INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Vista / Windows Server 2008 – Was bringen die neuen Betriebssysteme?

Vista ist bereits über ein Jahr auf dem Markt, bald soll Windows Server 2008 folgen. Grund genug, sich auch mit den Sicherheitsaspekten der beiden Betriebssysteme auseinanderzusetzen. Obwohl die Verbreitung von Vista sehr schleppend vorwärtsgeht, kann sich das Zusammenspiel mit Windows Server 2008 lohnen. Dieser INFONEWS beschreibt kurz die neuen Funktionen, welche die Sicherheit erhöhen können. Praktisch zu allen Themen finden Sie auf der Homepage von Microsoft weitere tiefer führende Informationen.

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
- Backup Images

Zusätzlich in Windows Server 2008

- Workload Based Roles
- Verbesserter Server Core
- Erweiterung des Eventlog
- Read Only Domain Controller
- Failover-Clustering
- Cryptography Next Generation CNG

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Inhaltsverzeichnis

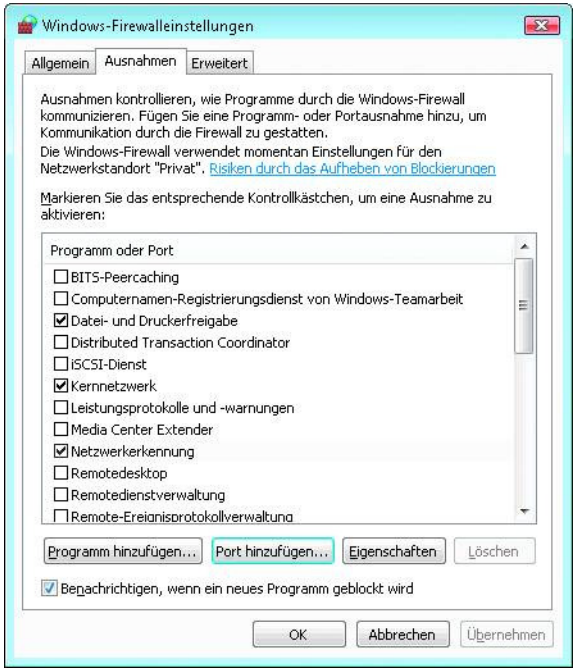
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Vista

1.1 Firewall

Microsoft hatte schon bei 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:



Als Vorbereitung auf Windows Server 2008 wurde die Integration von IPsec vorangetrieben, was die verschlüsselte Kommunikation in Unternehmens-Netzwerken erleichtert. Zusätzlich kann ein eingeschränktes Netzwerk zur Verfügung gestellt werden, bevor das gesamte Netzwerk sichtbar ist. Vorbereitend wird unter anderem überprüft, ob ein Client alle Sicherheitsupdates und die neuesten Virensignaturen installiert hat.

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

Eine der Verbesserungen, die jedem Anwender zugutekommt, ist die automatische Anpassung der Firewall an das Netzwerk, an dem der Rechner angeschlossen ist: Sie kann die drei unterschiedlichen Standorte Domäne, öffentliches und privates Netz unterscheiden und aktiviert darin jeweils eigene Sätze von Firewall-Regeln.

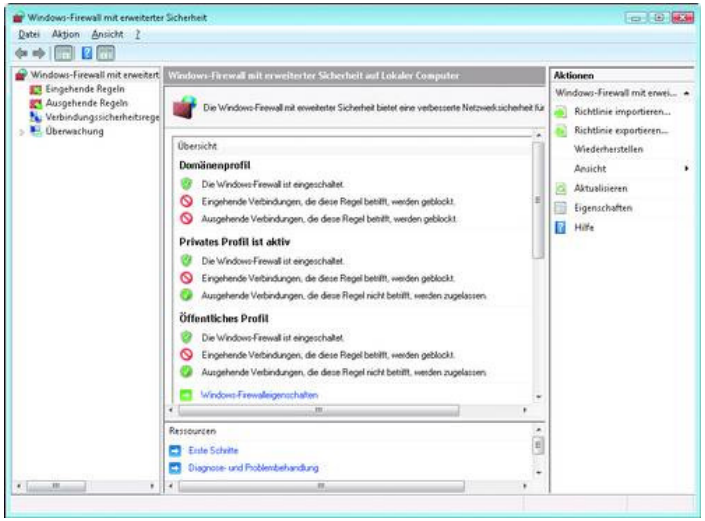
Vista beobachtet im Hintergrund die Hardware-Adresse des Internet-Gateways und speichert diese Zuordnung zu einem Standort-Profil ab. Wird das Gerät an einem anderen Netz angeschlossen, schaltet Vista erstmal auf das öffentliche Standort-Profil um, in dem im Auslieferungszustand alle Ports geschlossen sind. Anschliessend fragt Windows nach, ob es sich bei dem neuen Netzwerk um ein Öffentliches oder Privates handelt. Für verschiedene Netze lassen sich jedoch keine eigenen Regelsätze anlegen, die Regeln beziehen sich immer auf ein Standort-Profil.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

