Vista / Windows Server 2008

Was bringen die neuen Betriebssysteme?

Vista ist nun bereits ein Jahr auf dem Markt. Gemäss Aussage von Microsoft wurden bereits über 150 Millionen Exemplare davon verkauft. Grund genug, sich auch mit den Sicherheitsaspekten dieses Betriebssystems auseinander zu setzen.

Autor: Andreas Wisler

Folgende Funktionen wurden stark erweitert oder sind neu:

- Firewall (WFAS)
- Windows Defender
- Internet Explorer 7 mit Anti-Spyware und Zonenmodell
- Jugendschutz
- Bitlocker Festplattenverschlüsselung
- Service Hardening
- UAC – User Account Control
- Steuerung der Peripheriegeräte via GPO
- NAP – Network Access Protection

Hinweis: Praktisch zu allen Themen finden Sie auf der Homepage von Microsoft weiterführende Informationen.

Firewall

Abbildung 1

Microsoft hatte schon Windows XP eine einfache, aber effektive Firewall mit auf den Weg gegeben, die eingehende Netzwerkverbindungen blockieren kann. Die Vista-Firewall lässt sich detaillierter und trotzdem bequemer konfigurieren, indem sie die Regeln an die Netzwerkumgebung anpasst. Im Gegensatz zu Windows XP kann die Vista Firewall nun auch ausgehenden Traffic „steuern". Dabei sieht die Konfigurationsoberfläche noch immer identisch aus.

Die Vista-Firewall, von Microsoft als „Windows Firewall mit erweiterter Sicherheit" getauft, basiert auf der Programmierschnittstelle Windows Filtering Platform. Diese soll Programmierern die Überwachung und Kontrolle des Netzwerkverkehrs auf verschiedenen Ebenen erleichtern.

Eine der Verbesserungen, die jedem Anwender zugute kommt, ist die automatische Anpassung der Firewall an das aktuelle Netzwerk: Vista beobachtet im Hintergrund die Hardware-Adresse des Internet-Gateways und speichert diese Zuordnung zu einem Standort-Profil ab. Wird das Gerät an einem anderen Netz angeschlossen, schaltet Vista erstmal auf das öffentliche Standort-Profil um, in dem im Auslieferungszustand alle Ports geschlossen sind. Anschliessend fragt Windows nach, ob es sich bei dem neuen Netzwerk um ein öffentliches oder privates handelt.

Die in der Systemsteuerung sichtbare Oberfläche der Vista-Firewall ist dabei genauso einfach gehalten wie die unter Windows XP SP2. Sie erlaubt lediglich ein Programm oder einen Netzwerkport freizuschalten und dabei höchstens noch die IP-Adressen beziehungsweise Netzbereiche einzugrenzen. Eine detailliertere Konfiguration ist erst mit der erweiterten Firewall-Konfiguration in der Management-Konsole MMC möglich.

Mit dem Assistenten der erweiterten Bedienoberfläche können Regeln zusammengeklickt werden, die wesentlich flexibler sind und beispielsweise gezielt Programme oder Dienste einschränken können. Zusätzlich können Regeln auf unterschiedliche Netzwerkschnittstellen angewendet werden. Vista unterscheidet dabei die Schnittstellentypen LAN, Remotezugriff und Drahtlos. Einschränkend hingegen ist, dass Regeln, die Programme betreffen, nur mit dem Pfad und dem Dateinamen arbeiten, nicht etwa mit einem „Fingerabdruck" der Datei in Form eines Hash-Wertes. Ein simples Ersetzen der Datei ermöglicht daher das Umgehen der Firewall-Regeln. Zum Testen der Regeln können auch verworfene, akzeptierte oder beide Arten von Paketen mitprotokolliert werden.

