INFONEWS

infonews.ch

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.

RECHNERSICHERHEIT

Die vergangenen Wochen haben gezeigt, dass der Schutz der eigenen Infrastruktur sehr wichtig ist. Im grossen Stil wurden (und werden) Regierungen, Firmen und Private überwacht. Auch in der Schweiz ist die Cyber-Kriminalität auf dem Vormarsch. Dieser INFONEWS zeigt, wie die Rechnersicherheit erhöht werden kann.

Inhaltsverzeichnis

INFONEWS

infonews.ch

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.

1 Rechnersicherheit

1.1 Einleitung

Die vergangenen Wochen haben gezeigt, die Überwachung von Regierungen ist schon länger Tatsache. Im grossen Stil wurden (und werden) fremde Regierungen, Firmen, aber auch Privatpersonen überwacht. Auch in der Schweiz ist die Cyber-Kriminalität auf dem Vormarsch. Die Melde- und Analysestelle MELANI (http://www.melani.admin.ch) des Bundes zeigt in den halbjährlichen Lageberichten, dass die Schweiz immer mehr ins Visier von Kriminellen kommt. Der Bundesrat hat daher reagiert und am 27. Juni 2012 die „Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken" gutgeheissen. Mit dieser Strategie will der Bundesrat in Zusammenarbeit mit Behörden, Wirtschaft und den Betreibern kritischer Infrastrukturen die Cyber-Risiken minimieren, welchen sie täglich ausgesetzt sind.

Aber auch „normale" Firmen sind davon betroffen. Die Schweiz gilt nicht umsonst als ein sehr innovatives Land mit guten Ideen und weltweit den meisten neu veröffentlichten Patenten. Mit den Ideen und Erfindungen lässt sich viel Geld verdienen. Zudem sind die technischen Infrastrukturen von kleineren Unternehmen im Normalfall nicht so gut geschützt wie bei Firmen mit zum Teil eigenen IT-Abteilungen. Oft heisst es „an meinen Daten hat niemand Interesse" oder „wir sind ja keine Bank". Doch beide Aussagen sind heute sehr gefährlich. Daten und Informationen bedeuten Geld. Eine geschickte Verknüpfung aus diversen Informationsquellen und das Profil für einen Menschen ist erstellt.

Eine Firewall und ein Antivirenprogramm zu haben, reicht nicht mehr aus. Verschiedene Tools sind auf dem Markt verfügbar, mit welchen innert weniger Minuten eine Schadsoftware (Malware) erstellt werden kann, die von heutigen Antivirenprogrammen nicht erkannt wird. Gelangt es einem Verbrecher diese in eine Firma einzuschleusen, sind keine Hindernisse mehr vorhanden und er kann sich im Netzwerk frei bewegen und nach interessanten Daten suchen. Um diese Hürde so hoch wie möglich zu setzen, ist es wichtig, die Systeme, das heisst Betriebssystem und die installierten Programme immer auf einem aktuellen Stand zu halten. Auch hier gilt es, E-Mails genau anzuschauen, bevor ein mitgeschicktes Programm ausgeführt wird. Auch der vermeintlich gewonnene USB-Sticks gilt es erst nach einer genauen Prüfung mit dem Computer zu verbinden.

Dieser INFONEWS soll Ihnen einige technische Möglichkeiten zur Erhöhung der IT-Sicherheit bieten.

1.2 Einführung Rechnersicherheit

Die Rechnersicherheit hängt von mehreren Komponenten ab. Dazu zählen u.a. Hardware, Betriebssystem, Anwendungen, Aufstellungsort und der Faktor Mensch.

In den Anfängen des PC-Zeitalters war die Hardware massgeblich für die Rechnersicherheit verantwortlich. Mehrheitlich führten Hardware-Defekte zu Systemausfällen. Heute gilt die Hardware grundsätzlich als zuverlässig. Die Rechnersicherheit ist jetzt stärker von den eingesetzten Applikationen und Betriebssystemen abhängig. Mit der wachsenden Bedrohungslage ist es deshalb unabdingbar, dass ausschliesslich Betriebssysteme und Applikationen eingesetzt werden, welche die notwendigen Sicherheits-

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

anforderungen erfüllen. Während beispielsweise Windows NT 4.0 im nahezu „spamlosen“ Zeitalter mit wenig Malware konzipiert wurde, basieren heutige Betriebssysteme auf einer aktuellen Bedrohungslage. Entsprechend sind dann die neueren Betriebssysteme wie Windows 7 / 8 oder Windows Server 2008 / 2012 bezüglich IT-Sicherheit auf einem wesentlich fortgeschrittenem Stand, weil diesem Thema aufgrund der veränderten Bedrohungslage während der gesamten Entwicklung eine zentrale Rolle zugeordnet wurde.

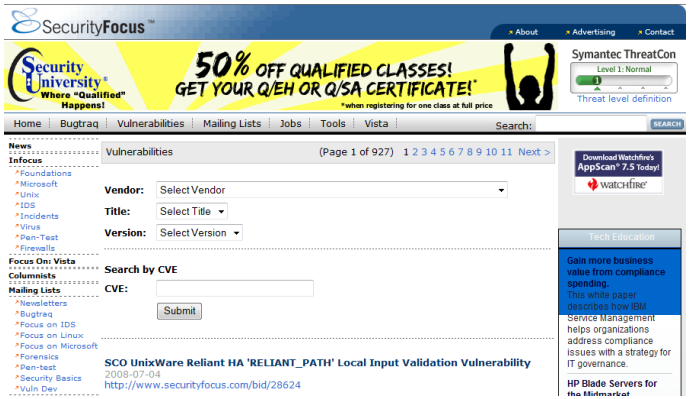
2 Vulnerabilities

Vulnerabilities (Schwachstelle, Schadenanfälligkeit, Verletzbarkeit) beinträchtigen nachhaltig die Rechnersicherheit. Sie können zu Systemausfällen führen oder bilden Angriffspunkte für bösartigen Code und Hacker.

Neue Betriebssysteme umfassen zusätzliche Sicherheitsfeatures, zahlreiche Funktionserweiterungen und viele Schnittstellen. Trotz Anstrengungen seitens der Hersteller zur Gewährung der Sicherheit enthalten diese erweiterten Funktionalitäten und Kommunikationsmöglichkeiten auch wieder neue Vulnerabilities, welche neue bisher noch nicht nutzbare Angriffsflächen für Hacker und Malware bieten.

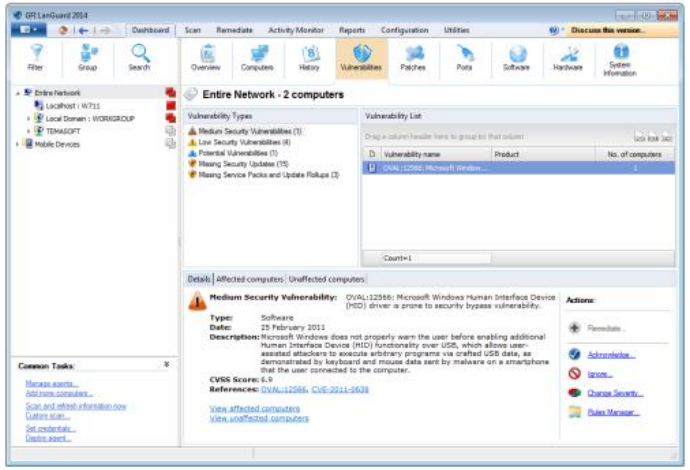
2.1 Vulnerability-Database

Eine unabhängige, kostenlose Aufstellung bekannter Vulnerabilities ist zum Beispiel unter http://www.securityfocus.com/ oder http://nvd.nist.gov/ erhältlich.



2.2 Vulnerability-Scanner

Verschiedene Vulnerability Scanner, wie beispielsweise der kommerzielle GFI LANGuard Network Security Scanner http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard, zeigen fehlende Sicherheitspatches an.

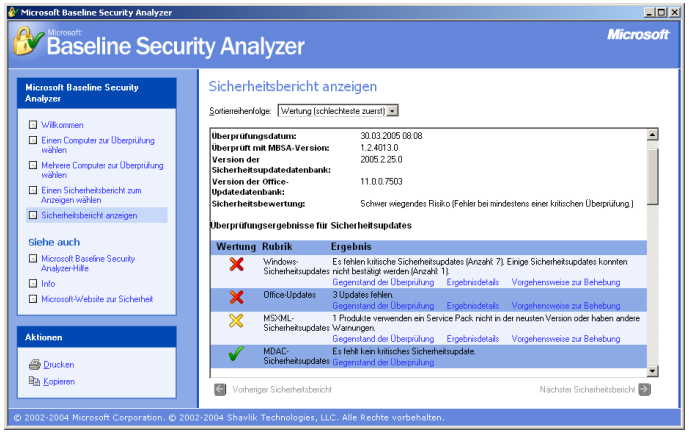


infonews.ch

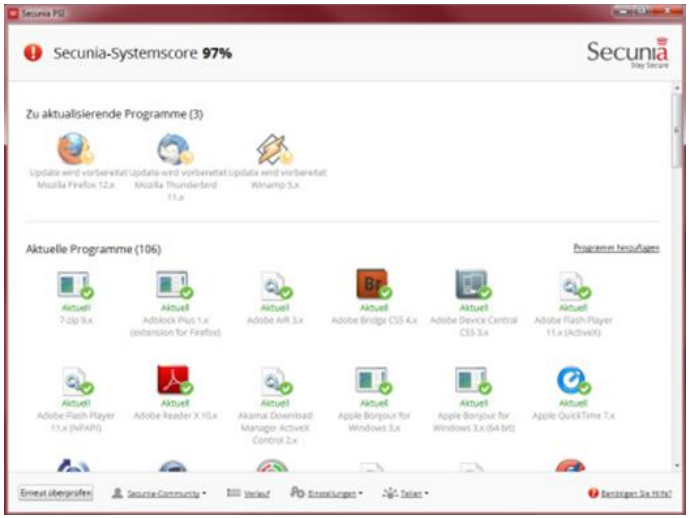
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Mit dem kostenlosen "Baseline Security Analyzer" von Microsoft http://www.microsoft.com/mbsa können ausschliesslich nur Windows Systeme u.a. auf Vulnerabilities oder fehlende Patches überprüft werden.



