Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Sichere Nutzung von PCs unter Microsoft Windows 7

Empfehlungen für kleine Unternehmen und Selbstständige

1 Ausgangslage

Viele nützliche und wichtige Dienstleistungen wie Online-Banking, E-Commerce oder E-Government, werden heute über das Internet angeboten und genutzt. Auch in Zukunft wird sich die Anzahl der Online-Services noch weiter erhöhen. Hinzu kommt der verstärkte Einsatz mobiler Endgeräte, wie Smartphones und Tablets, mit denen diese Dienste auch unterwegs genutzt werden können. Im Geschäftsleben setzen viele Unternehmer und Selbständige dennoch weiterhin auf Personal Computer (PCs), die mit verschiedenen Betriebssystemen wie Microsoft Windows, Apple Mac OS X oder einer Linux-Variante ausgestattet sind.

2 Ziel

Die vorliegende BSI-Veröffentlichung zur Cyber-Sicherheit bietet Hilfestellungen für die weitestgehend sichere Konfiguration eines Windows-PCs zum Einsatz in kleinen Unternehmen. Diese Empfehlung behandelt das verbreitete Microsoft Windows 7.

Sinnvoll ist dabei zunächst die Betrachtung des Lebenszyklus eines Rechners:

- Entscheidungen vor der Installation
- Installation und erste Inbetriebnahme
- Regelmäßiger Betrieb
- Entsorgung des Systems

Mit wenigen Maßnahmen können PCs unter einem aktuellen Microsoft Windows 7 so abgesichert werden, dass eine weitgehend sichere Nutzung von Dienstleistungen über das Internet möglich ist.

3 Entscheidungen vor der Installation

Bereits bei der Anschaffung des Systems gibt es wichtige Aspekte, die Sie für einen späteren sicheren Betrieb eines PCs beachten sollten.

3.1 Hardware und Betriebssystem

Achten Sie auf die Verwendung möglichst aktueller Hardware. Um die von Windows bereitgestellten Sicherheitsmechanismen vollständig nutzen zu können, sollte der PC über eine 64-Bit-CPU (Prozessorarchitektur) verfügen und eine 64-Bit-Version des Betriebssystems eingesetzt werden.

3.2 Virenschutzprogramm

Für einen hinreichenden Schutz des Systems gegen Computer-Viren und andere Schadprogramme kommen verschiedene Varianten von Virenschutz-Software infrage. Diese unterscheiden sich in der Erkennungsleistung, Bedienungskomfort und Funktionsumfang, wie beispielsweise:

- zentralisiertes Management
- DNS-Schutzfilter
- Überwachung Ihrer Browser- und E-Mail-Aktivitäten auf Schadprogramme sowie
- erweiterte, verhaltensbasierte Erkennung von Schadsoftware

Sofern erforderlich, können Sie einige dieser zusätzlichen Funktionen auch mithilfe von kostenlosen Lösungen abdecken, z. B.:

- Browserfilter mit Phishing- und Malwareschutz in Google Chrome oder Mozilla Firefox bzw. mit dem SmartScreen-Filter des Microsoft Internet Explorer
- DNS-Schutzfilter mit OpenDNS Premium DNS (http://opendns.com/business-solutions/premium-dns/benefits, engl.).

Entscheiden Sie sich für ein Virenschutz-Programm, das in seinem Funktionsumfang Ihren Anforderungen entspricht und, basierend auf Ergebnissen unabhängiger Testinstitute, eine möglichst gute Erkennungsleistung aufweist. Betreiben Sie Ihr System nicht ohne aktuelles Virenschutzprogramm und beachten Sie unbedingt die regelmäßig notwendige Verlängerung der Lizenz (in der Regel nach 12 Monaten).

Der gleichzeitige Betrieb mehrerer Virenschutzlösungen auf einem System kann zu unvorhersehbaren Wechselwirkungen führen. Daher gilt: Haben Sie zu jedem Zeitpunkt immer nur ein Virenschutzprogramm installiert bzw. aktiviert!

Sofern das Virenschutzprogramm eine integrierte Firewall anbietet, sollte diese nicht aktiviert werden. Nach Einschätzung des BSI reicht die Windows-eigene Lösung im Normalfall aus (siehe Abschnitt Personal Firewall).