Wichtig ist das Verständnis, wie Vista Regeln abarbeitet. Zuerst kommen mehrere Regeln zum Einsatz, auf die der Anwender keinen Einfluss hat. Sie sorgen als erstes im Rahmen des „Windows Service Hardening" dafür, dass ein Dienst nur Verbindungen öffnen darf, die sein Programmierer vorher angemeldet hat. Dann greifen die Regeln zur Verbindungssicherheit (erst wirksam in der Zusammenarbeit mit Windows Server 2008). Anschliessend folgen die Ausnahmeregeln für per IPsec verschlüsselte Verbindungen. Erst jetzt folgen explizite Deny-Regeln. An vorletzter Stelle beachtet Vista „positive Ausnahmen" (z.B. für Windows Updates). Zuallerletzt folgen die beiden Default-Regeln für ein- und ausgehenden Verkehr.

Windows Defender

Der Windows Defender geht auf lästige Spyware-Programme los. Es bietet neben einer Scan-Funktion auch einen Echtzeitschutz, welcher im Hintergrund läuft. Dieser prüft die Interneteinstellungen, das System und

Anwendungen auf gefährliche Änderungen durch Spyware. Integriert ist ebenfalls eine Auto-Update-Funktion. Ein speziell abgestelltes Team aus Microsoft-Experten durchsucht das Internet ständig nach neuer Spyware und entwickelt geeignete Gegenmassnahmen.

Nützlich sind die erweiterten Funktionen: Sie bieten die Möglichkeit, schwer zugängliche Systemfunktionen- und Einstellungen wie Autostart, laufende Prozesse oder heruntergeladene ActiveX-Objekte einfach zu konfigurieren.

Per Knopfdruck stellen Sie wieder die ursprüngliche Internet-Explorer-Startseite her, sollten Sie sich einen Browser-Hijacker eingefangen haben. Das Programm bindet sich in den System-Tray ein.

Internet Explorer 7

Sicherlich am meisten Veränderungen hat der Internet Explorer 7 erfahren. Neu unterstützt der IE7 Extended Validation SSL (EV-SSL-Zertifikate), hat einen Phishing-Filter integriert und verfügt unter Vista über einen geschützten Modus.

EV-SSL-Zertifikate

Betrugsversuche mittels so genannter Phishing-Seiten versuchen, Ihre persönlichen Daten wie Kennwörter, Pins und Tans oder ähnliches auszuspähen. Mit Hilfe der Extended Validation SSL-Zertifikate ist der Datenverkehr zwischen Ihrem Browser und dem jeweiligen Webserver wesentlich fälschungssicherer gegen Phishing-Angriffe, weil eine strenge Überprüfung der Identität des Webserver-Betreibers respektive SSL-Zertifikatsantragsstellers stattgefunden hat.

Wenn Sie beispielsweise eine Webseite öffnen, die die Anforderung des Extended Validation Standards erfüllt, färbt sich die URL-Leiste grün. Eine Anzeige neben dieser grünen Leiste stellt abwechselnd den im Zertifikat angegebenen Namen des Unternehmens und die Zertifizierungsstelle dar, die das Zertifikat ausgegeben hat (Abbildung 2).

Phishing-Filter

Der Phishing-Filter des Internet Explorer 7 verwendet einen Online-Service, der mehrmals in der Stunde neue Informationen über betrügerische Webseiten aktualisiert. Dieses Feature nutzt zwei Prüfverfahren, um Anwender vor Phishing-Betrug zu bewahren:

