendelijkheid ten koste van de veiligheid ingebouwd. De zwakkere instellingen maken het voor schadelijke programma's mogelijk om zich zonder waarschuwing op het systeem te nestelen. Dit halfslachtig ingevoerde gebruikersgemak gaat ten koste van de veiligheid. Op het gebied van het rechtenbeheer zou Microsoft zich moeten laten inspireren door de duidelijk effectievere en gebruiksvriendelijkere concepten uit de Unix- en Mac OS X-wereld.

3. Firewall

Microsoft heeft zich de kritiek over de Windows Firewall aangetrokken en in Windows 7 uitgebreid aan het gebruiksgemak gewerkt. Voor bepaalde toepassingen worden automatisch regels aangemaakt. Maar ook het beheer van de regelsets is dankzij de wizard voor regels eenvoudiger geworden. Hiermee kunnen nu zonder problemen nieuwe regelsets worden aangemaakt. Bovendien kan het gedrag van de Firewall in verschillende omgevingen worden geconfigureerd. Voor openbare WLANs kunnen bijvoorbeeld strengere regels worden gedefinieerd dan voor het bedrijfsnetwerk. Het is nu ook mogelijk om aan elke netwerkkaart verschillende profielen toe te wijzen.



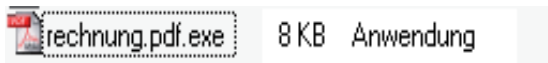
Hoe zinvol het gebruik van een Firewall ook is: slechts weinig gebruikers maken regelsets aan en onderhouden deze. Voor de meeste thuisgebruikers is dit te lastig en blijft het giswerk. Met één verkeerde klik kan men de toegang tot het internet blokkeren of de printer binnen het netwerk onbruikbaar maken. Het was en is geen goede oplossing om bij twijfel de beslissing bij de gebruiker te laten. Alleen een Firewall die zelf beslist welke gegevens mogen passeren, is echt nuttig. Deze functie wordt echter alleen door gespecialiseerde internetbeveiligingsproducten geboden.

De Firewall kan nog steeds volledig worden gedeactiveerd - ook door malware. Echte zelfverdediging, zoals de Firewalls van gangbare beveiligingsproducten, biedt de Windows Firewall niet. Hier werken commerciële producten duidelijk uitgebreider en effectiever.

4. Bestandsextensieweergave

Al sinds Windows 9x wordt steeds weer de omgang met de extensies van bestandsnamen bekritiseerd. Microsoft is nog steeds van mening dat een gebruiker de extensies aan het einde van een bestandsnaam bij bekende bestandstypen niet hoeft te zien. Van deze „feature“ maken online-oplichters al decennialang gebruik. Het werkt als volgt: In de standaardinstellingen worden bekende bestandsextensies zoals „.exe“, „.scr“ of ook „.doc“ verborgen. Alleen de bestandsnaam en het bijhorende pictogram worden weergegeven. Hierbij ontstaat het probleem dat aanvallers uitvoerbare bestanden van elk willekeurig pictogram kunnen voorzien. Als ze hun schadelijke programma's dus met het standaard

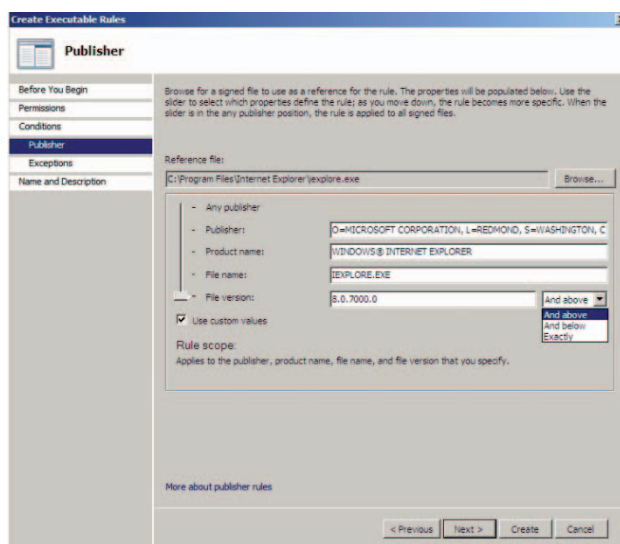
PDF-logo verspreiden, kan een gebruiker alleen met veel moeite nagaan of dit bestand daadwerkelijk van het weergegeven bestandstype is. Gebruikers die een dergelijk bestand bijvoorbeeld via e-mail ontvangen, kunnen op deze manier om de tuin worden geleid en denken dat ze het bestand zonder enig risico kunnen openen.



