Windows Vista Sicherheit

Werner Illsinger

Schutz vor Malware

Unter Malware – einer Zusammensetzung aus **mal**icious (boshaft) und Soft**ware** bezeichnet man Computerprogramme die vom Anwender unerwünschte Funktionen ausführen. In diese Kategorie fallen sowohl Computerviren als auch Würmer, Viren, Spyware (die ohne Erlaubnis Informationen über den Anwender sammelt) und andere ähnliche Programme.

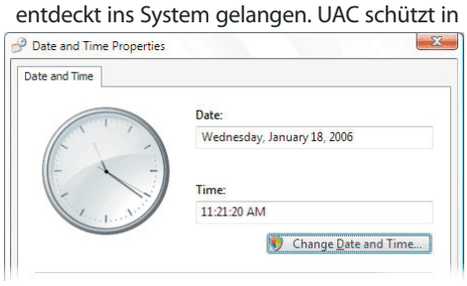
Neben den im Internet Explorer 7 vorhandenen Schutzmechanismen beinhaltet auch Windows Vista selbst einige neue Funktionen um das System sicherer gegen Malware zu machen.

User Account Control / Benutzerkontensteuerung (UAC)

Windows Vista trennt damit Aufgaben die ein normaler Benutzer durchführen soll und solche die nur vom Administrator ausgeführt werden können. In Windows XP und früher mussten für viele Funktionalitäten Administratorrechte verwendet werden. So konnte z.B. früher die Uhrzeit im Windows nur mit Administratorrechten verstellt werden – das ist auch gut so – jedoch musste man auch für die Konfiguration der Zeitzone Administrator sein. Das ist im Zeitalter der mobilen Geräte nicht mehr einzusehen. Des weiteren kann unter Windows Vista auch ein normaler Anwender vom Administrator freigegebene Gerätetreiber installieren (zum Beispiel Druckertreiber von einem bestimmten Hersteller). Damit sollte in Zukunft wesentlich seltener Administratorfunktionalität notwendig sein.

Zusätzlich kann der Administrator wenn die *User Account Control* aktiviert ist nicht mehr unbemerkt Administratorfunktionen aufrufen. Wenn ein Benutzer als Administrator angemeldet ist, versucht administrative Tätigkeiten auszuführen, dann rückt der Desktop in den Hintergrund und wird abgedunkelt. Es erscheint ein Eingabefenster bei dem der Benutzer diesen administrativen Eingriff ins System bestätigen muss. Zusätzlich sind alle Funktionalitäten die administrative Rechte erfordern mit dem bekannten Schild-Symbol gekennzeichnet. Damit weiß der Benutzer schon im Vorfeld, dass er für diesen Zugriff administrative Rechte benötigen wird.

Wie seit langem bekannt, sollten Benutzer nur mit „normalen" Benutzerkonten am System angemeldet sein. Windows hat das den Benutzern früher nicht leicht gemacht, da für viele Funktionalitäten Administrationsrechte notwendig waren. Aus diesem Grund arbeiteten viele Benutzer standardmäßig mit Administratorrechten. Malware kann damit sehr leicht unentdeckt ins System gelangen. UAC schützt in Windows Vista auch davor – denn wenn eine Komponente Administrationsrechte benötigt, wird der Administrator nochmals extra darauf hingewiesen und er muss diese Aktion gesondert bestätigen.



Windows Defender

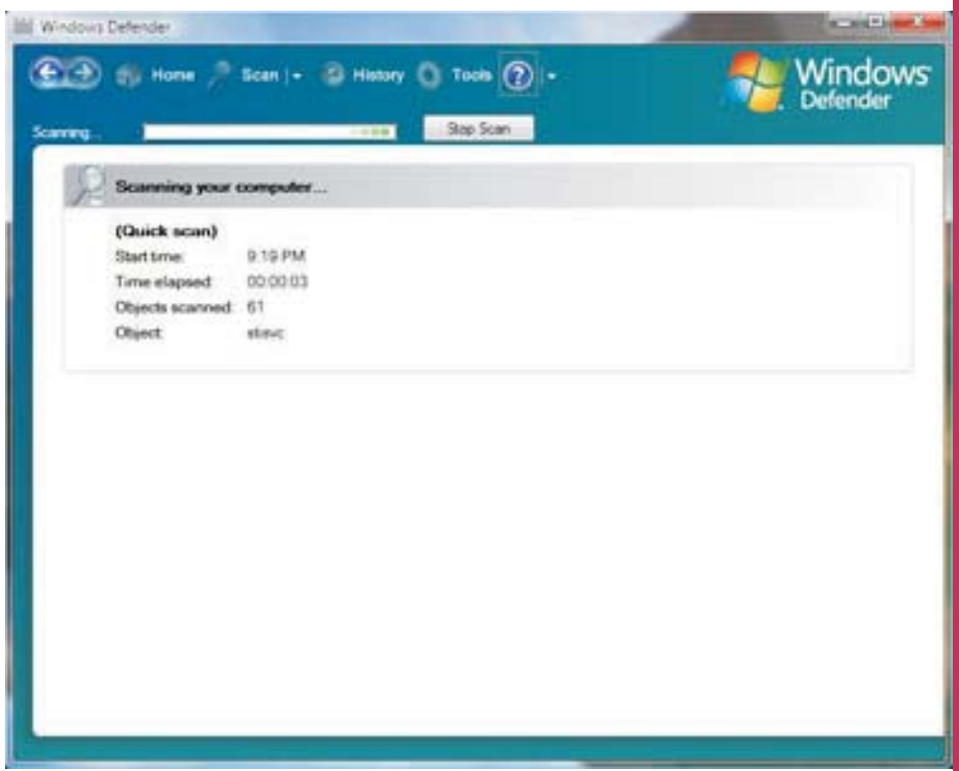
Windows Defender ist ein Programm zur Bekämpfung von Malware wie Popupfenster, Spyware und anderen unerwünschten Programmen. Windows Defender überwacht in Echtzeit das Betriebssystem und Punkte wie Autostart oder Registry, in dem sich Malware-Komponenten bevorzugt einnisten. Wenn ein Zugriff verdächtiger erfolgt, wird der Anwender darauf hingewiesen. Es wird empfohlen diesen abzulehnen. Falls der Zugriff erwünscht ist, kann der Anwender ihn aber auch genehmigen.