3.3 Backups

Um Sicherungskopien sowohl des Systems als auch Ihrer Daten zu erstellen, können Sie die in Windows 7 eingebaute Funktionalität verwenden (http://windows.microsoft.com/de-DE/windows7/products/features/backup-and-restore). Der Kauf einer gesonderten Backup-Software ist für Windows 7 im Allgemeinen nicht erforderlich. Im geschäftlichen Einsatz von Windows 7 ist gegebenenfalls zu prüfen, ob ein professionelles Sicherungssystem eingesetzt werden sollte, welches spezifische Anforderungen – beispielsweise an Revisionssicherheit, Reporting oder Disaster Recovery – gewährleisten kann.

3.4 Anwendungen

Prüfen Sie im Einzelfall, ob Sie wirklich jede installierte Anwendung zur Darstellung ihrer Dateien benötigen. Je weniger zusätzliche Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche des Systems.

Zur Darstellung von PDF-Dateien sollten Sie die jeweils aktuelle Version des kostenlosen Adobe Acrobat Readers (http://adobe.com/reader) nutzen, da diese über zusätzliche Sicherheitsmaßnahmen, wie eine „Sandbox“ (engl. übersetzt: „Sandkasten“, d. h. diese Software ist vom Rest des Systems abgeschirmt), verfügt.

Bei allen zusätzlichen Anwendungsprogrammen, die Sie etwa zur Bearbeitung von Fotos oder zum Komponieren und Abspielen von Musik nutzen, sollten Sie darauf achten, dass die Produkte mit einer Funktion zur automatischen Aktualisierung ausgestattet sind. In der Regel lässt sich dies unter dem Menüpunkt *Einstellungen* in der jeweiligen Software überprüfen und konfigurieren. Updates sollten idealerweise ohne Ihr Zutun automatisch im Hintergrund installiert werden. Verbreiteter sind Aktualisierungsfunktionen, die Sie bei verfügbaren Updates benachrichtigen. Die Installation sollten Sie stets zeitnah durchführen. Für die im Folgenden beispielhaft genannten Produkte aus dem Bereich Bürosoftware gibt es solche Aktualisierungsmechanismen, die standardmäßig nach der Installation bereits aktiviert sind:

- kostenlos: LibreOffice (http://www.libreoffice.org), OpenOffice (http://openoffice.org)
- kostenpflichtig: Microsoft Office (http://office.com)

4 Installation und erste Inbetriebnahme

Einen wichtigen Grundstein für die Systemsicherheit Ihres PCs können Sie bereits bei der Installation und ersten Inbetriebnahme des Rechners legen.

4.1 Installation aller vorhandenen Sicherheitsaktualisierungen

Üblicherweise ist Microsoft Windows 7 im Auslieferungszustand eines neu erworbenen PCs bereits vorinstalliert. Ist dies – etwa bei einem Gebrauchtgerät – nicht der Fall, so führen Sie zunächst eine vollständige Neuinstallation von Windows 7 durch.

Neben dem vorinstallierten Windows-Betriebssystem sind meist weitere Software-Produkte vorinstalliert. Diese sollten auf ihre Lizenzdauer, die unter Umständen zeitlich beschränkt ist, geprüft werden. Nicht benötigte Software-Produkte sollten deinstalliert werden.

Bei der ersten Inbetriebnahme eines Windows 7 Betriebssystems sollten Sie Ihren PC mit dem Internet verbinden und die von Microsoft angebotenen Software-Aktualisierungen herunterladen und installieren. Bei den Aktualisierungen von Microsoft über Windows-Update ist es dabei ausreichend die „wichtigen Updates“ zu installieren, um das Betriebssystem in einem geschützten Zustand zu halten. Das Häkchen bei „Empfohlene Updates auf die gleiche Weise wie wichtige Updates bereitstellen“ benötigen Sie hierfür nicht. Bitte achten Sie darauf, bei vorinstallierten PCs nicht nur Updates für Windows, sondern auch für andere möglicherweise installierte Microsoft-Produkte (z. B. Microsoft Office) herunterzuladen. Aktivieren Sie in diesem Zuge die Auto-Update-Funktion, sodass in Zukunft weitere Aktualisierungen automatisch heruntergeladen und installiert werden.

4.2 Benutzerkonten

Das bei der Installation von Windows 7 angelegte Benutzerkonto ist ein Administrator-Konto mit umfassenden Berechtigungen zur Systemkonfiguration. Achten Sie darauf, dass nur diejenigen Anwender Admin-Rechte erhalten, die diese Funktionalität auch benötigen und beherrschen. Legen Sie für die tägliche Verwendung des Windows-PCs auf jeden Fall zusätzlich ein Standard-Benutzerkonto an. Sollte der Windows-PC von mehreren Anwendern genutzt werden, sollten Sie für jeden Anwender ein eigenes Benutzerkonto anlegen.