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.

Wie bereits erwähnt, kann die Vista-Firewall neben eingehenden auch ausgehende Verbindungen kontrollieren. In der Grundeinstellung erlaubt sie jedoch in allen Standort-Profilen alle ausgehenden Verbindungen. Mit dem MMC Snap-in kann nicht nur die lokale Konfiguration der Firewall, sondern via Gruppenrichtlinieneditor auch die Festlegung von Firewall-Regeln als Gruppenrichtlinien durchgeführt werden.



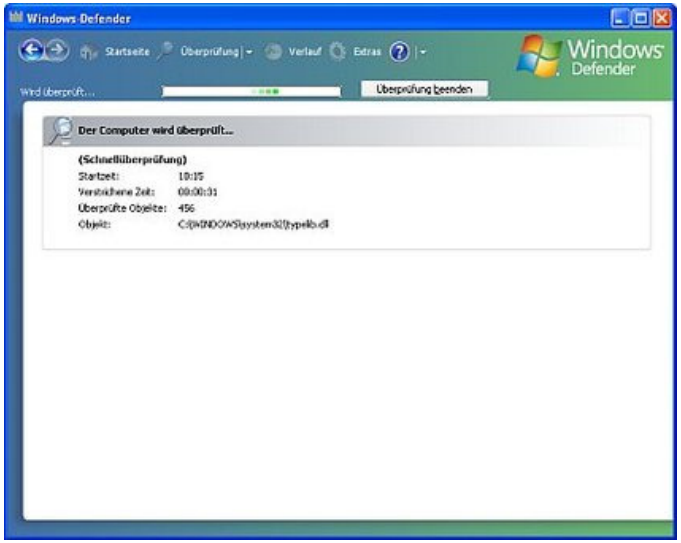
Mit dem Assistenten der erweiterten Bedienoberfläche können Regeln zusammengeklickt werden, die wesentlich flexibler sind, und können beispielsweise gezielt Programme oder Dienste einschränken. Zusätzlich können Regeln auf unterschiedliche Netzwerkschnittstellen angewendet werden. Vista unterscheidet 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 Firewallregeln. 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 und Ping). Zuallerletzt folgen die beiden Default-Regeln für ein- und ausgehenden Verkehr.

1.2 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. Weltweit beteiligen sich Benutzer von Windows Defender freiwillig an einem Netzwerk, das Microsoft dabei hilft, verdächtige Programme als Spyware einzustufen. Die teilnehmenden Benutzer erkennen rasch neue Bedrohungen und informieren die zuständigen Experten bei Microsoft, sodass letzten Endes alle Benutzer besser geschützt sind. Alle Benutzer von Windows Defender können diesem Netzwerk (mit dem Namen SpyNet AntiSpyware Community) beitreten und potenzielle Spyware an Microsoft melden. Je mehr Mitglieder der Community angeschlossen sind, desto schneller werden neue Bedrohungen entdeckt.

1.3 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.

1.3.1 EV-SSL-Zertifikate

Betrugsversuche mittels sogenannte 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 bzw. SSL-Zertfikatsantragsstellers stattgefunden hat.