Wij vinden het volstrekt onbegrijpelijk dat Microsoft enerzijds bereid is om de gebruiker te kwellen met dialoogvensters die ze alleen bij uitzondering juist kunnen beantwoorden, en anderzijds de gebruiker niet helpt bij het opsporen van het meest effectieve schijnmanoeuvre uit de malwaregeschiedenis.

5. AppLocker

Met AppLocker kunnen beheerders bepalen welke toepassingen binnen het bedrijfsnetwerk mogen worden uitgevoerd. Dit was weliswaar al via Software Restriction Policies onder Windows XP en Windows Vista mogelijk, maar werd door de beheerders nauwelijks gebruikt. De reden hiervoor was het feit dat het beheer van deze regels al snel erg tijdrovend kan worden. Zo moet bijvoorbeeld bij elke update een nieuwe hash-waarde worden aangemaakt en ingevoerd. Met behulp van de Publisher Rules kan software nu permanent worden opgenomen, want hierbij gebeurt de identificatie met de digitale handtekening die tegenwoordig door de meeste toepassingen wordt gebruikt. Hierbij kan het volgende worden ingesteld: fabrikant, productnaam, bestandsnamen en versienummer. Aan de hand van deze criteria zijn natuurlijk ook blokkeringen mogelijk die het uitvoeren van bepaalde toepassingen voorkomen.



AppLocker kan een effectief wapen in de strijd tegen malware zijn. De Publisher-Rules maken het gebruik van dit middel gemakkelijker. Certificaten kunnen echter ook worden verwijderd en daarom is te verwachten dat de hierdoor gerealiseerde beveiliging slechts tijdelijk is.

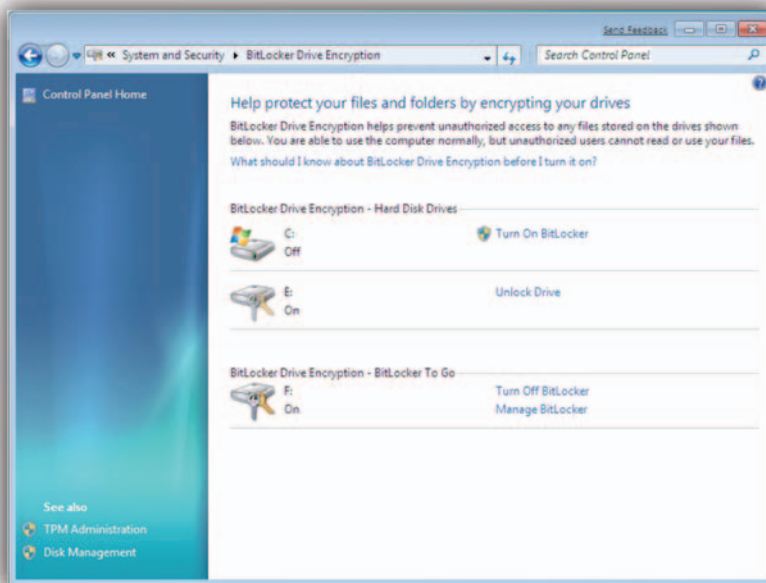
6. Windows Defender

De Windows Defender is sinds Windows Vista een vast bestanddeel. Het gaat hierbij om een scanner tegen spyware. In vergelijkende tests wist de Windows Defender echter niet te overtuigen. Zo werden in een enkele maanden oude vergelijkende test met andere virusbeveiligingsproducten slechts 20% van de geïnstalleerde schadelijke programma's herkend. Bij websites die probeerden spyware te installeren, scoorde men met 37,5% iets beter. Eén van de problemen is dat de Defender alleen een op hash gebaseerde herkenning gebruikt en geen eigen URL-filters.

Microsoft pretendeert niet met de Windows Defender een volwaardige virusbeveiliging te leveren. Hij moet bescherming bieden tegen de belangrijkste schadelijke programma's voor Windows en spyware. Onervaren Windows-gebruikers zouden echter kunnen denken dat Windows Defender een vervanging is van de virusbeveiliging en onterecht veronderstellen dat ze beschermd zijn. Windows Defender kan en mag een volwaardige virusbescherming echter niet vervangen.