Die Einstellungen von Windows Defender können in Unternehmensnetzwerken zentral über Gruppenrichtlinien gesteuert werden.

Windows Defender ist als Schutz gegen Malware empfohlen – ist aber kein Antivirenprogramm. Um einen umfassenden Schutz zu gewährleisten ist zusätzlich der Einsatz eines aktuellen Antiverenprogrammes unumgänglich erforderlich.

Das Programm benötigt ähnlich wie Virenscanner aktuelle Signaturen die bequem über Microsoft Update verteilt werden. Defender macht sich nach der Installation im Normalfall nur durch ein Icon in der Taskleiste bemerkbar.

Defender ist standardmäßig in Windows Vista enthalten, kann aber gratis auch für Windows XP unter `http://www.microsoft.com/defender/` nachinstalliert werden.



Windows Firewall

Seit Windows XP Servicepack 2 beinhaltet das Betriebssystem eine personal Firewall – d.h. eine Firewall die am Client installiert ist und das System schützt. Eine Firewall ist en wesentlicher Bestandteil des Schutzes eines Systems – neben dem Einspielen der aktuellen Sicherheitsupdates sowie eines aktuellen Virenscanners und Malware-Erkennung. Es schützt das System vor Angriffen von außen, auch wenn es grundsätzlich für diese Angriffe verwundbar wäre.

Die Vista Firewall filtert nicht nur eingehende Datenverbindungen – sondern auch ausgehende Verbindungen. Die Firewall ist in die Funktionen zur automatischen Netzwerkerkennung von Vista integriert – so dass auch standortspezifische Vorgaben (zum Beispiel im Büro, zu Hause und unterwegs) getroffen werden können. Man kann daher das System zum Beispiel bei Nutzung des öffentlichen Internets über Hotspot strikter schützen, als man das etwa im Büro machen würde.

Alle Einstellungen der Firewall können im Unternehmensnetzwerk wieder zentral über Gruppenrichtlinien gesteuert werden.

Automatische Updates

Automatische Updates sind ebenfalls ein alter Bekannter. Über automatische Updates kann ein Benutzer angeben, wann der Rechner sich die aktuellsten Sicherheitsupdates für das System aus dem Internet laden soll. Diese Funktion ist besonders sinnvoll, wenn man über eine Breitband-Internetverbindung verfügt und sich das System jede Nacht automatisch mit den aktuellsten Updates versorgt.

In einem Unternehmensnetzwerk kann man selbst seinen Update Server betreiben (WSUS

Windows Software Update Services). Dazu wird eine Serverkomponente installiert, die sich automatisch mit dem Microsoft Update Server verbindet und die aktuellsten Sicherheitsupdates einmal ins Unternehmen repliziert. Die Client Stationen laden dann ihre Updates nicht mehr aus dem Internet, sondern innerhalb des Unternehmens vom eigenen Update Server. Dies hat mehrere Vorteile: Man schont natürlich Bandbreite – zusätzlich kann der Administrator die Updates auch testen, bevor er sie hausintern zur Verteilung freigibt.