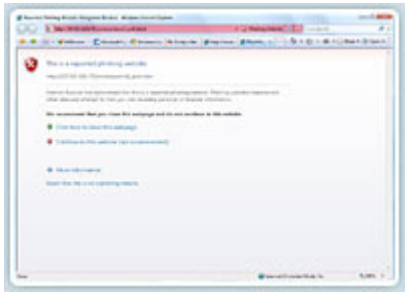
Wenn Sie beispielsweise eine Webseite öffnen, die die Anforderung des Extended Validation Standards erfüllt, färbt sich die URL-Leiste grün. Eine Anzeige neben dieser grünen Leiste stellt abwechselnd den im Zertifikat angegebenen Namen des Unternehmens und die Zertifizierungsstelle dar, die das Zertifikat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

Quelle: Verisign

1.3.2 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:

- 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.
Der Phishing-Filter ist nicht standardmässig eingeschaltet - Sie müssen die Funktion beim ersten Benutzen des Browsers nach der Installation aktivieren. Sie schalten den Phishing-Filter mit nur einem Klick im Browser-Menü ein und aus.

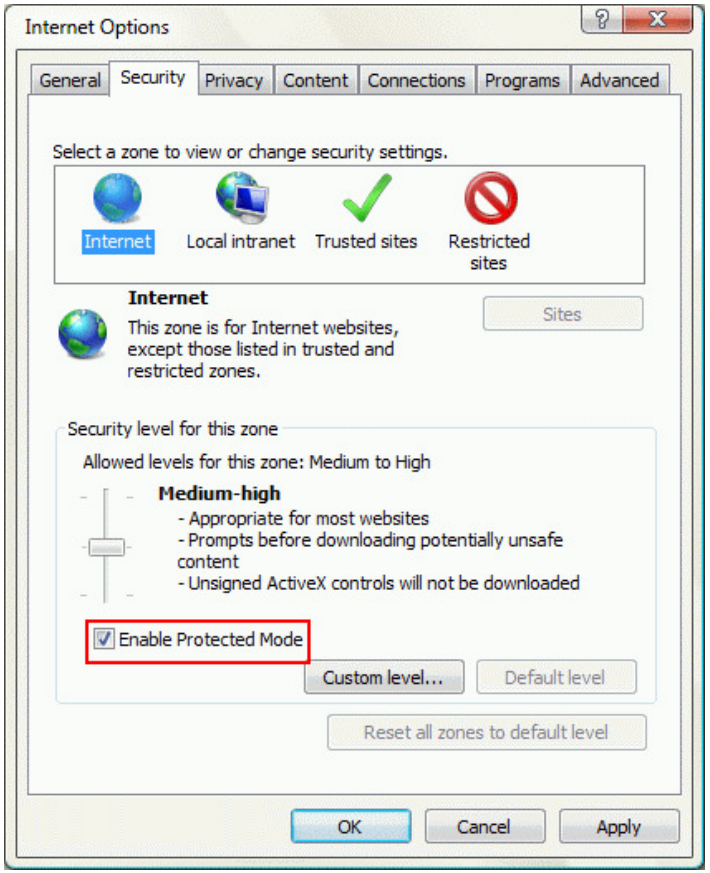
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1.3.3 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.



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

goSecurity.ch/infonews

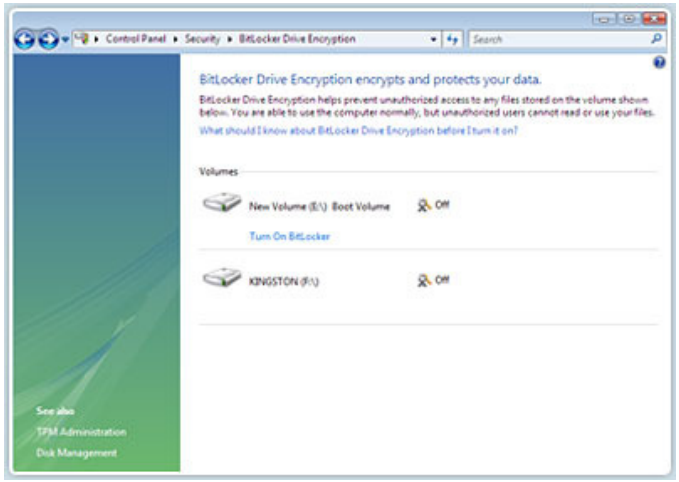
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1.4 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 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.

