German
Data
Security

G Data Whitepaper 2009

Systemsicherheit von Windows 7

Marc-Aurél Ester & Ralf Benzmüller
G Data Security Labs

Geschützt. **Geschützter. G Data.**

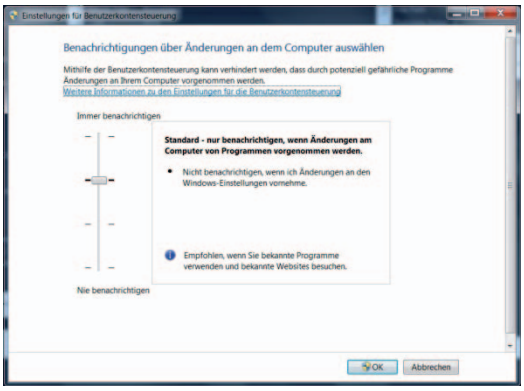
Inhalt

1. Windows 7 in den Startlöchern

Windows 7 ist der direkte Nachfolger von Windows Vista, das insbesondere bei Firmenkunden nur zögerlich angenommen wurde. Der Marktanteil von Windows Vista liegt bei ca. 30%, Windows XP hat immer noch einen Anteil von 58%. Mit Windows 7 versucht Microsoft viele Kritikpunkte zu beheben, die beim Release von Windows Vista sowohl bei Heimanwendern wie bei Firmenkunden für Unmut und Diskussionen sorgte. So verbraucht Windows 7 im Vergleich weniger Ressourcen als Vista, außerdem wird es bald eine spezielle Edition für Netbooks und ähnliche Geräte geben. Mit Windows 7 wird auch die neue Grafikschnittstelle DirectX-11 veröffentlicht. Das System wurde auch auf dem Umgang mit Solide State Disks optimiert, was eine verkürzte Startzeit zur Folge hat. Auch die Bedienung wurde modernisiert. Und last not least soll Windows 7 sicherer sein als seine Vorgänger. Nachfolgend werden die wichtigsten sicherheitsbezogenen Neuheiten und Änderungen an Windows 7 erläutert. Wir zeigen die Wirksamkeit der Schutzmechanismen, wo noch Nachbesserungsbedarf besteht und was sich im Vergleich zu Windows Vista verschlechtert hat. Außerdem werden wir sehen, dass auch die neueste Windows-Version den Einsatz einer leistungsfähigen Antivirenlösung ermöglicht.

2. Benutzerkontensteuerung

Leider ist Sicherheit nicht immer komfortabel. Der beste Beleg dafür ist die Benutzerkontensteuerung aus Vista. Von vielen Nutzern wurde bemängelt, dass die Abfragedialoge der Benutzerkontensteuerung zu oft den Arbeitsfluss bremsten. Daher haben viele Benutzer das Problem selbst in die Hand genommen und die nervigen Warnmeldungen kurzerhand abgeschaltet. Damit wird ein wirksames Mittel im Kampf gegen Schädlinge unwirksam, da die Malware sich die für die Installation notwendigen erhöhten Rechte automatisch besorgen kann.



Um dem entgegenzuwirken ist es in Windows 7 nun möglich, die Anzeige der UAC-Warnmeldungen in vier verschiedenen Stufen zu betreiben.

1. Immer melden, wenn ein Programm oder der Anwender das System verändern möchte;
2. Nur melden, wenn ein Programm Systemänderungen vornehmen will;
3. Nur melden, wenn ein Programm versucht, Systemänderungen vorzunehmen. Der Bildschirmhintergrund wird bei diesem Modus nicht abgedunkelt;
4. Keine Meldungen.

Dementsprechend ist es absehbar, dass viele Nutzer die ersten beiden Modi unter den Tisch fallen lassen. Dadurch wird aber auch die Schutzwirkung reduziert.

Aber auch wenn UAC eingeschaltet ist, kann sich Malware ins System schleichen.Während der Betaphase von Windows 7 gab es bereits erfolgreiche Angriffe, die zur Kompromitierung des Systems führten sund UAC gänzlich abgeschaltet wurde.