Windows Sicherheitscenter (WSC)

Das Sicherheitscenter prüft im Hintergrund den Status der wichtigsten Sicherheitsfunktionen von Windows Vista:

- Firewall
- Windows Defender
- Automatische Updates
- Virenscanner
- Weitere Sicherheitseinstellungen (UAC, Internet Explorer)

Zusätzlich zu den in Vista integrierten Funktionalitäten kann das Sicherheitscenter auch Sicherheitssoftware von bestimmten Drittherstellern überwachen (etwa Firewalls oder Virenscanner). Im Sicherheitscenter ist auf den ersten Blich zu erkennen, welche Komponenten installiert sind, bzw. auch auf dem neuesten Stand sind. Es gibt Ratschläge über zu aktivierende Komponenten. Sollte ein Abonnement für z.B. einen Virenscanner abgelaufen sind, stellt das Sicherheitscenter auch entsprechende Links zur Verlängerung der Funktionen auch zu Drittherstellern bereit.

Das gesamte Sicherheitscenter kann in Unternehmensnetzwerken wiederum zentral über Gruppenrichtlinien konfiguriert werden.

Internet Explorer 7 (IE7)

Neben den Funktionalitäten, die auch beim IE7 für Windows XP zur Verfügung stehen, bietet der IE7 unter Windows Vista eine zusätzliche Funktionalität – den geschützten Modus.

Der geschützte Modus für den IE7 beschränkt den Zugriff aus dem IE auf bestimmten Prozesse, Dateien und Systemressourcen. Im geschützten Modus wird der IE mit sehr eingeschränkten Rechten ausgeführt. Der IE kann ohne Zustimmung des Benutzers keine Einstellungen, Benutzerdateien oder Systemdateien verändern – sondern sich nur innerhalb der „temporären Internetdateien" bewegen. Standardmäßig ist der geschützte Modus unter Vista für alle Zonen außer den vertrauenswürdigen Sites aktiviert. Diese Einstellungen können wieder für Unternehmensnetzwerke zentral über Gruppenrichtlinien vorgegeben werden.

Datensicherheit

Bitlocker Drive Encryption

Die Bitlocker Laufwerksverschlüsselung verschlüsselt das gesamte Systemvolume des Betriebssystems, sodass nicht autorisierte Benutzer nicht darauf zugreifen können. Auch mit bekannten Methoden – z.B. die Festplatte in ein anderes System als zweite Platte einzubauen etc. kann hier nichts erreicht werden. Um größtmöglichen Schutz zu erzielen wird dazu ein im Computer vorhandener Chip (das *Trusted Platform Module* – TPM 1.2) verwendet. Der TPM-Chip überprüft beim Starten die Hardwareintegrität des Computers. Falls erkannt wird, dass Dateien auf der Platte manipuliert wurden, verweigert der Computer den Startvorgang. Zusätzlich wird der Schlüssel, mit dem die Platte verschlüsselt ist, sicher im TPM Modul abgelegt. Sollte der Computer über keinen TPM Chip verfügen, so kann der Schlüssel auch auf z.B. einem USB-Stick abgelegt werden. Die Überprüfung der Systemintegrität entfällt dann aber.

Bitlocker ist in der **Ulitmate Edition** von Windows und in der über Volumslizenzprogramme verfügbaren **Enterprise Edition** enthalten.

Bitlocker schützt vor allem dagegen, dass bei verlorenen oder gestohlenen Computern auch die Daten in die Hände der Diebe fallen. Es ersetzt jedoch nicht das *Encrypted Files System* (EFS), das schon aus Windows 2000 bekannt ist. EFS schützt auch die Daten von Benutzern die sich am System berechtigterweise anmelden.

Encrypted File System

Das *Encrypted File System* (Verschlüsseltes Dateisystem) oder kurz EFS ist seit Windows 2000 bekannt und auch in Windows XP enthalten. Das EFS ist in das Dateisystem integriert und schützt Daten vor unbefugtem Zugriff. Versucht ein berechtigter Benutzer auf eine Datei zuzugreifen, so wird im Hintergrund der Schlüssel dazu abgefragt, die Datei entschlüsselt und an die Applikation weitergegeben. Die betreffende Applikation bemerkt von diesem Vorgang nichts, und muss daher auch EFS nicht gesondert unterstützen. Windows Vista erweitert das System um folgende zusätzliche Funktionalitäten:

- Die Benutzerschlüssel können auf Smartcards gespeichert werden.
- Wiederherstellungsschlüssel können auf Smartcards gespeichert werden
- Die Auslagerungsdatei kann mit EFS verschlüsselt werden. Datei wird der Schlüssel beim Start des Systems erzeugt und beim Herunterfahren wieder vernichtet.
- Der Offlinedateicache kann mit EFS verschlüsselt werden – damit können gecachte Dokumente nur vom Benutzer gelesen werden, der den Cache angelegt hat.
- Es gibt zahlreiche neue Gruppenrichtlinien, um die Funktionalität von EFS besser steuern zu können.

Weiterführende Literatur

Microsoft Technet: Sicherheit und Datenschutz unter Windows Vista:

http://www.microsoft.com/germany/technet/prodtechnol/windowsvista/secprot/default.mspx

Grafik: Wikipedia