Zusätzlich kann die Option, den normalen Startprozess zu sperren bis der Benutzer eine PIN eingibt (ähnlich wie an einem Geldautomaten) oder ein USB-Gerät mit einem Schlüssel zur Verfügung stellt, aktiviert werden.

Für Firmen ist sicherlich interessant, dass dies vollständig über Gruppenrichtlinien steuerbar ist, inklusive dem Ablegen von Wiederherstellungsschlüsseln.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1.5 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.

1.6 UAC – User Access Control

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 Maleware 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.

Unter Windows Vista haben Standardbenutzer zusätzliche Privilegien. Diese sind zur Ausführung von Standardaufgaben notwendig. Die entsprechenden Privilegien haben nur minimale Auswirkungen auf das System und stellen ein geringes Risiko dar. Natürlich haben Administratoren trotzdem die Möglichkeit, diese Privilegien zu entfernen. Zu den neuen Berechtigungen für Standardbenutzer gehören:

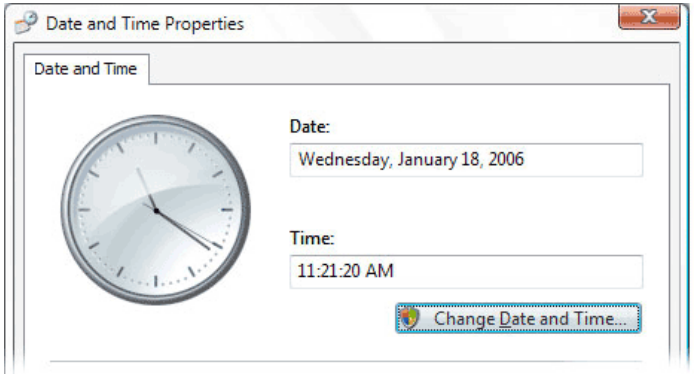
- Anzeigen der Systemuhr und des Kalenders,
- Ändern der Zeitzone,
- Installation von Wired Equivalent Privacy (WEP), um eine Verbindung zu einem WLAN aufzubauen.
- Ändern der Anzeigeinstellungen.
- Ändern der Energiesparoptionen.
- Installation von Schriftarten.
- Hinzufügen von Druckern und anderen 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.

Ausserdem handelt es sich bei der Defragmentierung nun um einen automatischen Prozess - die Benutzer müssen die Defragmentierung also nicht mehr von Hand anstossen.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Bisher war es jedoch nicht einfach festzustellen, welche Aktionen als nicht-administrativer Benutzer erlaubt waren und welche nicht. Dieses Problem wird durch ein neues Icon (das Schild - siehe zum Beispiel das Icon für das Sicherheitscenter unter Windows XP SP2) beseitigt, das für alle Befehle verwendet wird, für die administrative Rechte nötig sind. Dieses Icon findet sich im gesamten Betriebssystem wieder.



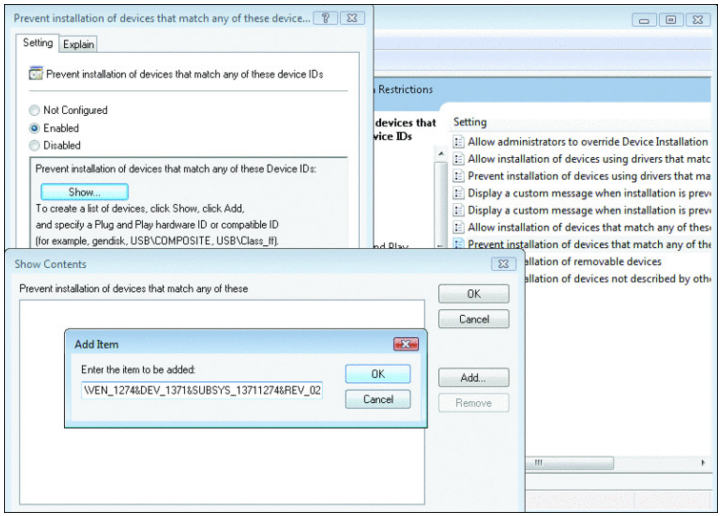
Wenn nun ein Standardbenutzer versucht, eine administrative Aufgabe auszuführen, zum Beispiel eine Softwareinstallation, wird er nach einem administrativen Kennwort gefragt. Wenn er das Kennwort des lokalen Administrators kennt, kann er dieses eingeben. Alternativ kann er den Administrator um Hilfe bitten. 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.