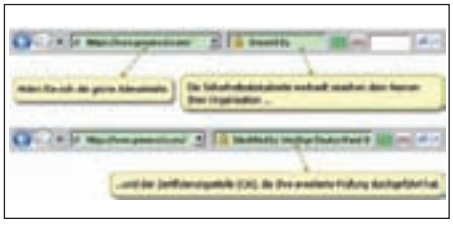

Abbildung 2

Bildquelle: Verisign

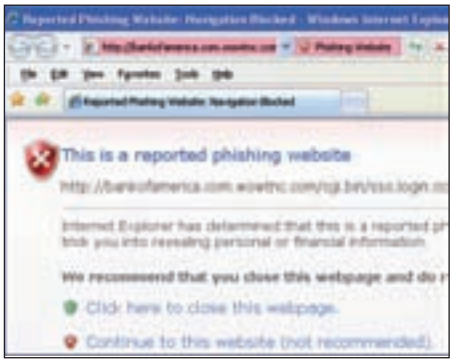

Abbildung 3

Abbildung 4

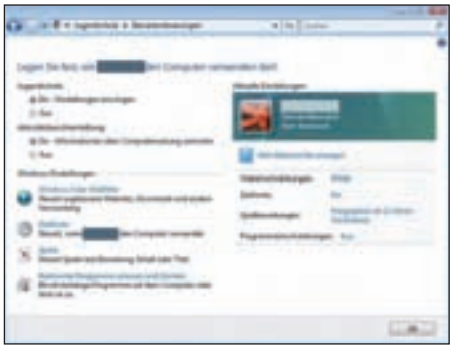

Abbildung 5

- Es analysiert die Internetseiten, die der Anwender besuchen möchte, hinsichtlich typischer Eigenschaften von Phishing-Seiten.
- Es sendet die Adresse der Webseite an den Online-Service bei Microsoft, um diese mit der ständig aktualisierten Liste bekannter Phishing-Seiten abzugleichen.

Wenn die gerade besuchte Webseite als Phishing-Seite bekannt ist, signalisiert der Internet Explorer 7 die Bedrohung anhand einer rot-eingefärbten Adressleiste und leitet Sie automatisch auf eine neutrale Warnseite. Ist eine Internetseite noch nicht als Phishing-Seite bestätigt, verhält sich aber so, werden Sie ebenfalls gewarnt und die Adressleiste färbt sich gelb. Sie können Phishing-Seiten und auch Seiten, die fälschlicherweise als solche eingestuft werden, direkt über das Phishing-Filter-Formular aus Ihrem Browser heraus melden (Abbildung 3).

Geschützter Modus

Im geschützten Modus kann Windows Vista nicht ohne Zustimmung des Anwenders Nutzer- und Systemdateien oder Einstellungen verändern. Der geschützte Modus verlangt bei jeder Aktivität, die den Computer verändern oder ein Programm starten will, das Eingreifen des Anwenders. Dadurch sinkt die Wahrscheinlichkeit deutlich, dass sich ein Programm automatisch und unerwünscht installiert. Diese Funktion fördert also zutage, was eine Internetseite versucht zu tun.

Der Internet Explorer ist zurzeit die einzige Applikation, die den geschützten Modus verwendet. Wie jedoch Praxisberichte zeigen, ist es möglich, auch andere Software in diesen Modus zu bringen. Beachten Sie jedoch, dass die Orte, auf welche diese Software zugreifen möchte (oder muss), entsprechend freigegeben werden müssen (Abbildung 4).

Jugendschutz

Der Jugendschutz ist in den Home-Versionen enthalten. Da er nicht zwingend die Firmensicherheit erhöht, nur einige wenige Kommentare dazu.

Der in Windows Vista integrierte Jugendschutz soll Eltern die Sicherheit geben, bestimmen zu können, was die Kinder am Computer machen. Mithilfe des Jugendschutzes legen Eltern fest, welche Spiele ihre Kinder spielen, welche Programme sie verwenden

Zum Autor

Andreas Wisler (Tel. 052 320 91 20), Dipl. Ing. FH, CISSP, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganz-heitlichen und produkteneutralen IT Sicherheitsüberprüfungen und -beratungen auseinander setzt. System Hardening rundet das Portfolio ab. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (INFONEWS) herunter geladen werden kann. Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.

und welche Websites sie sich ansehen dürfen. Eltern können die Computernutzung auf bestimmte Zeiten beschränken und darauf vertrauen, dass diese Beschränkungen von Windows Vista eingehalten werden, auch wenn sie nicht zu Hause sind (Abbildung 5).