Verwenden Sie neben dem Standard-Benutzerkonto, welches Sie für die tägliche Arbeit ver-

wenden, ein zusätzliches Benutzerkonto, um transaktionsbezogene Aktivitäten wie Online-Banking durchzuführen oder um kritische Daten online zu versenden.

4.3 Verschlüsselung der Festplatte

Falls Sie ein Notebook besitzen, das Sie auch unterwegs nutzen, sollten Sie unbedingt die Festplatte verschlüsseln, um Daten bei Verlust oder Diebstahl des Geräts zu schützen. Wenn Sie einen Desktop-PC besitzen, ist abzuwägen, ob ein möglicher Leistungsverlust Ihres Systems aufgrund der Verschlüsselung in einem angemessenen Verhältnis zum Schutz Ihrer Daten vor dem Zugriff unbefugter Dritter steht.

Das Betriebssystem Windows 7 verfügt in den Editionen *Ultimate* und *Enterprise* über die eingebaute Festplattenverschlüsselung *BitLocker Drive Encryption*, die eine Schlüsselverwaltung mithilfe eines TPM (Trusted Platform Module) durchführen kann. In diesem Fall wird der Kauf eines PCs mit TPM Version 1.2 empfohlen. Erstellen Sie nach der Festplattenverschlüsselung einen Wiederherstellungsschlüssel.

Wählen Sie hierfür ein sicheres Passwort, welches Sie sich gut einprägen können. Schreiben Sie sich dieses Passwort zusätzlich auf und bewahren Sie den Zettel räumlich getrennt von Ihrem PC an einem sicheren Ort auf. Hinweise zur Erstellung eines sicheren Passworts finden Sie bei auf der BSI-Webseite „BSI für Bürger[1]“.

Einen vergleichbaren Schutz können Sie durch die Verwendung der kostenfrei verfügbaren Lösung *VeraCrypt* (https://veracrypt.codeplex.com) erreichen. Erstellen Sie während des Verschlüsselungsvorgangs unbedingt eine „VeraCrypt Rescue Disk“. Diese hilft, wenn Probleme beim Entschlüsseln der Festplatte auftreten sollten.

4.4 Personal Firewall

Windows 7 besitzt eine integrierte Personal Firewall, die im Auslieferungszustand oder nach einer Neuinstallation bereits aktiviert ist. Achten Sie darauf, dass Sie diese Firewall in den Systemeinstellungen nicht versehentlich deaktivieren. Die Installation einer zusätzlichen Firewall ist nicht mehr erforderlich, da das System durch die von Windows 7 bereitgestellte Firewall hinreichend gegen Angriffe aus dem Netz geschützt wird.

4.5 Überprüfung auf Sicherheitsaktualisierungen

Um das Sicherheitsniveau des PCs konstant hoch zu halten, ist es erforderlich, alle Sicherheitsaktualisierungen nach deren Erscheinen zu installieren. Am einfachsten geschieht dies durch die Nutzung der sowohl im Betriebssystem (Microsoft-Update) als auch in den meisten gängigen Anwendungsprogrammen vorhandenen Auto-Update-Funktion.

4.6 Internet-Browser

Während der Installation bzw. der ersten Inbetriebnahme von Windows 7 werden Sie zur Auswahl eines Internet-Browsers aufgefordert.

Ihr Internet-Browser ist die zentrale Komponente für die Nutzung von Online-Angeboten im Internet und stellt somit eins der beliebtesten Ziele für Cyber-Angriffe dar. Verwenden Sie daher möglichst einen Browser mit Sandbox-Technologie. Konsequent umgesetzt wird dieser Schutz gegenwärtig z. B. von Google Chrome (https://www.google.com/chrome). Vergleichbare Mechanismen sind in anderen Browsern derzeit entweder schwächer implementiert oder noch nicht vorhanden.

1 https://www.bsi-fuer-buerger.de/Passwoerter

Vorteilhaft sind bei Google Chrome die kurzen Update-Intervalle sowie die Funktion zur automatischen Aktualisierung, die auch den integrierten Adobe Flash Player umfasst. Dadurch wird auch der Adobe Flash Player stets auf dem neuesten Stand gehalten. Wenn Sie ausschließlich Google Chrome verwenden, sollten Sie einen eventuell zusätzlich installierten Adobe Flash Player von Ihrem PC entfernen.