Um hingegen die Administratoren bei nicht administrativen Aufgaben zu schützen, steht das Admin Approval Mode-Feature zur Verfügung. Mit diesem Feature können Administratoren die täglichen normalen Aufgaben - wie die Arbeit mit Emails oder das Surfen im Web - mit einem Standardbenutzer-Token ausführen. Wenn administrative Rechte notwendig werden, wird der Administrator nach den entsprechenden Anmeldeinformationen gefragt. Es ist nicht mehr nötig, sich mit einem anderen Benutzerprofil anzumelden.

1.7 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. DMI ist Teil von Microsoft Windows Server 2008 und Windows Vista.

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. Ein Gerät hat für gewöhnlich mehrere Gerätekennungen - diese legt der Hersteller fest. Die gleichen Gerätekennungen befinden sich in der .inf-Datei des Gerätetreibers. Windows wählt aus, welcher Gerätetreiber installiert werden soll. Hierzu bedient es sich der Gerätekennungen.



Windows kann jede Kennung dazu benutzen, den passenden Treiber zu ermitteln. Die Gerätekennungen reichen von sehr spezifischen Kennungen (die sich auf ein einzelnes Modell eines Gerätes beziehen) bis zu sehr allgemeinen Kennungen (die sich zum Beispiel auf eine Geräteklasse beziehen). Es gibt zwei Arten von Gerätekennungen:

- Hardware IDs (Hardwarekennungen). Hardwarekennungen sind IDs, die am genauesten zwischen Geräte und Treiber übereinstimmen. Der erste String in der Liste der Hardwarekennungen wird auch Device ID (Geräte-ID) genannt (er bezeichnet die Version, das genaue Modell und die Revisionsnummer des Gerätes). Die anderen Hardwarekennungen in der Liste beziehen sich auf Details des Gerätes und sind nicht so eindeutig. Eine Hardwarekennung kann zum Beispiel die Version und das Modell des Gerätes enthalten, nicht jedoch die Revisionsnummer. Dieses Schema erlaubt es, Windows Gerätetreiber für Geräte mit verschiedenen Revisionsnummern zu verwenden, wenn kein Treiber für die entsprechende Revisionsnummer vorhanden ist.
- Compatible IDs (Kompatible Kennungen). Windows nutzt diese IDs, um einen Gerätetreiber auszuwählen, wenn dieser nicht über die Gerätekennung oder andere Hardwarekennungen gefunden werden kann. Kompatible Kennungen werden in einer bestimmten Reihenfolge aufgelistet. Die am genauesten beschreibenden Kennungen befinden sich am Beginn der Liste. Kompatible Kennungen sind sehr allgemein gehalten (eine solche Kennung kann zum Beispiel einfach Disk lauten).

Wenn Sie DMI nutzen, um die Installation von Geräten zu verhindern, die logische Geräte verwenden, dann müssen Sie alle Gerätekennungen für diese Geräte zulassen oder verbieten.

Um die Geräteinstallation zu steuern, stehen mit Windows Vista und Windows Server 2008 mehrere Richtlinieneinstellungen zur Verfügung. Sie können diese einzeln auf einem einzelnen Computer oder über Gruppenrichtlinien in einer Active Directory-Domäne konfigurieren. Egal, ob Sie die Einstellungen auf einen einzelnen Computer oder auf viele Computer anwenden möchten - Sie verwenden auf jeden Fall den Gruppenrichtlinienobjekteditor zur Konfiguration und Anwendung der Einstellungen. Die Einstellungen werden dem Gruppenrichtlinienobjekteditor über eine .adm-Datei hinzugefügt. Diese .adm-Datei trägt den Namen devinst.adm. Unter Windows Vista und Windows Server 2008 stehen die Einstellungen bereits

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

standardmässig zur Verfügung. Zur Konfiguration stehen drei Möglichkeiten zur Verfügung:

