



# PCs unter Microsoft Windows

– für kleine Unternehmen und Selbstständige –

## Ausgangslage

Viele nützliche und wichtige Dienstleistungen – wie Online-Banking, E-Commerce, E-Government etc. – werden heute über das Internet genutzt. In Zukunft wird sich die Anzahl der angebotenen Online-Services weiter erhöhen. Hinzu kommt der verstärkte Einsatz neuer mobiler Endgeräte (Smartphones und Tablets), mit denen diese Dienstleistungen genutzt werden können. Derzeit werden jedoch noch überwiegend Personal Computer (PCs) mit verschiedenen Betriebssystemen wie Microsoft Windows, Apple Mac OS X oder einer Linux-Variante eingesetzt.

## Ziel

Die vorliegende BSI-Empfehlung zur Cyber-Sicherheit bietet Hilfestellungen für die Konfiguration eines Windows-PCs für den Einsatz in kleinen Unternehmen. Dabei wird in den folgenden Abschnitten der Lebenszyklus eines PCs betrachtet:

- Kauf des Systems
- Installation und erste Inbetriebnahme
- Regelmäßiger Betrieb
- Entsorgung des Systems.

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

## Kauf des Systems

### Hardware und Betriebssystem

Achten Sie beim Kauf eines PCs auf möglichst aktuelle Hardware mit der jeweils neuesten Version des Betriebssystems (derzeit: Microsoft Windows 7).

Um die von Microsoft bereitgestellten Sicherheitsmechanismen nutzen zu können, sollte das neue Gerät über eine 64-Bit-CPU verfügen.

Neben dem Windows-Betriebssystem sind auf neuen Systemen 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.

### Virenschutzprogramm

Die Wahl eines geeigneten Virenschutzprogramms ist bei Windows-basierten Systemen besonders wichtig.

Für einen hinreichenden Schutz des Systems gegen Computer-Viren und andere Schadprogramme kommen sowohl kostenlose als auch kostenpflichtige Varianten von Virenschutz-Software infrage. Letztere verfügen unter Umständen über mehr Bedienungskomfort.

Sofern zusätzliche Funktionen der kostenpflichtigen Lösungen wie beispielsweise

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

nicht benötigt werden, sind kostenlose Virenschutzprogramme ausreichend. Dazu zählen z.B. Microsoft Security Essentials (<http://microsoft.com/securityessentials>) welches bis zu fünf Lizenzen kostenlos erhältlich ist.

Dieses Virenschutzprogramm verfügt über eine deutschsprachige Benutzeroberfläche. Es lässt sich einfach in das Windows-Betriebssystem integrieren, nutzt automatische Updates und hat eine sehr gute Erkennungsrate.

Die oben genannten zusätzlichen Funktionen sind in meist komfortabler zu bedienenden, kostenpflichtigen Lösungen der großen Hersteller von Virenschutzprogrammen zu finden.

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 aktivieren.
- DNS-Schutzfilter mit OpenDNS Premium DNS (<http://opendns.com/business-solutions/premium-dns/benefits>, engl.)
- erweiterte, verhaltensbasierte Erkennung von Schadsoftware mit Threatfire (<http://threatfire.com>, engl.), welches problemlos mit einem weiteren Virenschutzprogramm betrieben werden kann.

Wenn Sie sich für eine kostenpflichtige Lösung eines Virenschutzprogramms entscheiden, beachten Sie unbedingt die notwendige Verlängerung der Lizenz (in der Regel nach 12 Monaten).

Betreiben Sie Ihr System nicht ohne aktuelles Virenschutzprogramm.

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

## Backups

Für Backups, also Sicherheitskopien sowohl des Systems als auch Ihrer Daten, können Sie die in Windows 7 eingebaute Funktionalität verwenden (<http://windows.microsoft.com/de-DE/windows7/products/features/backup-and-restore>).

Beschaffen Sie beim Kauf des PCs für die Erstellung dieser Backups zusätzlich externe Speichermedien (z.B. CD, DVD, externe Festplatte, USB-Stick etc.).

Der Kauf einer gesonderten Backup-Software ist unter Windows 7 nicht erforderlich.

## Internet-Provider

Die Auswahl eines geeigneten Internet-Providers sollte nicht nur vom Preis des Internetanschlusses abhängig sein, sondern auch andere Kriterien berücksichtigen. So sollten Sie beispielsweise darauf achten, dass Ihr Internet-Provider Sie aktiv vor Internet-Kriminalität zu schützen versucht. Insbesondere sollte Ihr Internet-Provider die Abwehr von Botnetzen – auch zu Ihrem eigenen Schutz – mit wirksamen Maßnahmen auf demselben Niveau betreiben wie Provider, die in der Anti-Botnet-Initiative (<https://botfrei.de/teilnehmer.html>) zusammengeschlossen sind.