Damit wird aber nur das Betriebssystem aktualisiert. Immer mehr werden daher Schwachstellen in installierten Programmen ausgenutzt Gerade Software mit Berührungspunkten ins Internet, ist stark davon betroffen. Dies sind beispielsweise Browser (Internet Explorer, Chrome, Firefox, Safari, etc.), aber auch PDF-Reader und Flash. Auch diese Programme gilt es, regelmässig zu aktualisieren. Ein Tool, welches die installierte Software inventarisiert und mit den aktuell vorhandenen Versionen vergleicht, ist der Personal Software Inspector PSI von Secunia.



2.3 Patching - WSUS

Service Packs bilden eine Sammlung von einzelnen Patches oder Hot Fixes. Sie sollen Softwarefehler und somit auch Vulnerabilities beseitigen. Es ist jedoch möglich, dass mit dem Patching nicht nur Fehler behoben werden, sondern so auch neue Fehler und Vulnerabilities entstehen.

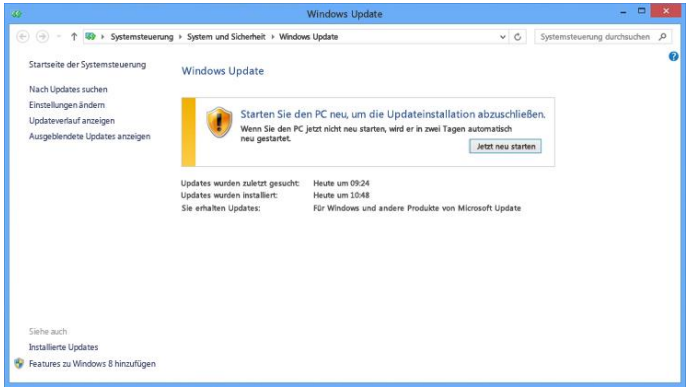
Werden Patches installiert, besteht die Gefahr, dass der Rechner oder einzelne Applikationen anschliessend nicht mehr korrekt arbeiteten. Deshalb müssen sämtliche Patches und Updates vor der Installation auf einem Testsystem geprüft werden. Weil Angriffe kurzfristig zu erwarten sind, müssen diese Tests rasch erfolgen. Innerhalb von einem bis zwei Tagen nach Veröffentlichung der Patches sollten diese mindestens auf kritischen Systemen (z.B. E-Mail- oder Webserver) installiert sein.

Werden die Patches zu spät oder nicht installiert, sind die Rechner einem grösseren Risiko betreffend Malwarebefall und Hacking ausgesetzt.

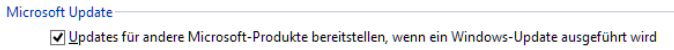
2.3.1 Automatisches Patchen

Automatisches Verteilen, bzw. Installieren von Microsoft Patches ist mittels entsprechenden Windows-Einstellungen und mittels Windows Server Update Service (WSUS) möglich. So können beispielsweise die Rechner so konfiguriert werden, dass sie automatisch die Patches vom Internet oder von einem WSUS-Server nach einem vorgegebenen Zeitplan herunterladen und installieren.

Folgende Einstellung unter Windows 8 (Pfad: Systemsteuerung\Alle Systemsteuerungselemente\Windows Update) bewirkt, dass der Rechner die Patches automatisch herunter lädt und diese zu einem festzulegenden Zeitpunkt installiert werden.

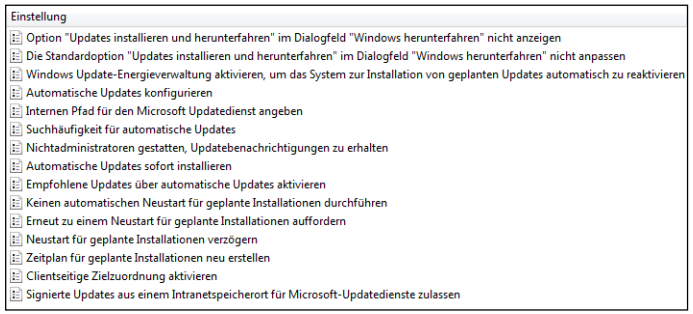


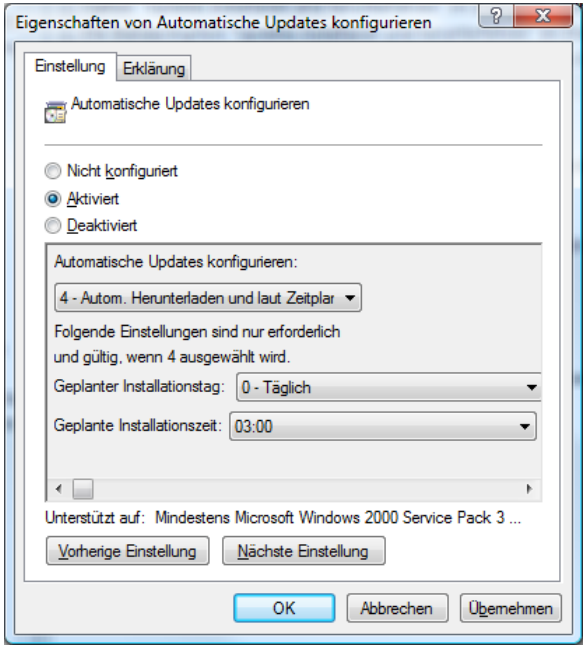
Wichtig ist auch, dass das untenstehende Kontrollkästchen gesetzt wird, damit alle Microsoft-Produkte aktualisiert werden (zusätzlich wird zum Beispiel das gesamte Office-Paket aktualisiert). Diese Option muss bei allen Betriebssystemen manuell gesetzt werden.

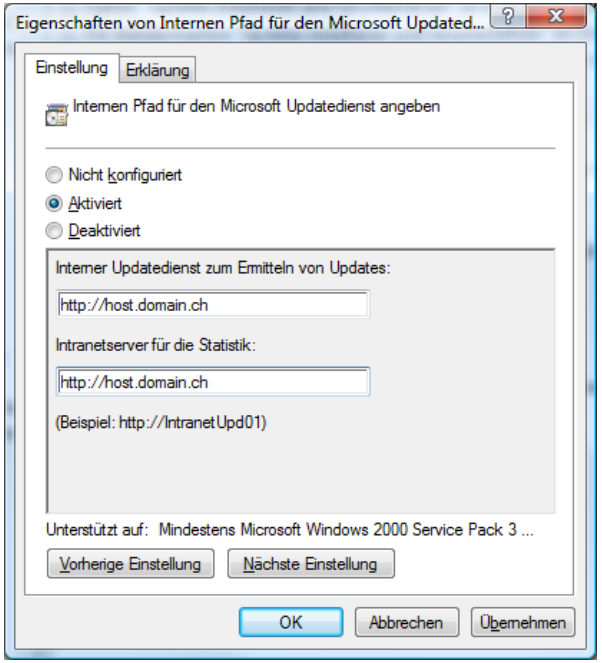


In einem Firmennetzwerk ist aus Security-Sicht zu empfehlen, eine WSUS-Infrastruktur einzurichten und die Installation der Patches auf den Rechnern mittels Group Policies automatisch und verbindlich zu steuern. Die entsprechenden GPO Settings zur Steuerung des Update-Bezugs sind in den folgenden Abbildungen zu sehen:

Pfad: Computerkonfiguration – Administrative Vorlagen – Windows Komponenten – Windows Update:







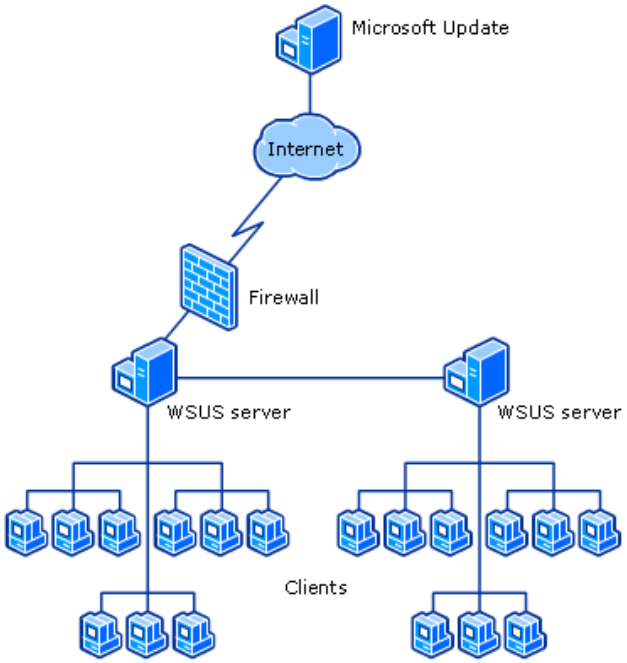
2.3.2 Windows Server Update Service (WSUS)

Mittels WSUS können die Updates und Patches für u.a. aktuelle Microsoft Betriebssysteme und vielen Applikationen von Microsoft verwaltet und verteilt werden. Dabei stehen verschiedenste Möglichkeiten der Softwareverteilung und ausführliche Statistiken zur Verfügung.