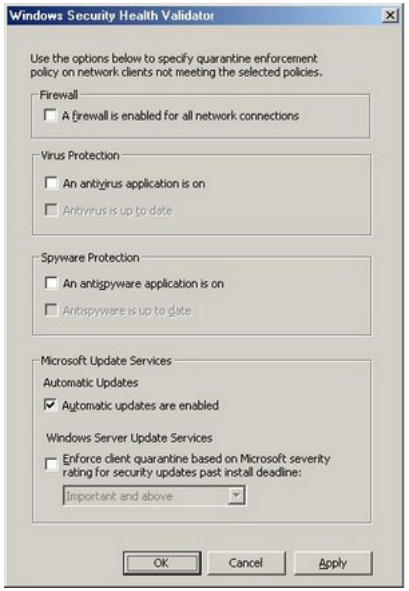
- Verhindern der Installation aller Geräte.
- Zulassen der Installation autorisierter Geräte.
- Verhindern der Installation von verbotenen Geräten

Hinweis: Sie können die Hardwarekennungen und kompatiblen Kennungen über zwei Wege ermitteln. Sie können den Gerätemanager nutzen oder ein Kommandozeilentool mit dem Namen DevCon aus dem Driver Development Kit (DDK). Microsoft hat auf seiner Homepage eine Schritt-für-Schritt-Anleitung veröffentlicht, die genau zeigt, wie beispielsweise ein Memory Stick integriert werden kann.

1.8 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 PCs über Personal-Firewall und Antivirus-Programm, und sind diese mit den aktuellsten Patches und Virensignaturen ausgestattet?



Die NAP-Technologie adressiert die folgenden drei Aspekte:

- Gültigkeitsprüfung von Netzwerkrichtlinien
  bei der Verbindungsaufnahme eines Computers mit dem Netzwerk wird als Erstes geprüft, ob sein gegenwärtiger Sicherheitsstatus die vom Administrator definierten Zugangsrichtlinien erfüllt. Findet lediglich eine NAP-Überwachung statt, wird eine Verletzung dieser Richtlinien zwar notiert, dem unsicheren Computern aber dennoch der

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Zugang zum Netzwerk gewährt. Ist NAP hingegen für die strikte Isolation konfiguriert, erhalten unsichere Computer, die die vorgegebenen Richtlinien nicht erfüllen oder nicht NAP-konform sind, keinen Zugang zum Netzwerk.

- Erfüllung von Netzwerkrichtlinien
  NAP sieht Administrations-Tools vor, mit denen sich der gewünschte Sicherheitsstatus schnell und einfach herstellen lässt. Unsichere Computer, die die geforderten Richtlinien nicht erfüllen, können dadurch während ihrer Isolierung im Quarantäne-Netzwerk eine Aktualisierung ihrer Sicherheitskonfiguration durchführen, um schliesslich den Zugang zum Netzwerk zu erlangen.
- Netzwerkisolation
  Erfüllen PCs bei der Verbindungsaufnahme mit dem Unternehmens-LAN die geforderten Netzwerkrichtlinien nicht und werden daher als unsicher eingestuft, kann NAP diese Computer automatisch isolieren. Vorgesehen sind mehrere Szenarien, die von der Überstellung in ein separates Quarantäne-Netzwerk über Zugriffsbeschränkungen lediglich auf eine einzelne Ressource bis hin zur Verweigerung jeglichen Zugriffs auf interne Ressourcen reichen. Ebenso lässt sich ein Quarantäne-Netzwerk für Gast-PCs verwenden, die zwar keinerlei Berechtigungen für das Firmennetz besitzen, zumindest aber auf das Internet zugreifen dürfen.

1.9 Backuperweiterung

Ab Vista Business können Sie Ihr System mit einer zusätzlichen Backup-Lösung
schützen, die 1:1-Abbilder der Festplatte sichert. Als Speichermedium kommen Brenner, externe Festplatten, aber auch Freigaben im Netzwerk in Betracht.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2 Windows Server 2008

Gemäss heutigem Wissensstand soll am 27. Februar 2008 die finale Version von Windows Server 2008 vorgestellt werden. Doch schon jetzt gibt der Release Candidate einen guten Überblick über das, was die neue Windows-Server-Version bieten wird.