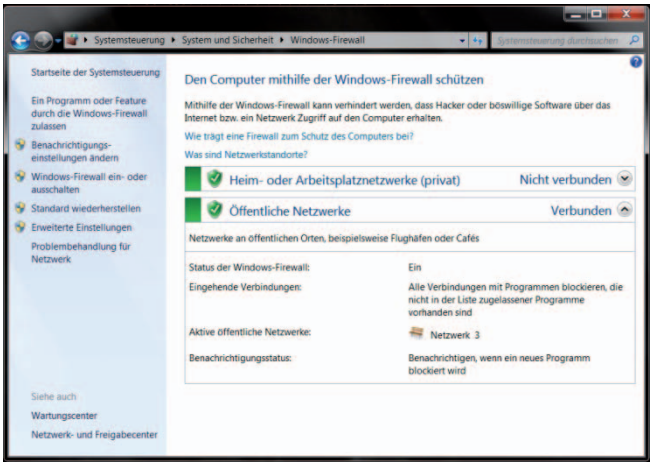
Ungeprüfte Aufgaben

Trotz der ständingen Überwachung gibt es einige Automatismen in Windows, die von der Benutzerkontensteuerung ausgelassen werden. So ist es möglich über die Aufgabenplanung Programme beim Systemstart mit Administratorrechten zu starten, ohne dass eine Abfrage beim Nutzer erscheint. So könnte sich Malware in ein System einnisten.

Microsoft hat mit der neuen Benutzerkontensteuerung ein wenig zusätzlichen Komfort auf Kosten der Sicherheit erkauft. Die schwächeren Einstellungen können es Schadprogrammen ungefragt erlauben, sich auf dem System breit zu machen. Diese halbherzig umgesetzte Bedienungserleichterungen gehen zu Lasten der Sicherheit. Im Bereich der Rechteverwaltung sollte Microsoft sich von den deutlich effektiveren und einfacher handhabbaren Konzepten der Unix- und Mac OS X -Welt inspiriren lassen.

3. Firewall

Microsoft hat sich die Kritik bezüglich der Windows Firewall zu Herzen genommen und in Windows 7 viel am Bedienkomfort der Firewall gearbeitet. Für bestimmte Anwendungen werden automatisch Regeln erstellt. Aber auch die Verwaltung der Regelsätze ist durch den Regel Assistenten einfacher worden. Mit diesem ist es nun problemlos möglich neue Regelsätze zu erstellen.Außerdem kann man das Verhalten der Firewall in verschiedenen Umgebungen konfigurieren, zum Beispiel lassen sich für öffentliche WLANS strengere Regeln definieren lassen als fürs Firmennetz. Es ist nun auch möglich jeder Netzwerkkarte unterschiedliche Profile zuzuordnen.



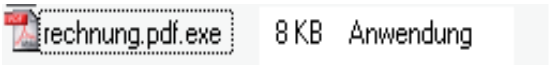
So sinnvoll der Einsatz einer Firewall auch ist, so wenig hat es sich bewährt den Nutzern den Aufbau und die Pflege der Regelsätze zu übertragen. Die meisten Heimanwender sind damit überfordert und können oft nur raten. Mit einem falschen Klick kann man sich vom Internet aussperren oder die Drucker im Netzwerk nicht mehr nutzen. Es war und ist keine gute Lösung im Zweifelsfall den Nutzer zu fragen. Wirklich hilfreich ist hier nur eine Firewall, die selbst entscheidet, welche Daten passieren dürfen. Diese Funktion bieten nur spezialisierte Internet Security Produkte.

Nach wie vor ist es möglich die Firewall komplett zu deaktivieren - auch von Malware. Einen Selbstschutz wie die Firewalls in gängigen Security-Produkten bietet die Windows Firewall nicht. Hier sind kommerzielle Produkte deutlich umfassender und effektiver.