Mit WSUS lassen sich die Client-PCs oder Server für die Patch-Verteilung zu Gruppen zusammenfassen. Damit können einige speziell dafür vorgesehene Arbeitsplätze und Server vorgezogen mit Patches beliefert werden, um die Stabilität der Updates vor einer Gesamtverteilung sicherzustellen.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21



2.3.3 Apple OS X

Auch andere Betriebssysteme gilt es zu aktualisieren. Das Betriebssystem von Apple kann beispielsweise unter „Apfel" – Softwareaktualisierungen… mit den neuesten Patches versorgt werden.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

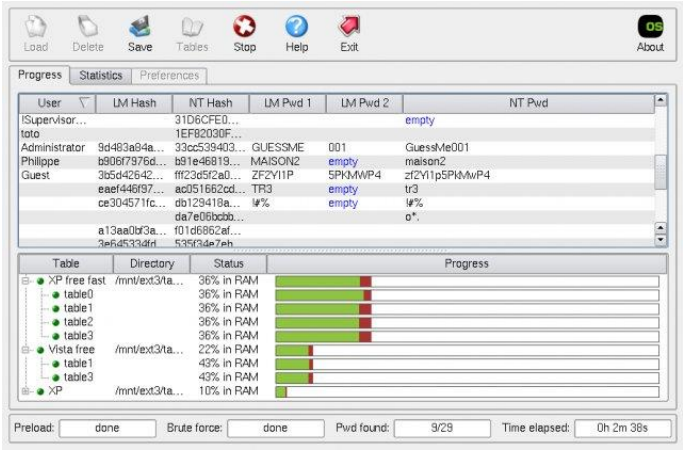
2.4 Kennwörter & Faktor Mensch

Ein Kennwort, auch Passwort (engl.: password), genannt, ist ein allgemeines Mittel zur Authentifizierung eines Benutzers innerhalb eines Systems, der sich durch eine eindeutige Information (das Kennwort) dem System gegenüber ausweist. Die Authentizität des Benutzers bleibt daher nur gewahrt, wenn das Kennwort geheim bleibt. Man spricht in diesem Zusammenhang auch von einem statischen Kennwort, im Gegensatz zu einem Einmalkennwort.

2.4.1 Kennwörter

Schwache Kennwörter sind leicht zu erraten oder mittels Wörterbuch-Attacke zu ermitteln. Folgende Abbildung zeigt, wie mit dem Tool NAT eine erfolgreiche Wörterbuch-Attacke durchgeführt werden konnte. Zusätzlich stehen im Internet so genannte Rainbow-Tables zum Herunterladen zur Verfügung. In diesen Tabellen sind die verschlüsselten Passwortwerde bereits abgelegt. Somit muss dieses nicht mehr berechnet, sondern nur noch ein Vergleich ausgeführt werden. Das Passwort-Knacken dauert dann nur noch Minuten, anstelle von Stunden. Heutige Rainbow-Tables enthalten zum Beispiel für Windows-Systeme mit Passwörtern bis acht Stellen praktisch alle Möglichkeiten. Daher gilt es, dass das Passwort heute mindestens 9, besser 10-12 Stellen aufweist.

Komplexe Kennwörter sind resistent gegen Wörterbuch-Attacken. Sie werden jedoch schnell vergessen und deshalb häufig auf einen Zettel unter der Tastatur geschrieben. Nebst Kennwortzusammensetzung sind auch Länge, Gültigkeitsdauer, Anzahl zu verwendende Kenn-wörter und Kontensperrung für die Rechnersicherheit von Bedeutung.



2.4.2 Faktor Mensch

Unachtsame, nachlässige oder ungeschulte Administratoren und Benutzer gefährden die Rechnersicherheit. Sie löschen z.B. aus Versehen wichtige Dateien, setzen falsche Berechtigungen, öffnen virenverseuchte E-Mails, sperren den Desktop während der Kaffeepause nicht, entsorgen Datenträger mit nicht richtig gelöschten Daten, halten sich nicht an die „Clear-Desk-Policy“ oder konfigurieren ihre Systeme nicht richtig.

Organisatorische Massnahmen, wie beispielsweise Awareness, Schulung oder Notfallplan helfen, diese Gefahren zu reduzieren. Auch technische Massnahmen, wie beispielsweise Backups erhöhen die Rechnersicherheit.

Mit dem Stichwort „Clear-Desk-Policy“ wird ein weiterer wichtiger Punkt im Bereich Faktor Mensch angesprochen. Mit einem wie in der folgenden Abbildung zu sehenden groben Chaos am Arbeitsplatz ist kaum ein akzeptables Sicherheitsniveau erreichbar. Es kann zusätzlich vermutet

werden, dass auch die dahinterliegende IT-Infrastruktur in ähnlichem Zustand ist.

3 Microsoft Windows

Die Rechnersicherheit hängt stark von den verwendeten Betriebssystemen ab. Dieses Kapitel zeigt verschiedene vorhandene Sicherheitsfunktionen unter Microsoft Windows.

3.1 Windows XP mit SP2 Security Übersicht

Microsoft hat mit dem Service Pack 2 für Windows XP das Sicherheitscenter eingeführt. Über das Sicherheitscenter können verschiedene sicherheitsrelevante Einstellungen verwaltet und überprüft werden: u.a., ob eine Firewall installiert, der Rechner gepatcht oder die Virendefinition aktualisiert ist.

- Neues Symbol in der Systemsteuerung
- Zentrale Verwaltung von sicherheitsrelevanten Einstellungen:
  - Ist eine Firewall installiert und aktiv?
  - Sind die automatischen Updates aktiviert?
  - Ist ein Virenscanner installiert und sind die Signaturen aktuell?

➔ Ist eine der Bedingungen nicht erfüllt, wird gewarnt!

3.1.1 Firewall

Die Windows Firewall unter Windows XP SP2 ist eine verbesserte Version der Internet Connection Firewall. Sie ist standardmässig aktiviert, lässt sich besser verwalten und unterstützt mehrere Profile.

Übersicht

- Windows Firewall ist eine softwarebasierte Firewall für Windows XP und Windows Server 2003

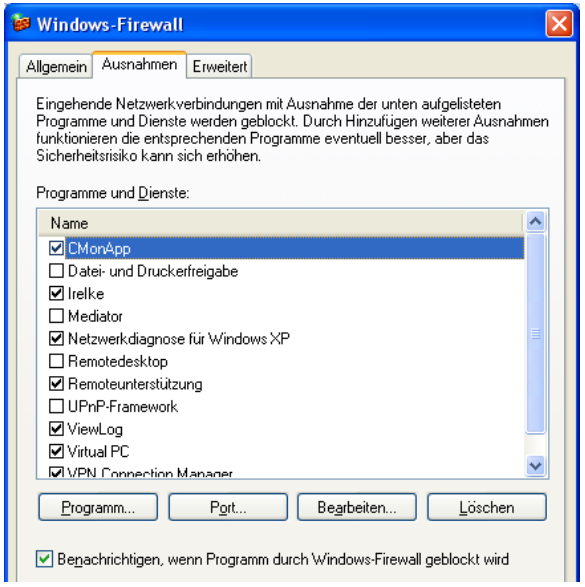
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

- Nachfolger der Internet Connection Firewall
- Standardmässig aktiviert
- Externe Ports werden dynamisch geöffnet und geschlossen (Stateful Filtering)
- Konfiguration pro Netzwerkverbindung möglich
- Unterstützen von Profilen:
    - Domain Policy (gilt im Firmennetzwerk)
    - Standard Policy (gilt ausserhalb des Firmennetzwerks)



Via „Programm…“ oder „Port…“ stehen zwei Möglichkeiten zur Verfügung, Ausnahmen zu definieren. In Firmennetzwerken lassen sich diese Einstellungen per Group Policies einheitlich für grössere Mengen von Clients festlegen.

3.1.2 Popup-Blocker

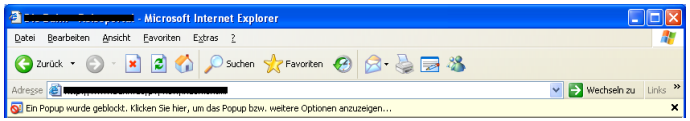
Die Internet Explorer-Informationsleiste in Windows XP SP 2 ersetzt viele allgemeine Dialogfelder, die in früheren Versionen die Benutzer zur Eingabe von Informationen aufgefordert hatten. Sie stellt einen wichtigen Bereich zum Anzeigen von Informationen dar, die Benutzer anzeigen oder als Grundlage heranziehen können. Beispiele für Dialogfelder, die durch Informationsleistenbenachrichtigungen ersetzt wurden, sind gesperrte ActiveX-Installationen, Popups, Downloads und aktive Inhalte. Die Informationsleiste enthält ähnliche Informationen wie der Infobereich in Outlook 2003, in dem Benutzer über gesperrte Inhalte informiert werden.

- Blockt Popup-Fenster, die nicht vom Benutzer aktiviert wurden
- Nur automatisch generierte Fenster werden geblockt
- Filterungsstufen: Hoch, Mittel, Niedrig!
- Informationsleiste
- Zeigt Meldung mit Sound an

Windows XP SP2 zeigt in der Informationsleiste eine Benachrichtigung an, wenn ein Popup geblockt wurde. Sie ermöglicht den Zugriff auf Funktionen des Popupblockers, wie z. B. erneutes Ausführen des Popups, Hinzufügen der Site zu einer Liste zulässiger Popups oder Navigieren zu Popupblockereinstellungen. Die Informationsleiste ermöglicht ausserdem auf oberster Ebene das Deaktivieren der Informationsleiste für Popups, falls der Benutzer entscheidet, dass die Benachrichtigung für dieses Ereignis zu gross ist.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

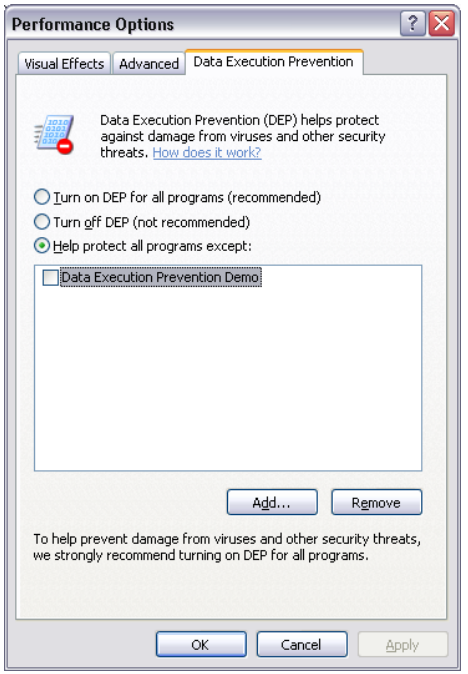


3.1.3 Sicherheitswarnung

Dateien die aus dem Internet heruntergeladen wurden oder von einer „unsicheren“ Quelle (z.B. Netzverbindungen) gestartet werden, erscheint eine Sicherheitswarnung. Diese muss bestätigt werden.