## E-Mail-Provider

Neben der Nutzung von Angeboten im World Wide Web (WWW) ist eine der Hauptaufgaben von Internet-PCs der Empfang und Versand von E-Mails. Für diesen Zweck benötigen Sie einen geeigneten E-Mail-Provider.

Die Mindestanforderungen an Ihren E-Mail-Provider sind:

- Bereitstellung eines E-Mail-Virenfilters

- Schutz vor Spam-E-Mails
- durchgehend verschlüsselter Zugang, unabhängig davon ob Sie per Internet-Browser oder E-Mail-Programm auf Ihr Postfach zugreifen. Konkret bedeutet dies eine Unterstützung der Protokolle https, pop3s, imaps und smtps.

## Anwendungen

Orientiert an Ihrem individuellen Bedarf werden Sie mit der Zeit verschiedene Anwendungsprogramme beschaffen. Achten Sie dabei auf Produkte mit automatischer Aktualisierung (Auto-Update). Für die im Folgenden beispielhaft genannten Produkte im Bereich Bürosoftware gibt es solche Auto-Updates, die standardmäßig nach der Installation bereits aktiviert sind:

- kostenlos: OpenOffice (<http://openoffice.org/>)
- kostenpflichtig: Microsoft Office (<http://office.com>)

Gleiches gilt u.a. für den kostenlosen Adobe Reader (<http://adobe.com/reader>) zur Darstellung von PDF-Dateien. Nutzen Sie hier die Version Adobe Reader X, da diese über zusätzliche Sicherheitsmaßnahmen wie eine „Sandbox“ (engl. übersetzt: Sandkasten, d.h diese Software ist vom Rest des Systems abgeschirmt) verfügt.

Bei allen Anwendungsprogrammen sollten Sie darauf achten, dass die Sicherheitsaktualisierungen vom Software-Hersteller auch tatsächlich automatisch installiert werden, ohne dass Sie bei den einzelnen Aktualisierungen aktiv werden müssen.

## Neuer Personalausweis

Für die Nutzung der eID-Funktion (eID = elektronische Identität) des neuen Personalausweises ([https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/Personalausweis/personalausweis\\_node.html](https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/Personalausweis/personalausweis_node.html)) benötigen Sie die Software AusweisApp. Diese finden Sie zum Download auf dem AusweisApp-Portal (<https://www.ausweisapp.bund.de>). Ebenso benötigen Sie ein zertifiziertes Lesegerät. Hinweise auf entsprechende Geräte finden Sie ebenfalls auf dem Portal der AusweisApp.

Hinweise zum Thema neuer Personalausweis finden Sie unter <http://www.personalausweisportal.de> bei „BSI für Bürger“ und (<https://www.bsi-fuer-buerger.de/NeuerPersonalausweise>).

# Installation und erste Inbetriebnahme

## Installation aller vorhandenen Sicherheitsaktualisierungen

Abhängig vom Auslieferungszustand des von Ihnen erworbenen PCs mit Microsoft Windows müssen Sie entweder Windows 7 neu installieren oder Windows 7 ist bereits vorinstalliert.

Bei der Neuinstallation von Windows 7 sollten Sie bereits während der Installation alle verfügbaren Aktualisierungen herunterladen.

Bei der ersten Inbetriebnahme eines vorinstallierten Windows 7 Betriebssystems sollten Sie Ihren PC mit dem Internet verbinden und die von Microsoft angebotenen Software-Aktualisierungen herunterladen und installieren. Bitte achten Sie darauf, nicht nur Updates für Windows, sondern auch für andere möglicherweise installierten 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.

## Personal Firewall

Windows 7 besitzt eine integrierte Personal Firewall, die im Auslieferungszustand 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 über das Netz geschützt wird.

## Verschlüsselung der Festplatte

Falls Sie ein Notebook besitzen, sollten Sie unbedingt eine Festplattenverschlüsselung aktivieren, um Daten bei Verlust

oder Diebstahl Ihres Notebooks zu schützen. Wenn Sie einen Desktop-PC besitzen, sollten Sie sich überlegen, ob der Performanceverlust Ihres Systems aufgrund der Verschlüsselung im Verhältnis zum Schutz Ihrer Daten vor dem Zugriff unbefugter Dritter steht.