Bitlocker

Die Datensicherheit auf verlorenen oder gestohlenen PCs ist für Sicherheitsexperten und Unternehmen ein immer grösseres Problem. Die auf einem PC gespeicherten Daten sind oftmals von deutlich grösserem Wert als der PC selbst. Wenn sie verloren gehen, gestohlen oder nicht autorisiert veröffentlicht werden, dann kann dies zu ernsthaften Problemen führen. BitLocker ist in Windows Vista (nur Enterprise und Ultimate) und Windows Server 2008 integriert. Es verhindert durch Datenverschlüsselung (inklusive der Auslagerungsdatei und der Datei für den Ruhezustand), dass ein Dieb ein anderes Betriebssystem startet oder ein Tool verwendet und so die Datei- und Systemverschlüsselung von Windows Vista umgeht. Auch das Offline-Anzeigen von Dateien auf geschützten Laufwerken ist nicht mehr möglich. Im Idealfall nutzt man das Feature TPM 1.2 (Trusted Platform Module), um die Daten des Benutzers zu schützen. Weiter wird beim Systemstart eine Integritätsprüfung durchgeführt, welche garantiert, dass eine Datenentschlüsselung nur dann stattfindet, wenn die entsprechenden Komponenten unverändert und nicht kompromittiert sind und sich das verschlüsselte Laufwerk im entsprechenden Computer befindet.

Service Hardening

Grundlage des Service Hardening ist die Einführung eines „Per-service security identifier (SID)“. Damit lassen sich folgende Massnahmen umsetzen:

- Dienste laufen nicht mehr auf Local System, sondern mit individueller SID.
- Unnötige Windows Privilegien lassen sich per Service entfernen.
- Zuordnung eines write-restricted Access Token zu einem Service
- Firewall Policies lassen sich mit der „Per-service SID“ eines Dienstes linken.

Vorteil des Service Hardenings: Durch die passende Vergabe von Rechten abgestuft auf individuelle Dienste lässt sich erreichen, dass allfällig verseuchte Windows Dienste andere Komponenten des Systems kaum mehr in Mitleidenschaft ziehen können.

UAC – User Access Control

Sicherlich am meisten zu diskutieren gibt UAC. Hauptziel von UAC ist die Reduzierung der Angriffsfläche des Betriebssystems. Hierzu arbeiten alle Benutzer als Standardbenutzer. Der administrative Zugriff ist auf autorisierte Prozesse eingeschränkt. Diese Einschränkung minimiert die Möglichkeiten der Benutzer, Änderungen vorzunehmen, die sich auf die Stabilität des Computers auswirken können oder den Computer versehentlich für Malware oder Viren anfällig zu machen. Mit UAC können Administratoren die meisten Anwendungen, Komponenten und Prozesse mit eingeschränkten Privilegien ausführen – sie haben aber gleichzeitig die Möglichkeit, bestimmte Aufgaben oder Anwendungen mit administrativen Rechten auszuführen. Wenn ein Benutzer einen Task ausführt, für den administrative Rechte notwendig sind (zum Beispiel die Installation einer Anwendung), dann benachrichtigt Windows Vista den Benutzer und fragt entsprechende Anmeldeinformationen ab. Als Erleichterung haben die Standardbenutzer, im Gegensatz zu Windows XP, folgende Rechte erhalten:

- Anzeigen der Systemuhr und des Kalenders
- Ändern der Zeitzone
- Installation von Wired Equivalent Privacy (WEP), um eine Verbindung zu einem WLAN aufzubauen
- Ändern der Anzeigeneinstellungen
- Ändern der Energiesparoptionen
- Installation von Schriftarten
- Hinzufügen von Druckern und anderen Geräten, für die die Installation von Treibern erforderlich ist
- Erstellen und Konfigurieren von VPN-Verbindungen
- Herunterladen und Installieren von Updates mit einem UAC-kompatiblen Installer

Bisher war es nicht ohne weiteres feststellbar, welche Aktionen als nicht-administrativer Benutzer erlaubt waren und welche nicht. Dieses Problem wird durch ein neues Icon beseitigt, das für alle Befehle verwendet wird, für die administrative Rechte nötig sind. Dieses Icon findet sich im gesamten Betriebssystem wieder. Wenn nun ein Standardbenutzer versucht, eine administrative Aufgabe auszuführen, zum Beispiel eine Softwareinstallation, wird er nach einem administrativen Kennwort gefragt. Wenn er das Kennwort des lokalen Administrators kennt, kann er dieses eingeben. Alternativ kann er den Administrator um Hilfe bitten. Dieses Verfahren wird Over-the-shoulder (OTS) genannt. Administratoren können das Feature deaktivieren. In diesem Fall wird der Benutzer einfach darüber informiert, dass er die gewünschte Aufgabe nicht ausführen darf.