3.1.4 Ausführungsschutz DEP

Microsoft Windows XP SP2 trägt zum Schutz Ihres Computers gegen das Eindringen von destruktivem Code in Speicherbereiche bei, die für nichtausführbaren Code reserviert sind. Hierfür wird eine Reihe von Hardware- und Software-gesteuerten Technologien implementiert, die als Datenausführungs-Verhinderung (DEP, Data Execution Prevention) bezeichnet werden. Bei hardwaregesteuerter Datenausführungs-Verhinderung handelt es sich um eine Funktion bestimmter Prozessoren, die die Ausführung von Code in Speicherbereichen verhindert, die als Datenspeicher markiert sind. Diese Funktion wird auch als „No Execute“ (NX) oder Ausführungsschutz bezeichnet. Windows XP SP2 umfasst zudem eine softwaregesteuerte Datenausführungs-Verhinderung, die den Missbrauch von Ausnahmebehandlungs-Verfahren in Windows reduzieren soll.



Im Gegensatz zu einem Antiviren-Programm verhindern Hardware- und Software-gesteuerte Technologien zur Datenausführungs-verhinderung nicht, dass schädliche

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Programme auf Ihrem Computer installiert werden. Stattdessen überwachen sie Ihre Programme, um festzustellen, ob diese den Systemspeicher auf sichere Weise verwenden. Die hardwaregesteuerte Datenausführungs-Verhinderung überwacht bestimmte als „nicht ausführbar" deklarierte Speicherbereiche. Wenn ein Programm in einem als „nicht ausführbar" deklarierten Speicherbereich versucht, Code auszuführen, wird dieses Programm von Windows geschlossen. Diese Aktion wird auch bei nicht bösartigem Code durchgeführt.

Hinweis: Die softwarebasierte Datenausführungs-Verhinderung ist ein Bestandteil von Windows XP SP2 und ist standardmässig aktiviert, unabhängig von den hardwaregesteuerten Ausführungsschutz-funktionen des Prozessors. Softwaregesteuerte Datenausführungsverhinderung wird standardmässig auf alle Kernkomponenten und -Dienste des Betriebssystems angewendet.

Die Standardkonfiguration der Datenausführungs-Verhinderung ist für den Schutz des Computers bei minimaler Beeinträchtigung der Anwendungskompatibilität konzipiert. Je nachdem, wie die Datenausführungs-Verhinderung konfiguriert ist, kann es jedoch sein, dass einige Programme nicht ordnungsgemäss ausgeführt werden.

3.2 Windows Vista Security Übersicht

Mit der Veröffentlichung von Windows Vista hat Microsoft die in Windows XP SP2 vorhandenen Sicherheitsfunktionalitäten weiter entwickelt und mit neuen Technologien ergänzt:

- Bitlocker Drive Encryption
- User Account Control (UAC)
- Windows Firewall with Advanced Security (WFAS)
- Zusätzliche ACLs (Access Control Lists) zur Steuerung von Zugriffen auf Resourcen
- Verwaltung von Hardware-Restrictions mittels Group Policies
- Windows Defender Spyware Detection
- Network Access Protection
- Windows Service Hardening
- IE7.0 Protected Mode
- Vista Jugendschutz

Das Windows Vista Sicherheitscenter wurde um zusätzliche Elemente erweitert und bietet den Zugriff auf:

- Erweiterte Firewall
- Automatische Updates
- Schutz vor schädlicher Software
- Antivirenprogramm
- Schutz vor Spyware (Windows Defender)
- Weitere Sicherheitseinstellungen
    - Internetsicherheitseinstellungen

3.2.1 Bitlocker Drive Encryption

Bitlocker-Laufwerkverschlüsselung ist ein Feature zur Datenverschlüsselung der Betriebssystem Partition (nicht in allen Versionen enthalten).

BitLocker verhindert, dass eine nicht berechtigte Person ein anderes Betriebssystem starten oder ein Tool verwenden kann, um damit die Datei- und Systemverschlüsselung von Windows zu umgehen. Im Idealfall nutzt BitLoker das Feature TPM 1.2 (Trusted Platform Module), um die Daten des Benutzer zu schützen.

BitLocker verbessert Vertraulichkeit und Integrität der Daten:

- Vollständig Verschlüsselung von Laufwerken
- Integritätsüberprüfung von Komponenten beim Systemstart

Die Laufwerksverschlüsselung umfasst das gesamte Windows-Volume, inklusive der Auslagerungsdatei und der Datei für den Ruhezustand. Dank Bitlocker lässt sich auf die Festplatte eines gestohlenen Laptop-PCs nicht mehr über ein alternatives Betriebssystem zugreifen.

Die Integritätsprüfung beim Systemstart führt dazu, dass eine Datenentschlüsselung nur dann stattfindet, wenn die entsprechenden Komponenten unverändert und nicht kompromittiert sind und sich das verschlüsselte Laufwerk im vorgesehenen Computer befindet.

Für Problemfälle kann BitLocker Active Directory-Domänendienste nutzen, um Wiederherstellungsschlüssel zu hinterlegen. Ausserdem steht dem Administrator eine Wiederherstellungskonsole zur Verfügung, welche in die Boot-Komponenten integriert ist.

3.2.2 User Account Control

User Account Control sorgt dafür, dass auch Accounts mit Administrator-Rechten unter „normalen“ Benutzerprivilegien arbeiten, solange für die Ausführung der erforderlichen Arbeiten keine besonderen Rechte notwendig sind. Bei einem Übergang zu erweiterten Rechten wird vorgängig zu einer Bestätigung aufgefordert.

Mit User Account Control werden zwei Ziele verfolgt:

- Administrator-Accounts arbeiten nur dann mit erweiterten Rechten, wenn dies auch tatsächlich nötig ist.
- Die mit Windows XP in Firmennetzwerken ab und zu vorhandene „Unsitte“, dass auch Anwender mit Administrator-Privilegien arbeiten, wird sicherheitsmässig etwas entschärft.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Funktionsweise von UAC:
Meldet sich ein Standard-Benutzer in Windows an, wird für ihn eine neue Sitzung erstellt und ein Zugangstoken (Access Token) mit Basisrechten zugeteilt. Loggt sich hingegen ein Benutzer aus der Administratorgruppe ein, so werden dabei nun zwei verschiedene Access Token erstellt:

- Das erste Access Token erhält alle Rechte, wie sie dem Administrator zugeteilt werden.
- Das zweite (eingeschränkte) Access Token erhält nur die Rechte, welche auch ein Standardbenutzer erhalten würde. Benutzeranwendungen, wie beispielsweise der Windows Explorer, werden dann auch für den Administrator mit dem eingeschränkten Token gestartet. Benötigt eine Anwendung erweiterte Rechte, so werden über den UAC-Mechanismus passende Privilegien angefordert. Ein Bestätigungsdialog wird dabei angezeigt. Wird die Anforderung nun vom Administrator bestätigt, so wird der Prozess mit dem uneingeschränkten Token weitergeführt.

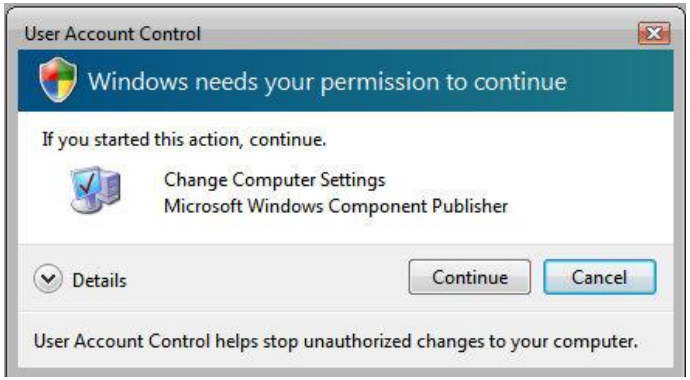
Hinweis: Der lokale built-in Administrator sowie der built-in Domain-Administrator Account sind von der UAC ausgenommen!

Im Secure Desktop Modus erfolgt die Abfrage der Benutzerdaten (Benutzername und Passwort) durch UAC so, dass der gesamte Bildschirm mit Ausnahme des Authorisierungsdialoges abgedunkelt und deaktiviert wird. Diese optische Kennzeichnung schützt vor Spoofing.

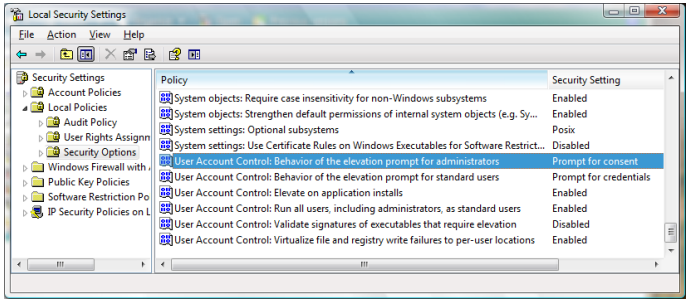
Zusätzlich zur beschriebenen Funktionalität mit zwei verschieden privilegierten Access Token sind im Umfeld von UAC noch weitere Sicherheitsfunktionalitäten eingeführt worden:

- Einzelne Aufgaben, die bis und mit Windows XP erweiterte Privilegien erforderten, können mittels Standard-Benutzerrechten ausgeführt werden. Durch diese zusätzlichen Privilegien des Standard-Benutzers soll der Versuchung, allgemeinen Benutzern administrative Rechte zu geben, widerstanden werden können:
  - Anzeigen der Systemuhr und des Kalenders
  - Ändern der Zeitzone
  - Ändern der Anzeigeeinstellungen
  - 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.
  - Die aufgelisteten default Privilegien können über Group Policies vom Standard Benutzer entfernt werden.
- UAC bietet eine Datei- und Registry-Virtualisierung an, so dass unpassend geschriebene Programme dennoch mit Standardrechten lauffähig sind.
- Einer Eingabeaufforderung, welche mit erweiterten Rechten läuft, wird das Präfix "Administrator" im Titel vorangestellt. Damit lässt sich dieses

Fenster einfach von Kommandozeilen unterscheiden, worin Standardrechte gelten.