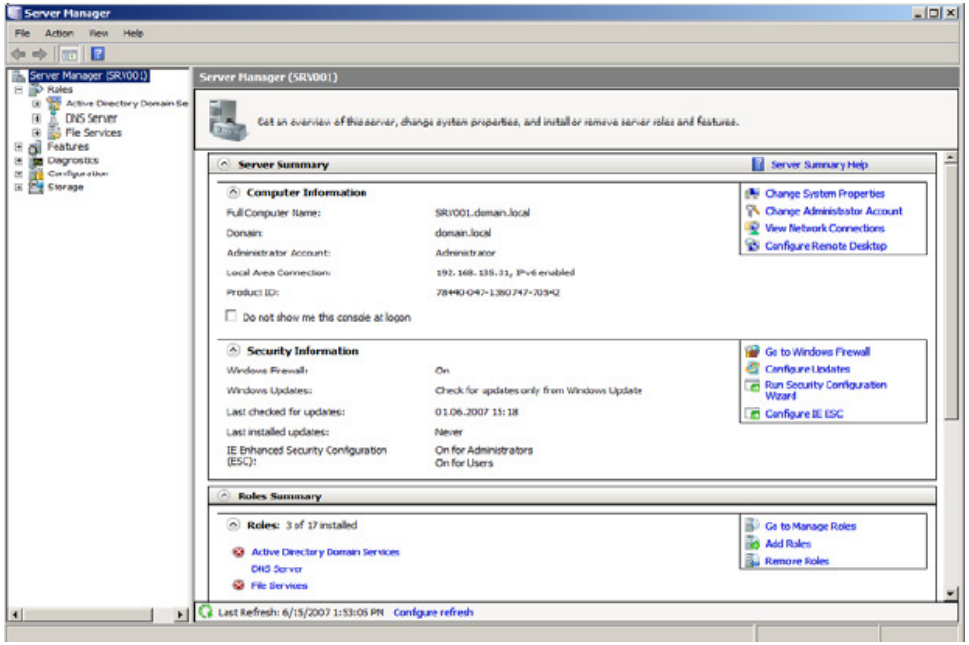
2.1 Workload based roles

Dem neuen Server von Microsoft stehen verschiedene Rollen zur Verfügung. Anhand dieser werden nur diejenigen Dienste installiert, die auch wirklich benötigt werden. Eine Rolle ist dabei eine logische Gruppierung von Komponenten auf Basis von häufig verwendeten Szenarien. Die Hierarchie und Abhängigkeiten einer Rolle sind im Modell abgebildet. Dazu gehören auch die Default-Einstellungen. Abhängigkeiten der verschiedenen Rollen werden bei der Installation geprüft. Sollten Komponenten fehlen, werden diese nachinstalliert.

2.2 Service Core

Neu kann eine minimale Version des Windows Servers installiert und betrieben werden. Somit stehen nur die grundlegenden Serverbetriebssystem-Funktionalitäten zur Verfügung. Das Booten und der Betrieb kann selbstständig in Headless bzw. Embedded-Szenarien erfolgen. Die Verwaltung erfolgt über drei Wege:

- Lokale und Remote Befehlszeilen-Tools
- Terminaldienste (nur Remote)
- Microsoft Management Console (nur Remote)



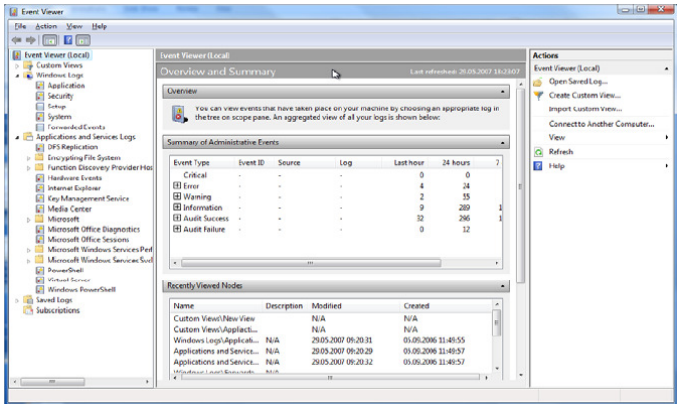
Somit wir die Angriffsfläche auf ein absolutes Minimum reduziert. Jedoch gilt es zu beachten, dass dies nur für bestimmte Serverrollen möglich ist (DNS, DHCP, Datei-Server, AD, File/Print, Media Stream).