Eine weitverbreitete Angriffsform bildet der Versuch, Sie unter Vortäuschung falscher Tatsachen zum Download schädlicher Programme zu bewegen und diese in der Folge auf Ihrem PC auszuführen – diese Angriffstechnik wird auch als eine Form des „Social Engineering“ bezeichnet. Solche Angriffe, bei denen Sie bewusst einen Download starten, ohne sich eines Angriffs bewusst zu sein, versuchen die Browser-Hersteller mit Filtermechanismen abzuwehren. Mit Hilfe dieser Filter können auch viele sogenannte „Drive-by-Download“-Angriffe erfolgreich abgewehrt werden.

Um von diesem Schutz zu profitieren, sollten Sie bei Nutzung des Internet Explorers unbedingt den SmartScreen-Filter aktivieren. Eine vergleichbare Funktion steht auch im Mozilla Firefox und in Google Chrome mit dem Phishing- und Malwareschutz zur Verfügung. Alle drei Filter können jedoch aufgrund der hohen Dynamik neuer Webseiten mit schädlichen Inhalten allein keine Garantie gegen eine ungewollte Infektion mit Schadsoftware bieten.

4.7 E-Mail

Für die weitgehend sichere Nutzung von E-Mails ist es nicht erforderlich, zusätzliche Software zu installieren. E-Mail-Provider bieten Webmail-Zugänge an, die Sie über den Internet-Zugang mit Ihrem Browser nutzen können. Wichtig ist, auf eine verschlüsselte Verbindung (https) zum Webmail-Zugang zu achten, um von den Schutzmechanismen Ihres Browsers zu profitieren. Achten Sie darauf, dass die verschlüsselte Verbindung nicht nur für den Login-Vorgang, sondern während der gesamten Webmail-Nutzung aktiviert ist.

Falls Sie erweiterte Anforderungen an Komfort und Funktionalität bei der Arbeit mit E-Mails haben, sollten Sie einen modernen E-Mail-Client installieren und sicher konfigurieren.

Insbesondere ist dabei auf die Verwendung verschlüsselter Übertragungsprotokolle (POP3S, IMAPS, SMTPS) zu achten.

Verzichten Sie zudem auf die Darstellung und Erzeugung von E-Mails im HTML-Format. Die Anzeige externer Inhalte, wie Bilder in HTML-E-Mails, sollten Sie unbedingt deaktivieren, da über diese eine zusätzliche Möglichkeit zur Ausführung von Schadcode besteht.

4.8 Java-Laufzeitumgebung

Einige Anwendungen benötigen unter Umständen die Java-Laufzeitumgebung[2], die nicht in einer Standard-Installation von Windows 7 enthalten ist. Um die Angriffsfläche Ihres Systems zu reduzieren, sollten Sie Java nur dann installieren, wenn Ihre Anwendungsprogramme diese Laufzeitumgebung tatsächlich benötigen. Beim Start einer entsprechenden Anwendung wird im Normalfall auf das Fehlen von Java hingewiesen. Nach der Installation sollten Sie darauf achten, dass Java über die automatische Updatefunktion auf einem aktuellen Stand gehalten wird. Empfehlenswert ist die Änderung der Standardeinstellung auf eine tägliche Überprüfung.

Wenn Sie die Java-Laufzeitumgebung installieren müssen, schalten Sie trotzdem die Java-Unterstützung in den Einstellungen Ihres Webbrowsers ab. Sie können Java dann fallweise aktivieren, wenn es von einer vertrauenswürdigen Website benötigt wird. Alternativ können Sie das Dienstprogramm „Java-Einstellungen“ verwenden, um Java systemweit ein- und auszuschalten.

2 http://java.com/de

4.9 Erzeugung eines Datenträgers zur Systemreparatur

Die meisten neuen Systeme werden heute ohne Installationsmedien, wie beispielsweise Programm-CDs, ausgeliefert. Wenn dies bei Ihrem neuen PC der Fall ist, sollten Sie nach der ersten Inbetriebnahme einen Systemreparaturdatenträger („Rescue Disk“) erzeugen. Im Falle eines Defekts oder Absturzes können Sie mit diesem Ihr Windows 7-Betriebssystem wiederherstellen. Näheres dazu kann unter
http://windows.microsoft.com/de-DE/windows7/Create-a-system-repair-disc nachgelesen werden.

5 Regelmäßiger Betrieb

Beachten Sie im täglichen Umgang mit Ihrem PC die folgenden Ratschläge für einen sicheren Betrieb:

5.1 Sicherheitsaktualisierungen

Wenn Sie während der Installation eingestellt haben, dass sowohl das Betriebssystem als auch alle installierten Anwendungen automatische Updates durchführen, dann achten Sie auf entsprechende Hinweise im laufenden Betrieb.