Das Verhalten von UAC lässt sich über Group Policies steuern. Die folgende Abbildung zeigt die entsprechenden Einstellungsmöglichkeiten.

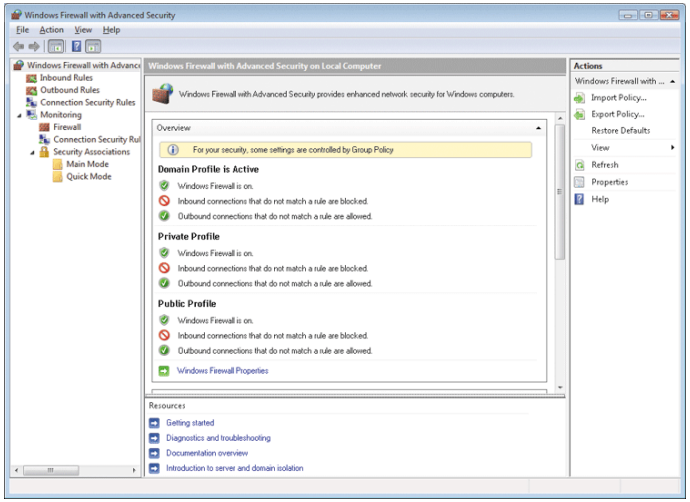


3.2.3 Windows Firewall with Advanced Security

Die bereits in Windows XP SP2 vorhandene Firewall wurde unter Vista erheblich erweitert:

- Auch für ausgehende Verbindungen lassen sich nun Regeln einrichten und Verkehr blocken.
- Neues User Interface zur Konfiguration der Firewall Regeln
- Voller Group Policy Support zur zentralen Konfiguration aller Firewall Einstellungen
- Integration von IPSec und Firewall

Die folgende Abbildung zeigt das User Interface von Vista WFAS.



Durch die Integration von Firewall und IPSec in Vista und Windows Server 2008 wird in dieser Betriebssystem-Kombination auch IPSec zwischen Client-PCs und Domain Controllern unterstützt. Microsoft empfiehlt in Netzen mit

erhöhtem Sicherheitsbedarf, diese Möglichkeit zu nutzen und alle Rechner einer Domäne nur noch per IPSec miteinander kommunizieren zu lassen. Rechnern, welche nicht zur Domäne gehören, wird dadurch bereits auf Stufe Netzwerk-protokoll die Kommunikation mit Domänenmitgliedern verunmöglicht. Zudem wird mittels flächendeckendem IPSec die Vertraulichkeit der übermittelten Daten gewährleistet. Unter dem Stichwort „Domain-Isolation“ wird dieses Netz-Sicherheitskonzept bei Microsoft vermarktet.

3.2.4 Neue ACLs in Vista

Im Bereich Access Control Lists bestehen in Windows XP sicherheitsmässig einige Schwachstellen. Beispiele dazu sind:

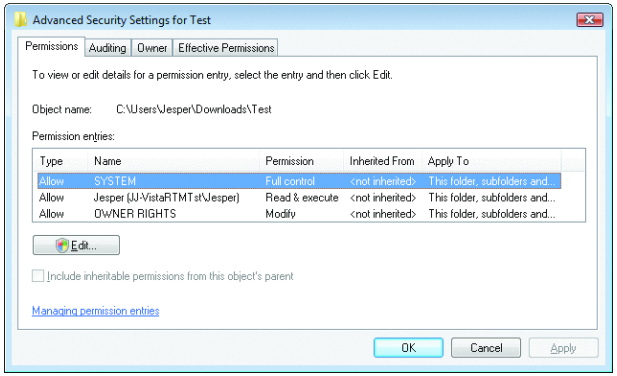
- Standard-Berechtigungen im Root-Ordner eines NTFS-Laufwerks sind mit Everyone Read und der Möglichkeit, dass Benutzer neue Ordner erstellen können, zu grosszügig ausgelegt.
- Bei einem Wechsel des Eigentümers (Change Ownership) werden die bestehenden Berechtigungen des Owners nicht übertragen.
- Ist man Owner eines NTFS-Objekts, hat man immer volle Rechte darauf.

Mit angepassten Standardrechten werden die genannten Mängel sowie weitere kleinere Security Schwachstellen in Vista gegenüber dem Vorgänger XP behoben:

- Der Standard Administrator Account mit RID 500 (Relative ID) ist per Default disabled. Er soll nur für spezielle Recovery-Funktonalitäten wieder aktiviert werden. Für alle täglichen Administrationsarbeiten sind persönliche Accounts mit Mitgliedschaft in „Domain Admins“ zu erstellen.
    - In Windows XP hat der built-in Administrator verschiedene spezielle Rechte, welche keinem anderer Account sonst zugewiesen sind. Mit Vista sind alle diese Spezialprivilegien entfernt worden, abgesehen von zwei Ausnahmen:
    - Ein Disabled Administrator Account kann in der Recovery-Konsole verwendet werden, wenn sonst kein anderes Admin-Konto mehr vorhanden ist.
    - Der built-in Administrator (lokal und Domäne) ist nicht der UAC (User Account Control) unterworfen und hat somit ständig volle Administrator-Rechte.
- Die Power User Gruppe ist in Windows Vista zwar weiterhin vorhanden, ihre speziellen Rechte wurden aber entfernt. Grund dafür ist, dass ein Profi mit wenig Aufwand sich selber aus einem Power User Account heraus zum Administrator heraufstufen konnte.
- Einführung von Berechtigungsvergaben für Dienste wie „TrustedInstaller“ (OS Installer Service). Im Fall des Installers lassen sich nun Rechte in NTFS direkt auf seinen Namen vergeben, um Systemdateien für ein Update durch diesen Service freizugeben.
- Help- und Support Accounts sind bei Neuinstallationen von Vista nicht mehr vorhanden.
- Einführung von neuen Network Location SIDs. Neben den bereits bekannten location Based SIDs wie NETWORK oder INTERACTIVE sind in Vista zusätzlich zwei weitere dazugekommen: DIALUP und INTERNET. Mit diesen sich selbstständig

verwaltenden Gruppen lassen sich Berechtigungen je nach Herkunft der Verbindung steuern.

- Im Vergleich zu Windows XP wurden zwei bedeutende Änderungen an den Rechten des Owners vorgenommen:
  - Gibt es für ein Objekt einen gültigen Eintrag in der Zugriffssteuerung (Access Control Entry, ACE), dann haben diese Rechte Vorrang vor den Rechten des Owners. Dies ist eine bedeutsame Änderung im Bereich File-System Security, da bisher dem Owner immer implizite Rechte auf das Objekt zugeordnet sind.
  - Die neue OWNER RIGHTS-SID kann dazu verwendet werden, durch den Admin einzuschränken, welche Funktionen der Eigentümer mit seinem Objekt ausführen kann. Die folgende Abbildung zeigt beispielsweise, dass dem Eigentümer der Datei „test“ nur die als „Modify“ zusammengefassten Rechte zugestanden werden.

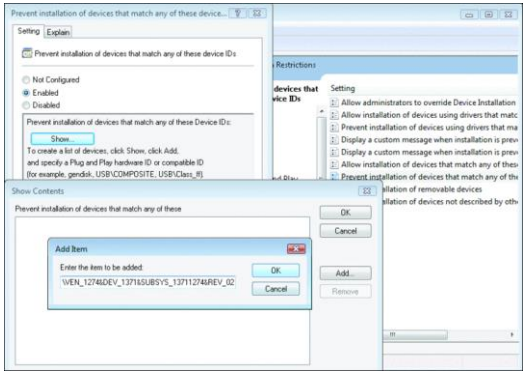


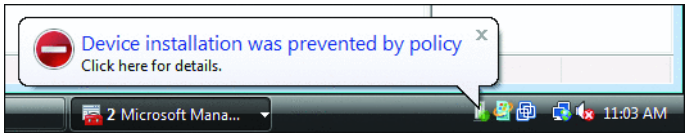
3.2.5 Hardware Restrictions mittels GPOs

Die reichlich vorhandenen mobilen Speichersysteme wie USB Sticks, Digitalkameras oder MP3 Player sind für jeden Sicherheitsverantwortlichen eine grössere Herausforderung. Wird ein solches Gerät an einem Firmen-PC angeschlossen, kann damit unter Umgehung von Firewalls und anderen Sicherheitsmechanismen Malware ins Netzwerk eingeschleust werden.

Mit Windows Vista und Group Policies lässt sich nun die Verwendung solcher Datenträger stark und gezielt eingrenzen. Mittels Hardware Restriction Polices lässt sich genau definieren, welche Gerätetypen an welchen Rechnern angeschlossen werden können. Dabei ist es auch möglich, nur einen einzelnen USB-Stick über seine Geräte-ID zu berechtigen.

Die folgende Abbildung zeigt die Group Policy Einstellung, über die ein spezifisches Gerät mittels seiner ID für den Anschluss an USB ausgeschlossen wird. Auf der nachfolgenden Abbildung ist die Meldung zu sehen, die Vista ausgibt, wenn das „verbotene Gerät“ mit USB verbunden wird.