4. Dateinamenerweiterungen

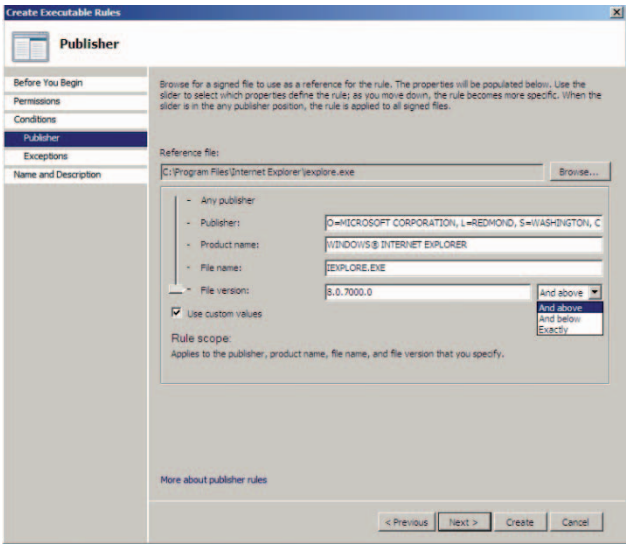
Schon seit Windows 9x wird immer wieder der Umgang mit den Erweiterungen der Dateinamen bemängelt. Microsoft ist nach wie vor der Meinung, dass ein Nutzer die Kürzel am Ende eines Dateinamens bei bekannten Dateitypen nicht sehen muss. Dieses „Feature“ machen sich Online-Betrüger schon seit Jahrzehnten zunutze. Das funktioniert so: Mit den Standardeinstellungen werden bekannte Dateinamenerweiterungen wie zum Beispiel „.exe“, „.scr“ oder auch „.doc“ ausgeblendet. Es wird nur der Dateiname und das dazu passende Icon angezeigt. Hierbei ergibt sich das Problem, dass ein Angreifer ausführbare Dateien mit jedem Icon seiner Wahl versehen kann. Wenn er sein Schadprogramm also mit dem Standard PDF Logo verbreitet, kann ein Nutzer nur mit viel Aufwand entscheiden, ob es

sich bei dieser Datei wirklich um den angezeigten Dateityp handelt. Anwender, die eine solche Datei z.B. per E-Mail erhalten, kann so getäuscht werden und glauben, dass er die Datei ohne Risiko öffnen kann.



Aus unserer Sicht ist es absolut unverständlich, dass Microsoft auf der einen Seite bereit ist die Nutzer mit Dialogen zu quälen, deren Fragen sie nur in Ausnahmefällen richtig beantworten können, auf der anderen Seite aber den Nutzer beim Aufspüren des effektivsten Täuschungsmanövers der Malwaregeschichte weiterhin nicht unterstützt. Beispiel: 2 -3 Sätze

5. AppLocker



Mit AppLocker können Administratoren kontrollieren, welche Applikationen im Unternehmensnetz ausgeführt werden dürfen. Dies war zwar schon mit Software Restriction Policies unter Windows XP und Windows Vista möglich, jedoch traf diese Funktion bei den Administratoren auf geringe Akzeptanz. Dies rührte daher das die Pflege dieser Regeln sehr schnell sehr zeitintensiv werden kann. So muss zum Beispiel bei jedem Update ein neuer Hashwert erzeugt und eingepflegt werden. Mit Hilfe der Publisher Rules ist es nun möglich Software permanent einzubinden, denn hierbei erfolgt die Identifikation über die digitale Signatur welche derweilen von den meisten Anwendungen genutzt wird. Einstellbar sind hierbei: Hersteller, Produktname, Dateinamen und Versionsnummer. Anhand dieser Kriterien sind natürlich auch Sperrungen die das Ausführen bestimmter Anwendungen verhindert möglich.