Steuerung von Peripheriegeräten

Mit DMI (Device Management and Installation) können Sie die Geräteinstallation auf den von Ihnen verwalteten Computern steuern. Sie können unter anderem festlegen, welche Geräte vom Benutzer installiert werden können und welche nicht. Ein Gerät ist ein Stück Hardware, mit dem Windows interagiert, um eine Funktion auszuführen. Windows kann nur über eine bestimmte Software mit der Hardware kommunizieren: dem Gerätetreiber. Um einen Gerätetreiber zu installieren, führt Windows eine Erkennung des Gerätes durch, stellt fest, was für ein Typ das Gerät ist, und sucht dann einen passenden Gerätetreiber. Um die Geräteinstallation zu steuern, stehen mit Windows Vista mehrere Richtlinieneinstellungen zur Verfügung. Sie können diese einzeln auf einem Computer oder über Gruppenrichtlinien in einer Active-Directory-Domäne konfigurieren. Egal, ob Sie die Einstellungen auf einen einzelnen oder auf viele Computer

anwenden möchten – Sie verwenden auf jeden Fall den Gruppenrichtlinienobjekteditor zur Konfiguration und Anwendung der Einstellungen. Unter Windows Vista stehen die Einstellungen bereits standardmässig zur Verfügung. Zur Konfiguration stehen drei Möglichkeiten zur Verfügung:

- Verhindern der Installation aller Geräte
- Zulassen der Installation autorisierter Geräte
- Verhindern der Installation von verbotenen Geräten

NAP – Network Access Protection

Die Technologie NAP soll vor zwei Gefahren schützen:

- Notebooks, die von Mitarbeitern auch ausserhalb des Unternehmens genutzt werden und währenddessen einem Malware-Angriff zum Opfer fallen. Nimmt der Anwender sein Notebook in der Firma wieder in Betrieb, kann sich die Malware dann im Unternehmens-LAN ungehindert verbreiten. Zentrale Schutzinstanzen für das Firmennetz, die Administratoren zum Schutz vor Angriffen aus dem Internet eingerichtet haben, kommen hierbei nicht mehr zum Zuge – schliesslich erfolgt der Angriff aus dem vermeintlichen sicheren Intranet.
- Heimische PCs, mit denen Mitarbeiter über ein virtuelles privates Netzwerk (VPN) auf das Unternehmens-LAN zugreifen, und Notebooks von Besuchern, die per WLAN-Connectivity über das Firmennetz Zugang zum Internet erhalten, stellen ebenfalls ein Sicherheitsrisiko dar. Verfügt der PC über Personal-Firewall und Antivirus-Programm, und sind diese mit den aktuellsten Patches und Virensignaturen ausgestattet?

Bei der Verbindungsaufnahme eines Computers mit dem Netzwerk wird zuerst geprüft, ob sein gegenwärtiger Sicherheitsstatus die vom Administrator definierten Zugangsrichtlinien erfüllt. Ist NAP für die strikte Isolation konfiguriert, erhalten unsichere Computer, die die vorgegebenen Richtlinien nicht erfüllen oder nicht NAP-konform sind, keinen Zugang zum Netzwerk.

Abbildung 6

Schlusswort

Vista bietet ein vielseitiges Spektrum an neuen und verbesserten Technologien, die die Sicherheit massiv erhöhen können. Damit steigt natürlich auch der Aufwand zur Konfiguration. Planen Sie daher genügend Zeit für Tests ein, bevor Sie diese in Ihre produktive Umgebung implementieren. Wir sind überzeugt, dass Sie mit diesen Möglichkeiten auch Ihre IT-Sicherheit erhöhen können.

PS: Besten Dank an Microsoft für die vielen Informationen.