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2.3 Erweiterung des Event Viewers

Das Eventlog von Windows ist die Anlaufstelle Nummer Eins, wenn es um die Behandlung von Fehlern geht. Diesem Umstand hat Microsoft Rechnung getragen und diverse Anpassungen vorgenommen. So werden die Daten neu als XML Daten gespeichert und sind somit schnell an andere Applikationen angepasst, bzw. übernommen. Zudem können Events an andere Windowssysteme weitergeleitet werden, dies in Abhängigkeit von ID, Quelle, etc. Die Auswertung wird durch diverse Filtermöglichkeiten erweitert, dies sogar über mehrere Eventlogs hinweg.

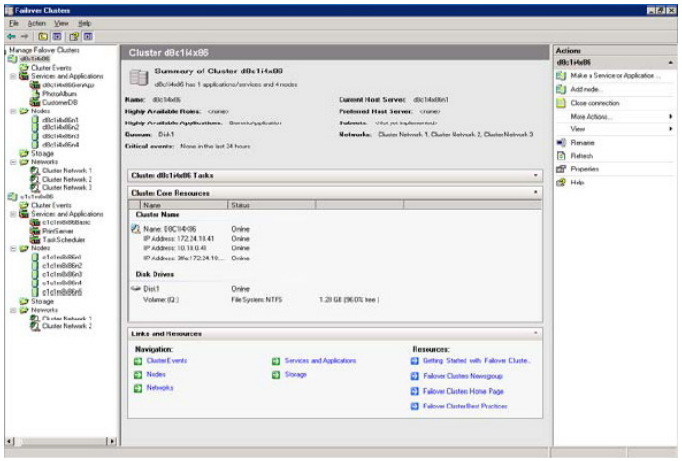


2.4 Read Only Domain Controller

Dieser neue Domänencontroller-Typ ermöglicht Unternehmen, einen Domänencontroller auch in solchen Standorten sicher einzusetzen, wo die physikalische Sicherheit nicht gewährleistet ist. Ein RODC führt lediglich eine Nur-Lese-Kopie von der Active Directory-Verzeichnisdienst-Datenbank der betreffenden Domäne. Passwörter werden zudem standardmässig nicht gespeichert. Vor Windows Server 2008 mussten sich Anwender in Niederlassungen über eine langsame WAN (Wide Area Network) -Verbindung bei einem Domänencontroller in der Zentrale authentifizieren – wenn in dem entfernten Standort keine ausreichende physikalische Sicherheit für die Vor-Ort-Platzierung eines lokalen Domänencontrollers bestand. In vielen Fällen war diese Methode jedoch recht ineffizient. Durch die Möglichkeit, eine lediglich lesbare Replikation der Active Directory-Datenbank direkt in der Niederlassung nahe bei den Benutzern zu platzieren, profitieren diese von zügigeren Anmeldungen. Genauso kann der Zugriff auf Netzwerkressourcen, die eine Authentifizierung erfordern, nun effizienter erfolgen. RODC ist somit eine ideale Lösung für Standorte, deren physikalische Sicherheit nicht ausreicht, um dort einen regulären Domänencontroller zu platzieren.

2.5 Failover-Clustering

Die Verbesserungen in diesem Bereich zielen darauf ab, die Konfiguration von Server-Clustern zu vereinfachen, um darüber den Schutz und die Verfügbarkeit von Daten und Anwendungen zu verbessern. Das neue Validierungs-Tool prüft, ob Ihre System-, Storage- und Netzwerkkonfiguration Cluster-geeignet sind. Durch die neuen Funktionen für das Failover-Clustering können Administratoren die Einrichtung und Verwaltung von Server-Clustern mit Windows Server 2008 wesentlich leichter durchführen.



2.6 Cryptography Next Generation CNG

Die CNG implementiert einen neuen Verschlüsselungsalgorithmus, welcher durch die US-Regierung definiert wurde. Dieser Standard kann für Verschlüsselung, Signierung, Schlüsselaustausch und Hash-Bildung verwendet werden. Zusätzlich ist die Möglichkeit gewährleistet, dass Dritt-Hersteller diese Schnittstelle verwenden können, beispielsweise für Smart Cards.

3 Schlusswort

Die neuen Versionen für Client und Server bieten 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.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21