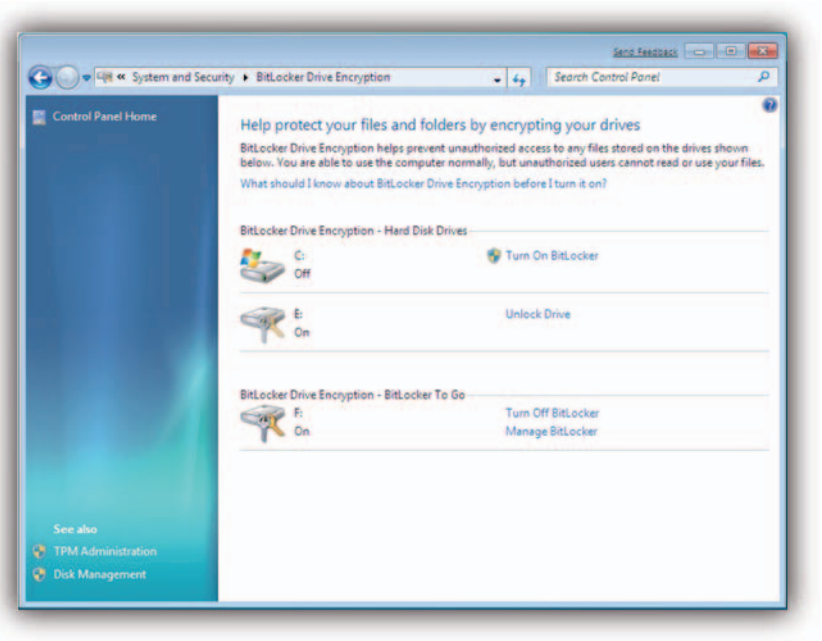
AppLocker kann eine wirkungsvolle Waffe im Kampf gegen Malware sein. Die Publisher-Rules erleichtern es dieses Mittel einzusetzen. Allerdings lassen sich auch Zertifikate aushebeln und es ist zu befürchten, dass die dadurch erzielte Schutzwirkung nur temporär ists.

6. Windows Defender

Der Windows Defender seit Windows Vista fester Bestandteil. Hierbei handelt es ich um einen Anti-Spyware Scanner. In Vergleichstest weiß der Windows Defender jedoch nicht zu überzeugen. So wurden in einem wenige Monate alten Vergleichstest mit anderen Virenschutz Produkten lediglich 20% der installierten Schädlinge erkannt. Bei Websites, die versuchten Spyware zu installieren, kam man auf eine geringfügig bessere Quote von 37,5%. Einer der Probleme ist das der Defender nur eine Hash basierte Erkennung nutzt und keine eigenen URL Filter.

Der Windows Defender ist von Microsoft nicht als vollwertiger Virenschutz vorgesehen. Er soll vor den wichtigsten Windows-Schädlingen und Spyware. Unbedarfte Windows-Nutzer könnten Windows Defender für einen Ersatz des Virenschutzes halten und sich völlig zu Unrecht in Sicherheit wägen. Einen vollwertigen Virenschutz kann und soll Windows Defender aber nicht ersetzen.

7. Bitlocker



Die Verschlüsselung von brisanten Daten wird immer wichtiger. Daher hat Microsoft mit Vista die Bitlocker-Technologie eingeführt. Im Vergleich zu Windows Vista hat Microsoft ein großes Problem des BitLockers ausgeräumt. So war es bisher nur mit großem Aufwand möglich nachträglich BitLocker zu nutzen, so musste u.a. die Systempartition verkleinert werden. Später liefert Microsoft das „BitLocker Drive Preparation Tool“ nach, welches die ganze Prozedur vereinfachte. Nach wie vor sind die Verschlüsselungsfunktionen für die Festplatte von BitLocker nur für die Ultimate und Enterprise Versionen erhältlich. Aktuell legt Windows 7 direkt bei der Installation die 200MB große BitLocker Partition an beziehungsweise 400MB wenn das „Windows Recovery Environment“ installiert wurde. BitLocker arbeitet mit den in vielen Notebooks anzutreffenden TPM Chips zusammen. Bei Desktop Computern findet man sich hauptsächlich in Business Geräten. Falls das Gerät über keinen TPM Chip verfügt, so besteht die Möglichkeit den notwendigen Encryption-Key auf einen USB Stick zu speichern, den man dann immer bei dem Startvorgang einstecken muss.