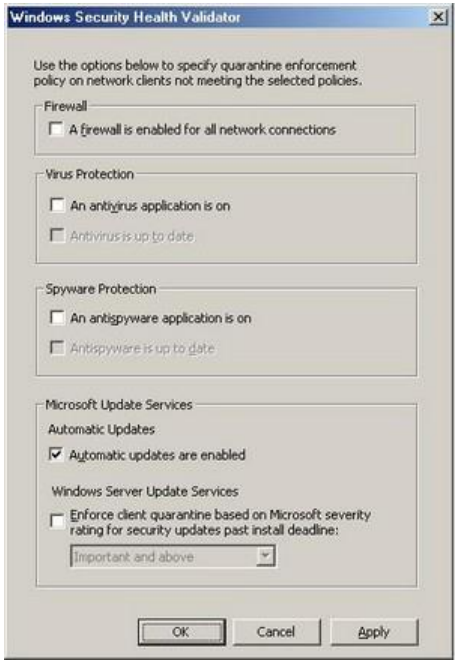
3.2.6 Windows Defender

Windows Defender ist eine Anti-Spyware, welche Microsoft von GIANT Software übernommen hat und nun in Vista standardmässig installiert und frei nutzbar ist. Für Windows XP ist dieser ebenfalls verfügbar.

3.2.7 Network Access Protection

Windows Vista ist vorbereitet für die mit Windows Server 2008 eingeführte Funktionalität „Network Access Protection NAP“. Damit wird sichergestellt, dass sich nur Client-PCs mit dem Firmennetzwerk verbinden können, die passende und aktuelle Sicherheitseinstellungen aufweisen. So lässt sich z.B. überprüfen, dass nur Clients mit eingeschalteter Firewall und aktuellem Virenschutz-Pattern mit dem LAN verbunden werden.

Die folgende Abbildung zeigt die Einstellungen im Dialog Windows SHV (Security Health Valitator) eines System Health Servers. Mit den abgebildeten Auswahlmöglichkeiten lässt sich festlegen, welche Bedingungen erfüllt sein müssen, damit uneingeschränkter Netzzugang gewährt wird.



3.2.8 Windows Service Hardening

Das Service Hardening schränkt kritische Windows Services so ein, dass abnormale Aktivitäten in File-System, Registry, Netzwerk oder mit anderen Systemressourcen nicht ausgeführt werden können. Damit lässt sich der Missbrauch dieser Dienste durch Malware wesentlich einschränken.

Beispielsweise lässt sich der RPC Service so konfigurieren, dass über diesen Dienst keine Systemdateien ersetzt oder Registry-Einträge modifiziert werden können.

Funktionsweise Service Hardening:

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

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

- Statt alle Dienste unter Local System mit weitgehenden Rechten zu betreiben lassen sich nun pro Service-Identität die standardmässigen Sicherheitsmechanismen von Windows nutzen (ACLs). Services können damit Ressourcen exklusiv zugeordnet werden, ohne dass andere Dienste darauf Zugriff haben.
- Unnötige Windows Privilegien lassen sich per Service ent¬fernen.
- Zuordnung eines write-restricted Access Token zu einem Service Prozess. Ein derart eingeschränktes Access Token verhindert ganz grundsätzlich schreibenden Zugriff aus dem Service-Prozess heraus auf das System.
- Diensten können Network Firewall Policies zugeordnet werden, die einem Dienst ausgehende Verbindungen nur auf die zugeordneten Rechner und Ressourcen ermöglichen. Die Firewall Policies sind dabei direkt gelinkt mit der „Per-service SID" des Dienstes.

Vorteil des Service Hardenings ist: 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.

3.2.9 IE 7.0 mit Vista Geschützter Modus

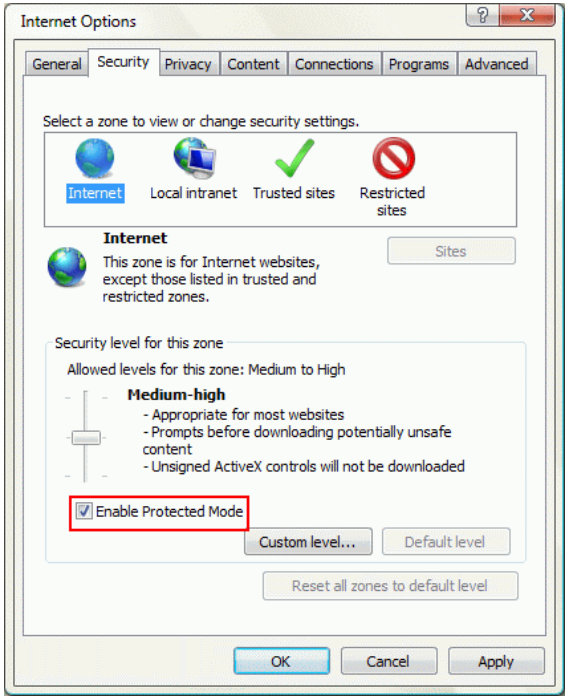
Unter Windows Vista ist in IE7.0 für das Browsen im Internet ein zusätzlicher Sicherheitsmechanismus vorhanden, genannt „Protected Mode". Dieser geschützte Modus schafft eine zusätzliche Hürde, welche die Anwender des Internets vor eindringender Malware schützt.

Der Protected Mode in IE7.0 nutzt drei grundlegende Sicherheitsfeatures, welche das Betriebssystem bereitstellt:

- User Account Control (UAC)
  Mit UAC wird das Prinzip "least Privilege" umsetzt.
- Mandatory Integrity Control (MIC)
  Ab Windows Vista lässt sich dem Access Token jedes Prozesses ein „Integrity Level" zuordnen. Die Stufen dieses Integrity Levels sind Low, Medium, High und System. Zu sichernde Daten wie Files und Registry-Keys können nun über einen zusätzlich vorhandenen mandantory ACE Eintrag vor dem Zugriff durch „Lower-Integrity-Applications" geschützt werden.
- User Interface Privilege Isolation (UIPI)
  UIPI blockiert den Zugriff aus Prozessen mit niedrigerem Integrity Wert auf solche mit einer höheren Stufe. So lässt sich beispielsweise verhindern, dass ein lower-integrity Prozess direkt mit einem higher-integrity Prozess kommuniziert und dabei versucht, schadhaften Code in ein Programm mit zusätzlichen Privilegien einzufügen (Bsp. Shatter Attack unter Windows).

IE7.0 läuft per Default im Protected Mode mit Integrity Stufe Low. Dies ist auch dann so, wenn der Benutzer als Administrator angemeldet ist. Einzige Ausnahme sind Verbindungen in die „Trusted Security Zone". Im Protec-

ted Mode sind UAC, MIC und UIPI aktiv. Weil der IE-Prozess im Protected Mode die Stufe Low-Integrity aufweist, sind damit weite Teile von File-System, Registry sowie andere Prozesse vor einem Zugriff geschützt. Auch Add-Ins wie ActiveX Controls oder Toolbars, die innerhalb des Prozesses funktionieren, sind diesen Restriktion ganz unterworfen.



Gewinnt nun beispielsweise ein Attacker die Kontrolle über den Prozess und kann darin Malicious Code einschleusen, ist dank Protected Mode sein Wirkungsradius trotzdem sehr gering, weil die Privilegien für den Zugriff auf Files, Startup Folder und System aus dem0 Low-Integrity-Prozess heraus nicht genügen.

IE7.0 hat getrennte Cache- und andere temporäre Speicherplätze für den Protected Mode sowie den Ausnahmefall „Trusted Security Zone“, so dass kein Übergang für Malicious Code zwischen den beiden Betriebsarten besteht. Einziges gemeinsames Element zwischen Protected Mode und „Trusted Security Zone“ sind die Favoriten-Listen.

3.2.10 Vista Jugendschutz

Ein besonderes Gebiet der Vista Security ist der neu darin eingebaute Jugendschutz (nicht in allen Versionen). Folgende Gebiete lassen sich damit kindergerecht steuern:

- Maximale Benutzungsdauer des PCs
- Erlaubte Spiele-Kategorien
- Freigegebene Web-Seiten

Der Vista Jugendschutz im Detail:

Die Eltern erstellen ein eingeschränktes Benutzerkonto (das dann selbstverständlich nicht Administrator sein sollte,...) für den Jugendlichen und aktivieren für diesen Benutzer die Jugendschutz-Einstellungen. Als Eigenschaften dieses Accounts lassen sich dann die folgenden Einstellungen vornehmen:

- Zeitlimits erlauben dem Kind, sich nur zu bestimmten Zeiten einzuloggen (inkl. automatisch ausloggen, wenn die Zeit vorbei ist). Dieser Wert lässt sich dann auch unterschiedlich pro Wochentag festlegen, z.B. am Samstagabend etwas länger.
- Altersschutz verhindert, dass die Kinder Games spielen, die für ihr Alter nicht geeignet sind. Man kann dabei aus verschiedenen Rating Systemen wählen, z.B. die im deutschsprachigen Raum ge-

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

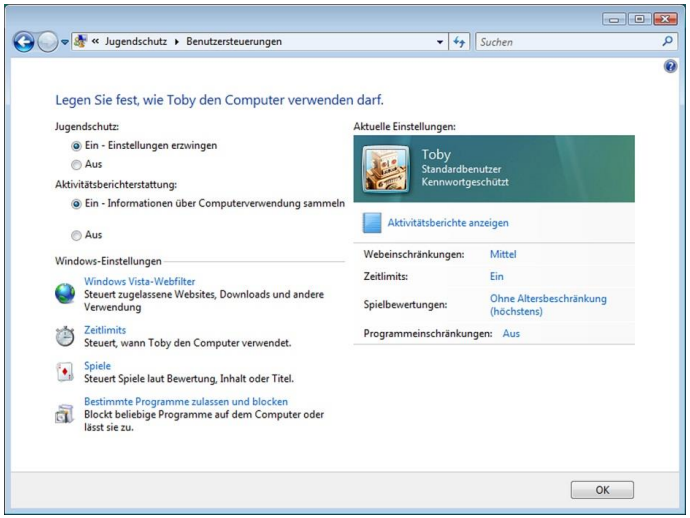
Telefon 052 320 91 20
Fax 052 320 91 21

bräuchlichen USK (Unterhaltungssoftware Selbstkontrolle).