In manchen Fällen werden Sie aufgefordert, die Installation von Updates zu bestätigen. Andere Softwareprodukte, wie beispielsweise der Browser Google Chrome, installieren die Updates selbsttätig und ohne eine weitere Nachfrage.

5.2 Backups

Bei einem defekten System ist die Gefahr eines unwiederbringlichen Verlusts Ihrer Daten sehr hoch. Regelmäßige Datensicherungen (Backups) auf externen Speichermedien, wie externen Festplatten, DVDs oder USB-Sticks, bieten Abhilfe.

Die integrierten Funktionen von Windows 7 können für regelmäßige Backups verwendet werden, siehe:
http://windows.microsoft.com/de-DE/windows7/products/features/backup-and-restore

Sie sollten mindestens einmal wöchentlich ein Backup Ihrer Daten anfertigen. Ein vollständiges Systemabbild ist seltener erforderlich, etwa nach größeren Updates oder Installationen von Betriebssystem oder Anwendungssoftware, mindestens jedoch einmal jährlich.

Bedenken Sie stets, dass Sie im Ernstfall alle Daten verlieren können, die im Zeitraum nach der letzten Sicherung erstellt wurden.

5.3 Passwörter

Der Zugang zu Online-Services im Internet erfolgt häufig mittels der Abfrage eines Benutzernamens und Passworts. Wenn Sie verschiedene Online-Dienste nutzen, verwenden Sie dafür jeweils unterschiedliche, komplexe Passwörter. Um sich diese besser behalten zu können, sollten Sie Merkhilfen verwenden, etwa die Anfangsbuchstaben eines längeren Satzes. Notieren Sie Ihre Passwörter zudem auf Zetteln und bewahren Sie diese räumlich getrennt von Ihrem Rechner an einem sicheren Ort auf. Hinweise zur Passwort-Sicherheit finden Sie bei auf der BSI-Webseite „BSI für Bürger“.

Die empfohlenen Internet-Browser besitzen integrierte Funktionen, mit denen Sie Kennwörter für besuchte Webseiten verwalten können.

Zudem sind kostenlose technische Lösungen zum Erzeugen und Verwalten komplexer Passwörter verfügbar, z. B. *keepass* (http://keepass.info).

5.4 Notfallmaßnahmen

Bereiten Sie sich auf die skizzierten potenziellen Notfälle vor und überlegen Sie sich Ihre Reaktion in folgenden Situationen:

- Der Rechner startet nicht mehr.
- Sie können keine Verbindung mehr mit dem Internet herstellen.
- Sie können sich nicht mehr in Ihrem E-Mail-Postfach anmelden.
- Sie bemerken eine nicht von Ihnen vorgenommene Überweisung von Ihrem Bankkonto.

Microsoft gibt Ihnen verschiedene Hilfestellungen für solche Situationen unter:

http://windows.microsoft.com/de-DE/windows7/help/system-repair-recovery

Wenn Sie das Gefühl haben, dass Sie in diesen Situationen unsicher reagieren werden oder keine angemessenen Antworten finden, dann suchen Sie sich schon jetzt einen vertrauenswürdigen Ansprechpartner, der Sie bei der Bewältigung unterstützen kann.

6 PC-Entsorgung

Wenn Sie Ihren PC eines Tages entsorgen möchten, dann sollten Sie sicherstellen, dass alle Daten auf der Festplatte vernichtet sind. Ein einfaches Löschen in den „Papierkorb“ oder im Windows Explorer ist hierfür nicht ausreichend.

Zur sicheren Löschung der Daten sollten Sie Ihren PC von einer in das CD-ROM-Laufwerk eingelegten Live-CD starten (z. B. http://www.ubuntu.com/download/ubuntu/download), dann die Festplatte in das gestartete Live-System einbinden und schließlich in der Kommandozeile mit der Eingabe des Befehls

```
dd if=/dev/urandom of=/dev/GERAETENAME
```

löschen. Dabei steht der GERAETENAME für die erste Festplatte, die meistens mit „hda“ oder „sda“ bezeichnet wird. Sie sollten auf die Angaben der Kommandozeile achten.

Sie können Ihre Festplatte auch mit *BitLocker Drive Encryption* oder *TrueCrypt*, siehe Verschlüsselung der Festplatte, verschlüsseln und lediglich das Schlüsselmaterial vernichten.

Um Ihre Festplatte alternativ unbrauchbar zu machen, können Sie diese ausbauen und physisch zerstören. Ein Verkauf einer gebrauchten Festplatte lohnt sich in den meisten Fällen nicht, wenn man den möglichen Erlös ins Verhältnis zum Wert Ihrer Daten setzt.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.