Im Vergleich zur Open Source Alternative „True Crypt“ ist dies umständlich. Jedoch bietet BitLocker die gerade für Firmen interessante Option, dass ein Generalschlüssel im „Active Directory“ hinterlegt werden kann. Sollte es dazu kommen, dass ein Anwender sein Passwort vergisst oder seinen USB-Stick verliert, so ist der Administrator in der Lage den Zugang zu den Daten wieder herzustellen. Wie hoch das damit verbundene Missbrauchspotenzial ist, hängt von der Absicherung des Active Directory ab.

8. Bitlocker to go

Bitlocker „zum Mitnehmen“ ist eine Neuerung in Windows 7. Damit ist es möglich mobile Datenträger wie USB-Sticks und SD-Karten zu verschlüsseln. Die Authentifizierung ist über Eingabe eines Passworts oder via Smartcard möglich. Auch hier ist es möglich einen Generalschlüssel im „Active Directory“ zu hinterlegen. Desweiteren ist es für Administratoren möglich das Nutzen von „Bitlocker to go“ zu erzwingen sobald Daten auf mobilen Datenspeichern abgelegt werden. Es ist auch unter Windows XP und Vista möglich mit „Bitlocker to go“ verschlüsselte Daten zu lesen, jedoch ist dies aufwändig. Dazu müssen die Daten nach Eingabe des Passworts auf die Festplatte kopiert werden. Aber auch dann sind die Medien nicht beschreibbar. Sicherheitstechnisch ist es nicht gerade glücklich, es zu erzwingen, dass die Daten auf eine ggf. nicht verschlüsselte Festplatte kopiert werden.

9. Fazit

Abschließend stellt sich natürlich die Frage wieviel Sicherheit in Windows 7 gewonnen wurde. Ist Windows jetzt so sicher, dass man keine Security-Software mehr braucht? Mit Vista hat Microsoft viele neue Schutzfunktionen in Windows integriert. Die Neuerungen sind vielfach kosmetischer Natur und größtenteils auf Firmenkunden ausgerichtet. „BitLocker“„BitLocker to go“ und „AppLocker“ sind nur in der Ultimate und Enterprise Version enthalten und damit vorwiegend für den Einsatz im Unternehmen vorgesehen. Für Heimanwender hat Microsoft versucht die mit Vista etablierten Schutztechnologien bedienbar zu machen.

- Die Benutzerkontensteuerung ist durch die verschiedenen Stufen anfälliger für Missbrauch geworden. Geplante Aufgaben werden nicht einbezogen.
- Noch immer werden die Dateinamenerweiterungen nicht angezeigt. Betrüger können also weiterhin ihre Schadprogramme mit den Icons von harmlosen Dateien tarnen.
- Mit Windows Defender wird dem Nutzer ein Schutz vorgegaukelt, der nicht wirkt.

Windows 7 hat zwar einige Schutzfunktionen bekommen. Eine wirkliche Weiterentwicklung gegenüber Vista hat allerdings nicht stattgefunden. Leider lassen sich viele Schutzfunktionen umgehen und es ist nur eine Frage der Zeit, bis die Malware-Spezialisten über Untergrundmärkte Online-Kriminelle mit angepassten Angriffstechniken versorgen. Security-Software, die Rechner effizient und wirkungsvoll schützt und darüber hinaus auch noch einfach zu bedienen ist, wird auch in Zukunft notwendig sein, um Windows-Rechner vor Missbrauch zu schützen.

Anhang:

Verfügbarkeit der Schutzmechanismen in den unterschiedlichen Versionen von Windows 7

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