Konfigurationsmaßnahmen für einen Windows 2000/XP-Rechner

In der heutigen vernetzten Zeit ist es wichtig, Rechnersysteme sicher zu konfigurieren, um Angreifern nur geringe Möglichkeiten zu geben, Schäden an der IT-Infrastruktur im Unternehmen oder am Privat-PC anzurichten. Es ist bewußt von "gering" die Rede, da es eine 100%ige Sicherheit nicht geben kann.

(1) Benutzerrechte verwenden

Arbeiten Sie unter Windows 2000/XP immer mit **Benutzerrechten** und **nie mit Administratorrechten**. Voraussetzung dafür ist, daß unbedingt **NTFS** als Dateisystem verwendet wird. Nur so können Sie weitesgehend verhindern, daß z.B. unerwünschte Software wie Dialer o.ä. auf ihr System gelangen kann und/oder Schäden am Systemverzeichnis entstehen.

- **Windows XP Home:** Sie sollten unbedingt überprüfen, ob für den Administrator-Account ein **Passwort** vergeben wurde. Standardmäßig ist dies nicht der Fall, sodaß jeder, der Zugriff auf den Rechner hat (auch über Netzwerk/Internet), sich als Administrator anmelden und so möglicherweise dem System Schaden zufügen kann.

(2) Betriebssystem ständig aktuell halten

Da täglich neue Sicherheitslücken in aktuellen Betriebssystemen entdeckt werden, ist es erforderlich, Windows 2000/XP immer auf dem aktuellen Stand zu halten. Dies geschieht am einfachsten mit Hilfe von Windows-Update . Neben Schwachstellen im Betriebssystem, die somit versucht werden, zu beheben, erhält man oft verbesserte Geräteunterstützung für aktuelle Hardware und/oder bessere Stabilität des Betriebssystems.

- Alle "**Wichtigen Updates & Service Packs**" installieren:
  => http://windowsupdate.microsoft.com
  Zur Überprüfung, welche sonstigen Patches noch fehlen:
  => http://hfnetchk.shavlik.com/
- **LSASS-Sicherheitsanfälligkeit**
  Der Mitte April 2004 erschienene Patch KB835732 schließt Sicherheitslücken im *Local Security Authority Subsystem (LSASS)* auf Windows NT4/2K/XP/2K3 Systemen, welche sonst durch BufferOverflows das Ausführen von Code über ein Netzwerk ermöglichten. Der Wurm "Sasser" nutzt diese Schwachstelle, um seinen Code auf befallenen Rechnern auszuführen. Daher ist es **dringend erforderlich**, den angebotenen Patch sofort zu installieren.

(4) Internet Explorer/Outlook Express nicht nutzen!

Von der Benutzung der bei Windows 2000/XP mitgelieferten Programme *"Internet Explorer"* sowie *"Outlook Express"* muß eindringlich **abgeraten** werden, da die konzeptionellen Schwächen (u.a. ActiveX, Nichteinhalten von Standards) sowie sicherheits-kritischen Fehler dieser Programme einfach inakzeptabel sind. Selbst das Zonenmodell bietet keinen ausreichenden Schutz mehr.

Als Alternativen wären die Suite **Mozilla** (Browser/Email/News) oder einzeln Firebird/Firefox (Browser) und Thunderbird (eMail/Newsgroup) sowie Opera zu empfehlen.

(5) Aktivieren der WindowsXP-Firewall

WindowsXP bringt eine *im TCP/IP stack integrierte Internet-Verbindungs-Firewall (ICF)* mit. Da sie bis SP1 nicht global aktiviert werden kann, muß dies für jede Verbindung einzeln erfolgen. Empfohlen wird, die XP-Firewall *vor der Verbindung zum Internet zu aktivieren.* Es sei aber noch anzumerken, das hierdurch kein umfassender, sondern nur ein geringer Schutz erreicht werden kann, welcher aber i.d.R. größer ist, als von Personal/Desktop Firewalls.

Überreicht durch: Entropia e.V., Steinstraße 23, 76133 Karlsruhe, http://www.entropia.de
Urheber: http://www.ntsvcfg.de, Thomas Mann, St. Petersb. Str. 29, 01069 Dresden