7. Bitlocker

De codering van gevoelige gegevens wordt steeds belangrijker. Daarom heeft Microsoft met Vista de BitLocker-technologie geïntroduceerd. In vergelijking met Windows Vista heeft Microsoft een groot probleem van de BitLocker opgelost. Tot nu toe was het erg omslachtig om achteraf BitLocker te gebruiken. Hiervoor moest o.a. de systeempartitie worden verkleind. Later leverde Microsoft de "BitLocker Drive Preparation Tool" waardoor het hele proces werd vereenvoudigd. De coderingsfuncties voor de harde schijf van Bit-



Locker zijn nog steeds alleen voor de versies Ultimate en Enterprise verkrijgbaar. Momenteel maakt Windows 7 direct bij de installatie de 200 MB grote BitLocker-partitie aan, respectievelijk 400 MB als de "Windows Recovery Environment" is geïnstalleerd. BitLocker werkt samen met de in veel notebooks aanwezige TPM-chips. Bij desktop-pc's is deze hoofdzakelijk in zakelijke apparaten te vinden. Wanneer het apparaat niet over een TPM-chip beschikt, kan de noodzakelijke Encryption-Key op een USB-stick worden opgeslagen. Deze stick moet dan bij elk opstartproces op het apparaat worden aangesloten.

In vergelijking met het open source-alternatief "True Crypt" is dit omslachtig. BitLocker biedt echter de voor bedrijven interessante optie dat een algemene sleutel in de "Active Directory" kan worden opgeslagen. Wanneer een gebruiker bijvoorbeeld zijn wachtwoord vergeet of zijn USB-stick verliest, kan de beheerder de toegang tot de gegevens toch herstellen. Hoe hoog het hiermee gepaarde misbruikrisico is, is afhankelijk van de beveiliging van de Active Directory.

8. Bitlocker to go

BitLocker „voor onderweg“ is een nieuwigheid in Windows 7. Hiermee kunnen mobiele gegevensdragers, zoals USB-sticks en SD-kaarten, worden gecodeerd. De verificatie is via de invoer van een wachtwoord of via smartcard mogelijk. Ook hiervoor kan een algemene sleutel in de „Active Directory“ worden opgeslagen. Bovendien kunnen beheerders het gebruik van "BitLocker To Go" afdwingen zodra gegevens op mobiele apparaten voor gegevensopslag worden opgeslagen. Ook onder Windows XP en Vista is het mogelijk om met "BitLocker To Go" gecodeerde gegevens te lezen, maar dat is erg omslachtig. Hiervoor moeten de gegevens na invoer van het wachtwoord naar de harde schijf worden gekopieerd. Maar ook dan zijn de media niet beschrijfbaar. Veiligheidstechnisch is het niet erg handig om af te dwingen dat de gegevens naar een eventueel niet gecodeerde harde schijf worden gekopieerd.

9. Conclusie

Tot slot rijst natuurlijk de vraag hoeveel meer bescherming Windows 7 biedt. Is Windows nu zo veilig dat er geen beveiligingssoftware meer nodig is? Met Vista heeft Microsoft veel nieuwe beveiligingsfuncties in Windows geïntegreerd. De vernieuwingen zijn echter vooral cosmetisch en grotendeels op zakelijke klanten gericht. "BitLocker", "BitLocker To Go" en "AppLocker" zijn alleen opgenomen in de Ultimate- en Enterprise-versie en dus vooral voor gebruik in bedrijven bestemd. Voor thuisgebruikers heeft Microsoft geprobeerd de met Vista geïntroduceerde beveiligingstechnologieën bedienbaar te maken.

- Het gebruikersaccountbeheer is door verschillende niveaus kwetsbaarder geworden voor misbruik. Er wordt geen rekening gehouden met geplande taken.
- Nog steeds worden de bestandsextensies niet weergegeven. Oplichters kunnen hun schadelijke programma's dus nog steeds voorzien van pictogrammen van ongevaarlijke bestandstypen.
- Met Windows Defender wordt de gebruiker een bescherming voorgespiegeld die niet werkt.

Windows 7 heeft enkele beveiligingsfuncties gekregen. Er is echter geen sprake van een echte verdere ontwikkeling ten opzichte van Vista. Helaas kunnen veel beveiligingsfuncties worden omzeild en het is slechts een kwestie van tijd tot de malwarespecialisten de online-criminelen via underground-markten van aangepaste aanvalstechnieken voorzien. Beveiligingssoftware die computers efficiënt en effectief beveiligt en die bovendien gebruiksvriendelijk is, zal ook met Windows 7 nodig zijn om pc's tegen misbruik te beschermen.

Bijlage:

Beschikbaarheid van de beveiligingsmechanismen in de verschillende versies van Windows 7

Feature	Windows 7 Versie					
	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
EFS				●	●	●
Bitlocker					●	●
Bitlocker to go					●	●
UAC	●	●	●	●	●	●
Windows Defender	●	●	●	●	●	●
Windows Firewall	●	●	●	●	●	●
DEP	●	●	●	●	●	●