- Der Webfilter setzt der Nutzung im Internet Grenzen. Es lassen sich beispielsweise die Sites definieren, worauf die Kinder Zugriff haben, Inhaltsfilter sind aktivierbar oder Downloads lassen sich freischalten.
- Programme können einzeln gesperrt oder umgekehrt einzeln freigegeben werden.

Vista ersetzt das Gespräch mit den Eltern nicht, aber es hilft :-)

Folgende Abbildung zeigt die grundlegenden Einstellungsmöglichkeiten des Jugendschutzes:

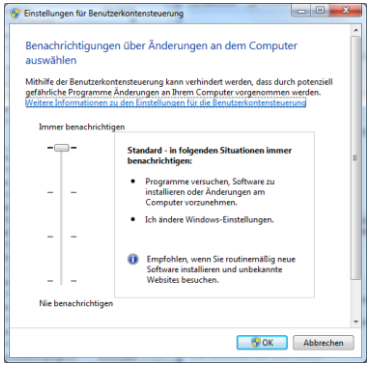


3.3 Windows 7 Security Übersicht

Am 22. Oktober 2009 wurde Windows 7 veröffentlicht. Für die einen ist es eine Revolution der Betriebssysteme, für die anderen «nur» ein grösseres Service Pack für Vista. So geteilt die Meinungen auch sind, unter der Haube hat sich im Bereich der Sicherheit einiges getan. Die nachfolgenden Erweiterungen oder Ergänzungen sollen dies aufzeigen. In Klammern finden Sie jeweils, in welcher Version von Windows 7 diese Funktion enthalten ist.

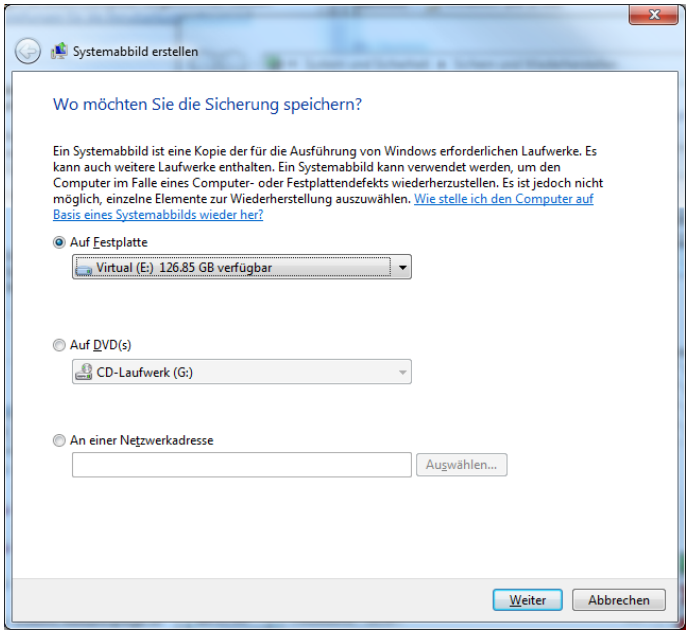
3.3.1 User Access Control UAC (alle)

Dies ist sicherlich die meist verpönte Erweiterung von Vista. Obwohl die Idee dieser Funktion hervorragend ist, nervt doch die ständige Nachfrage nach «Darf ich dies wirklich machen?» oder «Bist du dir wirklich, wirklich sicher?». Aus diesem Grund ist es bei Windows 7 möglich, aus vier Stufen zu wählen. Je weiter unten der Hebel ist, umso „unsicherer" wird der Betrieb. Viele Sicherheitsprofs empfehlen, infolge einer schlechten Umsetzung seitens Microsoft, den Hebel zuoberst zu lassen. Windows 7 verhält sich zwar dann fast wie Vista, aber der erhöhte Schutz ist dies wert.



3.3.2 Systemabbild erstellen (alle)

Mit Windows 7 ist es auf eine einfache Art und Weise möglich, ein Systemabbild (Image) zu erstellen. Sollte der Rechner zum Beispiel einmal infolge eines Festplattenfehlers nicht mehr starten, kann eine neue Festplatte eingebaut und das Image zurück gespielt werden. Als Ziel kann eine zweite Festplatte, eine andere Partition (nicht empfohlen!), ein DVD-Brenner oder eine Netzwerkadresse angegeben werden.

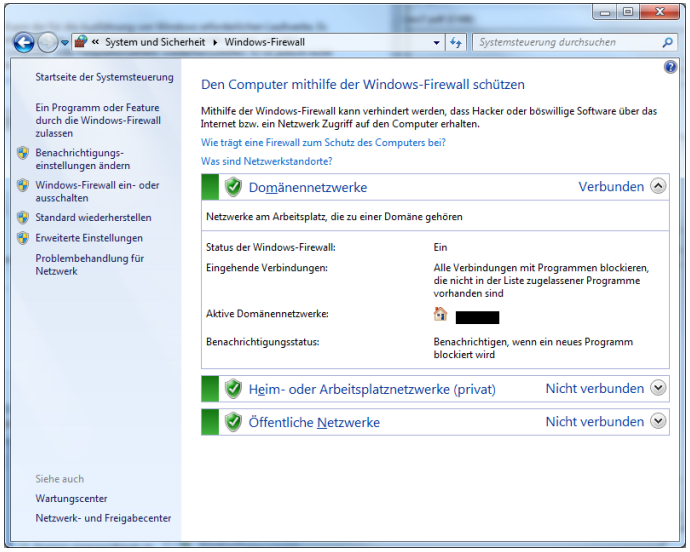


3.3.3 Safe Unlinking (alle)

Angriffe die direkt auf den Kernel, das heisst auf das Herz von Windows 7 zielen, sollen mit dieser Technologie praktisch keine Chance mehr haben. Vermieden werden damit sogenannte Buffer-Überläufe, mit welchen der geschützte Bereich verlassen und Manipulationen ausgeführt werden können. Eine Attacke ist damit mit deutlich mehr Aufwand verbunden.

3.3.4 Firewall (alle)

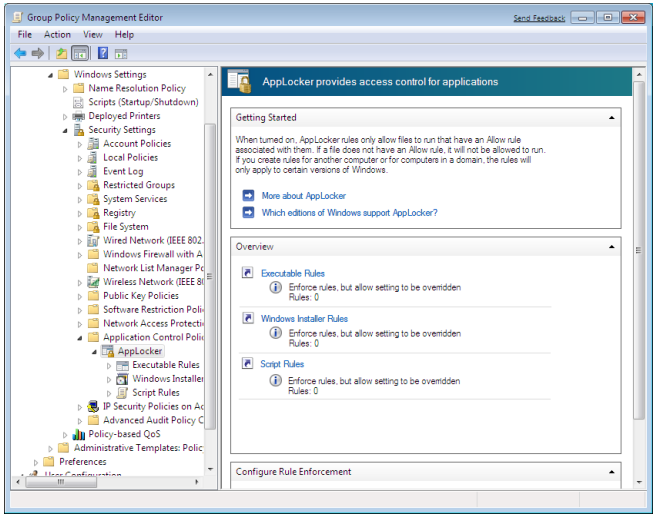
Überarbeitet wurde auch die Firewall. So ist es nun möglich, für verschiedene Profile (Domäne, Privat, Öffentlich) eigene Einstellungen im Detail vorzunehmen. Dies ermöglicht beispielsweise die vereinfachte Konfiguration eines Laptops. Im Büro ist die Firewall aus, unterwegs ist die Firewall komplett ein.



3.3.5 Applocker (Enterprise, Ultimate)

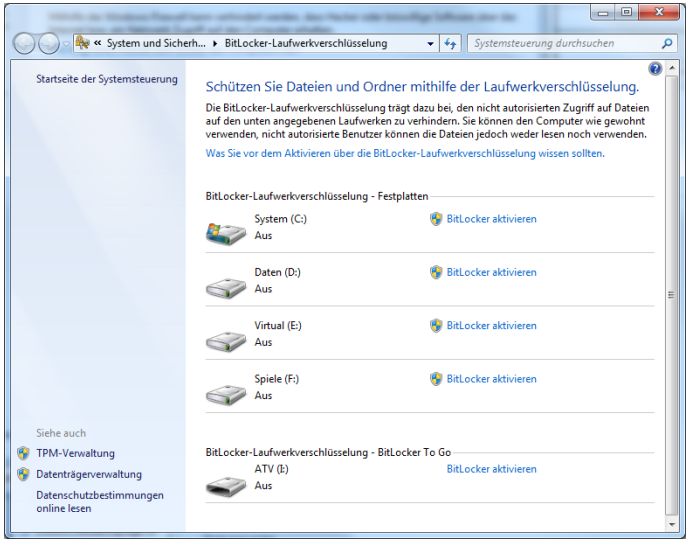
Mit dieser Funktion können Administratoren festlegen, welche Anwendungen im Firmennetzwerk ausgeführt werden dürfen. Diese Technologie ist zwar teilweise be-

reits bei Vista und XP vorhanden, jedoch kompliziert zu konfigurieren. Neben Angabe von Pfad und Programm ist es neu möglich, anhand von Zertifikaten, welche ein Softwarehersteller vergibt, eine Anwendung zu erlauben oder zu sperren. Weiter ist es möglich, diese Vorgaben via Gruppenrichtlinien im Unternehmen zu verteilen.



3.3.6 Bitlocker (Enterprise, Ultimate)

Das mit Vista eingeführte Bitlocker wurde stark erweitert. So wird Bitlocker nun bereits bei der Installation integriert. Das zeitaufwendige nachträgliche Installieren entfällt daher. Bei Windows 7 ist es nun möglich, einen Data Recovery Agent (Wiederherstellungsagent) zu bestimmen. Somit kann ein Administrator über einen Generalschlüssel alle im Unternehmen verschlüsselten Daten wiederherstellen. Dies macht dann Sinn, wenn der Mitarbeiter seinen Schlüssel verliert, erhöht aber gleichzeitig das Risiko, wenn der Schlüssel in falsche Hände kommt. Erweitert wurde mit Windows 7 auch die Steuerung über Gruppenrichtlinien. Hier sind zahlreiche Einstellungsmöglichkeiten dazugekommen.



