CHECKLISTE – SICHERES EINRICHTEN EINER WORKSTATION

PLANUNG

Machen Sie sich Gedanken über eine schlüssige Struktur des Dateisystems!

1.

Das stumpfe abspeichern von Daten und installieren vom Betriebssystem und Programmen auf einer Partition sollte unbedingt vermieden werden. Das Abspeichern der persönlichen Dateien sollte auf eine eigene Partition geschehen, da beispielsweise bei einer Neuinstallation des Systems, Daten die zum Beispiel auf persönlichen Ordnern auf der Systempartition abgelegt wurden verloren gehen können.

Überlegen Sie sich im Vorfeld, wie Sie Ihre Festplatte partitionieren (aufteilen) wollen. Verwenden sie ggf. eine zweite interne Festplatte oder lagern Sie Ihre persönlichen Daten auf einen Fileserver aus.

Entwickeln Sie ein angemessenes Backup Konzept, um Ihren Datenbestand zu schützen!

1.

Vor einem technischen Defekt ist niemand geschützt. Es kann jederzeit passieren, dass ein System ausfällt. In vielen Fällen hört man dann den Spruch: „Ich wollte gerade bevor der Bildschirm schwarz wurde eine Sicherung durchführen." Denken Sie daran: „Egal wie groß Ihr Unternehmen ist, ohne regelmäßige Datensicherung geht es heutzutage einfach nicht mehr!"

Überlegen Sie sich ein zuverlässiges Backupkonzept. Lagern Sie zum Beispiel Daten auf ein externes Speicher System aus. Für kleinere Unternehmen stellen zum Beispiel Network Attached Storage Systeme eine kostengünstige Alternative zu größeren Storage Lösungen. Eine weitere Möglichkeit wäre der Einsatz einer Kollaborationssoftware wie Team Drive, bei dem Sie Ihren Datenbestand, verschlüsselt im Netzwerk mit ihrem Team teilen können. Hierdurch erhöhen Sie die Verfügbarkeit Ihrer Daten und gewährleistet durch den Zugriff auf den gleichen Datenbestand die Integrität.

Deaktivieren Sie das automatische booten von externen Datenträgern und schützen Sie Ihr BIOS!

1. 2. 3.

Viele Motherboard Hersteller haben standartmäßig das automatische Booten vom CD-Rom Laufwerk oder anderen externen Datenträgern aktiviert, damit das Windows 7 Setup oder andere Betriebssysteme automatisch geladen werden können.

Deaktivieren Sie diese Funktion, nachdem Sie die Windows Installation durchgeführt haben! Dritte könnten ein Live System von einem externen Datenträger aus starten und so Zugriff auf Ihre Daten erlangen! Darüber hinaus sollten Sie ihr BIOS mit einem sicheren Kennwort versehen damit Unbefugte diese Optionen nicht wieder aktivieren können.

INSTALLATION

Nutzen Sie nur Installationsmedien die aus vertrauenswürdigen Quellen stammen!

2. 3.

Im Internet gibt es viele Möglichkeiten an Betriebssysteme oder Software zu gelangen, viele Quellen stellen jedoch rechts- sowie auch sicherheitskritische Gefahren dar.

Benutzen Sie nur Installationsmedien aus vertrauenswürdigen Quellen. Sollten sie unsicher sein, fragen Sie ihren Administrator.

Verwenden Sie nur Treiber aus vertrauenswürdigen Quellen!

2. 3.

Windows 7 beinhaltet eine riesengroße Treiberdatenbank, die das nachinstallieren von Gerätetreibern meistens überflüssig macht. Sollte ein Gerät jedoch nicht korrekt installiert sein, sollten Sie nicht den erst besten Treiber aus dem Internet installieren.

Nutzen Sie nur Treiber von zertifizierten Herstellerseiten oder vertrauenswürdigen Portalen. Sollten sie unsicher sein, fragen Sie ihren Administrator.

Installieren Sie eine Anti Viren Software!

1. 2. 3.

Nie war der Einsatz von AntiViren Software so unverzichtbar wie heute. In den Jahren wurde es immer einfacher Schadsoftware in Umlauf zu bringen, der Schaden den so etwas nach sich ziehen kann, ist den Verursachern meist nicht bewusst. Nutzen Sie die von Microsoft angebotene Antivirenlösung Microsoft Security Essentials.

Verfügbar unter http://www.microsoft.com/de-de/security_essentials/

INSTALLATION

Nutzen und konfigurieren Sie eine Firewall Lösung nach ihren Anforderungen!

2. 3.

Die Angriffe aus dem WWW um Zugriff auf Ihre Daten zu gelangen, sind ebenfalls in den letzten Jahren enorm angestiegen. Datendiebstahl ist gerade im Aspekt der Wirtschaftsspionage eine große Gefahr, vor der es sich zu schützen gilt.

Aktiviren die in Windows 7 integrierte Firewall und lassen Sie nur den Datenverkehr zu den Sie einwandfrei zuordnen können. Sollte die Firewall Sie vor nicht definierbaren Datenverkehr hinweisen, dann blocken Sie diesen und versuchen herauszufinden wodurch dieser zustande kommt.

KONFIGURATION

Richten Sie für jeden Benutzer der Arbeitsstation ein eigenes Konto ein!

2. 3.

Die Benutzung einer Arbeitsstation mit dem Standardtuser ist zu vermeiden, da dieser über komplette Administrationsrechte verfügt, die der User in den meisten Fällen gar nicht benötigt oder ihn zu einer potentiellen Sicherheitsgefährdung machen könnte.

Erstellen Sie für jeden Benutzer ein eigenes Konto mit Standardtrechten. So kann jeder User mit seinem eigenem Konto arbeiten und das Standardtkonto kann zu reinen Administration genutzt werden.

BETRIEB

Vergeben Sie nur sichere Passwörter und ändern diese regelmäßig!

3.

Eines der beliebtesten Passwörter der Welt ist 123456, sollte Ihnen dieses Passwort bekannt vorkommen, dann handeln Sie!

Beachten Sie die Grundlagen zur Wahl eines sicheren Passwortes. Mischen Sie große und kleine Buchstaben mit Zahlen und Sonderzeichen. Wählen Sie ein Passwort mit mindestens 8 Zeichen und verwenden Sie möglichst keine gängigen Wörter. Darüber hinaus sollten Sie in regelmäßigen Abständen ihr Kennwort abändern.

Halten Sie Ihr System auf dem neuesten Stand und überprüfen diesen regelmäßig!

2. 3.

Durch täglich entstehende neue Gefahren und das Aufdecken von Sicherheitslücken, arbeiten die Softwarehersteller mit Hochdruck daran, ihre Produkte durch Updates und Patches immer auf dem neuesten Sicherheitsstandardt zu halten.

Installieren Sie nach dem Aufsetzen ihrer Arbeitsstation die fehlende Windows Updates und aktivieren unter den Update Einstellungen das automatische Installieren der neuen Updates. Beachten Sie beim Systemstart oder dem Öffnen verschiedener Anwendungen Meldungen, die Ihnen ein Update vorschlagen und klicken diese nicht einfach weg. Nur ein aktuelles System ist auch ein sicheres System.

Kontrollieren Sie darüber hinaus selbstständig die Aktualität folgender Anwendungen (falls Installiert).

2. 3.

- *Adobe Reader*
- *Adobe Flash Player*
- *JAVA*
- *Mozilla Thunderbird (oder anderes eingesetzter E-Mail Client)*

1. **Verfügbarkeit** 2. **Integrität** 3. **Vertraulichkeit**