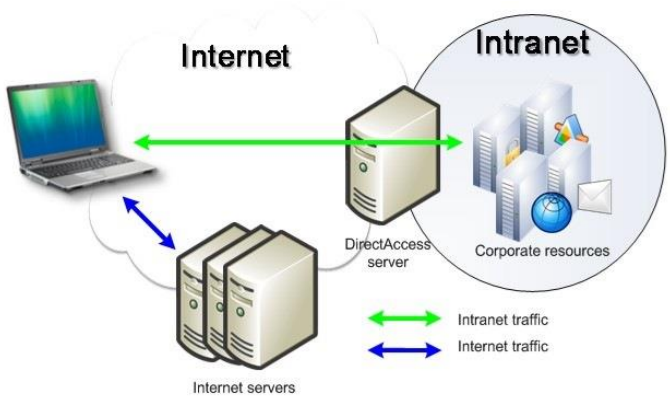
3.3.7 Bitlocker to go (Enterprise, Ultimate)

Bitlocker wird zur Verschlüsselung von Festplatten verwendet. Erst bei korrekter Authentifizierung wird der Zugriff darauf erlaubt. Mit Bitlocker to go wird diese Technologie auf USB-Sticks erweitert. Erst nach korrekter Eingabe wird der Zugriff auf die mobilen Daten erlaubt. Dazu sind aber, im Gegensatz zur Festplattenverschlüsselung, keine Administratorenrechte notwendig.

3.3.8 Direct Access (Enterprise, Ultimate)

In Kombination mit Windows Server 2008 R2 soll Direct Access das klassische VPN ablösen. Anstelle einer Einwahl über einen VPN-Client soll der Client automatisch

beim Starten Zugriff auf die Firmenserver erhalten. Der mobile Client ist daher immer erreichbar. Auch die gefürchtete Verbindung über NAT (Anpassen der Netzwerkadresse von einer privaten Adresse zu derjenigen des Providers) ist kein Problem. Verwendet wird dazu IPv6 als Transportmittel. Verschlüsselt werden die Datenpakete mit IPsec.



Windows 7 erhöht in vielen Bereichen die Sicherheit. Jedoch sind die meisten Erweiterungen den teureren Versionen vorbehalten. Möchte eine Firma diese Funktionen verwenden, muss zwingend die Enterprise oder die Ultimate Version eingesetzt werden. Die Professional Version bleibt hier aussen vor.

3.4 Windows 8 Security Übersicht

Seit Mitte Oktober 2012 ist das Betriebssystem Windows 8 von Microsoft da. Windows 8 bietet eine Vielzahl von Möglichkeiten und soll das Erscheinungsbild auf verschiedenen Plattformen vereinheitlichen. Dieser Bericht geht nicht auf die neue Oberfläche ein, sondern beleuchtet die neuen oder erweiterten Sicherheitsmöglichkeiten.

3.4.1 Malware-Schutz

In Microsoft Windows 7 war das Programm Defender bereits integriert, konnte aber nur Spyware erkennen. Neu ist ein vollwertiges Antivirenprogramm mit an Bord. Gleichzeitig soll die CPU und Memory Belastung sinken. Das Programm verhält sich sehr dezent und greift nur ein, wenn eine Malware entdeckt wird.

3.4.2 UEFI Schutz

Der Nachfolger des klassischen BIOS ist das UEFI. Microsoft erweitert UEFI um ein sicheres Booten des Rechners. Das heisst, dass das System bereits beim Start des Computers auf Computerviren untersucht wird. Zusätzlich ist es möglich, nur zertifizierte Firmware zu starten. Änderungen an der Firmware sind nur durch Programme mit gültigem Zertifikat möglich. Schadprogrammen und Rootkits soll dadurch Einhalt geboten werden. Der Nachteil ist, dass andere Betriebssysteme nicht mehr starten können, ausser diese sind ebenfalls zertifiziert.

3.4.3 ASLR

Hinter der Abkürzung ASLR versteckt sich (Address Space Layout Randomization, zufälliges Adressspeicher-Layout). Damit wird es Schadprogrammen erschwert, sich im Arbeitsspeicher auf bekannte Programme zu stürzen und diese zu verändern. Bei jedem Start eines Programmes landet dieses in einem anderen Adressspeicher.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

infonews.ch

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

3.4.4 Passwort

Neu ist es möglich, auch ein Bild als Passwort zu haben. Mit der von Smartphones gewohnten eigenen Bewegung kann mit der Maus das Betriebssystem entsperrt werden.

3.4.5 AppLocker

Wie bei der vorherigen Version ist es auch mit Windows 8 möglich, genau festzulegen, welche Programme gestartet oder gesperrt werden. Dies kann über verschiedene Attribute wie Anbieter, Produktreihe, Version, wie auch einzelnen Dateien geschehen. Die Vorgaben werden zentral via Gruppenrichtlinien definiert und auf die verbundenen Clients verteilt.

3.4.6 Bitlocker

Bitlocker ist neu auch für die Pro-Versionen verfügbar. Damit kann die gesamte Festplatte verschlüsselt werden. Ist ein entsprechender Chip (TPM) auf dem Motherboard vorhanden, findet das Booten wie gewohnt statt. Erst mit der bekannten Anmeldung wird die Festplatte entschlüsselt und der Benutzer kann auf seine Dateien zugreifen. Ein Muss für alle mobilen Geräte! Neu ist, dass in Firmennetzwerken trotzdem Wartungsarbeiten durchgeführt werden können, ohne dass der Benutzer anwesend sein muss.

3.4.7 Firewall

Ebenfalls erweitert wurde die integrierte Firewall. Sie bietet auch spezielle Schnittstellen für Drittprodukte. In Zusammenspiel mit dem Netzwerkzugriffsschutz (NAC) können individuelle Regeln erstellt werden. Als zusätzliches Highlight wurde IKEv2 integriert, was den Verbindungsaufbau von verschlüsselten IPsec Verbindungen massiv erleichtert.

3.4.8 Windows To Go

In der Enterprise Version ist es nun auch möglich, ein gesamtes Betriebssystem auf einen USB Stick zu kopieren und direkt von dort zu starten. Somit ist es möglich, sein eigenes Windows mit den vorkonfigurierten Einstellungen überall hin mitzunehmen.

Quellen:
http://www.techrepublic.com/blog/security/what-you-should-know-about-windows-8-security-features/7900
http://www.chip.de/news/Security-Duell-Windows-8-schlaegt-Windows-7_55153714.html
http://www.experto.de/b2b/computer/betriebssysteme/mehr-sicherheit-bei-windows-8-lohnt-sich-der-umstieg.html
http://www.welt.de/wirtschaft/webwelt/article110601084/Wie-sicher-ist-die-Virenabwehr-von-Windows-8.html

infonews.ch

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

3.5 Windows 8.1 Security Übersicht

Gemäss der offiziellen Microsoft Webseite kommen in der neuen Version Windows 8.1 folgende neue bzw. erweiterte Sicherheitsfunktionen zum Einsatz (Originaltext der Seite: http://technet.microsoft.com/en-us/windows/dn140266.aspx)

- **Remote Business Data Removal**
  Corporations now have more control over corporate content which can be marked as corporate, encrypted, and then be wiped when the relationship between the corporation and user has ended. Corporate data can now be identified as corporate vs. user, encrypted, and wiped on command using EAS or EAS + OMA-DM protocol. This capability is requires implementation in the client application and in the server application (Mail + Exchange Server). The client application determines if the wipe simply makes the data inaccessible or actually deletes it.
- **Improved Biometrics**
  All SKUs will include end to end biometric capabilities that enable authenticating with your biometric identity anywhere in Windows (Windows sign-in, remote access, User Account Control, etc.). Windows 8.1 will also be optimized for fingerprint based biometrics and will include a common fingerprint enrollment experience that will work with a variety of readers (touch, swipe). Modern readers are touch based rather than swipe and include liveliness detection that prevents spoofing (e.g.: silicon emulated fingerprints). Access to Windows Store Apps, functions within them, and certificate release can be gated based on verification of a user's biometric identity.
- **Pervasive Device Encryption**
  Device encryption previously found on Windows RT and Windows Phone 8 is now available in all editions of Windows. It is enabled out of the box and can be configured with additional BitLocker protection and management capability on the Pro and Enterprise SKUs. Consumer devices are automatically encrypted and protected when using a Microsoft account. Data on any Windows connected standby device is automatically protected (encrypted) with device encryption. Organizations that need to manage encryption can easily take add additional BitLocker protection options and manageability to these devices.
- **Improved Internet Explorer**
  Internet Explorer 11 improvements include faster page load times, side-by-side browsing of your sites, enhanced pinned site notifications, and app settings like favorites, tabs and settings sync across all your Windows 8.1 PCs. Internet Explorer 11 now includes capability that enables an antimalware solution to scan the input for a binary extension before it's passed onto the extension for execution
- **Malware Resistance**
  Windows Defender, Microsoft's free antivirus solution in Windows 8, will include network behavior monitoring to help detect and stop the execution of known and unknown malware. Internet Explorer will scan binary extensions (e.g. ActiveX) using the antimalware solution before potentially harmful code is executed.

- **Device Lockdown**
  With Assigned Access, a new feature offered in Windows 8.1 RT, Windows 8.1 Pro, and Windows 8.1 Enterprise, you can enable a single Windows Store application experience on the device. This can be things like a learning application for kids in an educational setting or a customer service application at a boutique, Assigned Access can ensure the device is delivering the intended experience. In our Windows Embedded 8.1 industry product, we deliver additional lockdown capabilities to meet the needs of industry devices like point of sale systems, ATMs, and digital signs.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21