Nutzen Sie zur Verschlüsselung ein Passwort, welches Sie sich gut einprägen können. Schreiben Sie sich dieses Passwort zusätzlich auf und achten Sie unbedingt auf eine räumliche Trennung von Passwortzettel und PC. Bei Verlust dieses Passwortes können Sie nicht mehr auf Ihre Daten zugreifen. Hinweise zur Passwort-Sicherheit finden Sie bei „BSI für Bürger“ (<https://www.bsi-fuer-buerger.de/Passwoerter>).

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.

Einen vergleichbaren Schutz können Sie durch die Verwendung der kostenfrei verfügbaren Lösung TrueCrypt (<http://truecrypt.org>) erreichen. Erstellen Sie während des Verschlüsselungsvorgangs unbedingt eine „TrueCrypt Rescue Disk“. Diese hilft, wenn Probleme beim Entschlüsseln der Festplatte auftreten sollten.

## Java-Laufzeitumgebung

Einige Anwendungen benötigen die Java-Laufzeitumgebung (<http://java.com/de>). Um die Angriffsfläche Ihres Systems zu reduzieren, sollten Sie Java jedoch nur dann installieren, wenn Ihre Software tatsächlich diese Laufzeitumgebung benötigt.

Wenn Sie Java installiert haben, achten Sie auch hier auf die Aktivierung der automatischen Updatefunktion. Empfehlenswert ist die Änderung der Standardeinstellung auf eine tägliche Überprüfung.

## Überprüfung auf Sicherheitsaktualisierungen

Um das Sicherheitsniveau des PCs 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.

Um keine Aktualisierungen zu verpassen und so möglicherweise den PC angreifbar zu machen, empfiehlt sich die Installation eines speziellen Überwachungsprogramms wie Secunia Corporate Software Inspectors (CSI, [https://secunia.com/vulnerability\\_scanning](https://secunia.com/vulnerability_scanning)). Diese Software warnt Sie, sofern eine Aktualisierung verpasst wurde oder fehlgeschlagen ist.

## 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 WWW und stellt somit die hauptsächliche Angriffsfläche für Cyber-Angriffe dar. Verwenden Sie daher möglichst einen Browser mit Sandbox-Technologie. Konsequenterweise 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.

Durch den Einsatz von Google Chrome in Verbindung mit den anderen bereits aufgeführten Maßnahmen können Sie das Risiko eines erfolgreichen IT-Angriffs stark reduzieren.

Ebenso vorteilhaft ist in Google Chrome die Auto-Update-Funktion, die auch den integrierten Adobe Flash Player umfasst. Dadurch wird der Adobe Flash Player stets auf dem neuesten Stand gehalten.

## 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 wie 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 Inhalte eine zusätzliche Möglichkeit zur Ausführung von Schadcode besteht.

## 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 Datenträger Ihr Windows 7-Betriebssystem wiederherstellen. Näheres dazu kann unter <http://windows.microsoft.com/de-DE/windows7/Create-a-system-repair-disc> nachgelesen werden.

## Benutzerkonten

Legen Sie für jeden Anwender ein eigenes Benutzerkonto an. Achten Sie darauf, dass nur diejenigen Anwender administrative Aufgaben auf dem System wahrnehmen dürfen, die diese Funktionalität auch benötigen und beherrschen.

Schadprogramme nutzen inzwischen vermehrt Schwachstellen aus, die innerhalb des Benutzerkontos schadhafte Aktivitäten erlauben. Nutzen Sie daher neben Ihrem normalen Benutzerkonto für die tägliche Arbeit ein zweites Benutzerkonto, um transaktionsbezogene Online-Aktivitäten wie Online-Banking durchführen oder um sensible Informationen online zu versenden.

## Router und WLAN

Sollte der PC von mehreren Anwendern genutzt werden, sollten Sie für jeden Anwender ein eigenes Benutzerkonto anlegen. Im Gegensatz zu DSL-Modems sind bei Routern Firewall und Verschlüsselungsfunktionen integriert, die Sie aktivieren bzw. einstellen müssen. Ändern Sie unbedingt das voreingestellte Passwort des Routers.

Viele Router verfügen heute über die Möglichkeit, Ihren PC drahtlos mit dem Internet zu verbinden (WLAN). Deaktivieren Sie die WLAN-Funktionalität, wenn Sie diese nicht benötigen.

Wenn Sie WLAN nutzen möchten, muss die Verbindung sicher verschlüsselt werden. Der aktuelle Verschlüsselungsstandard ist WPA2. Ändern Sie nach der Inbetriebnahme das voreingestellte WLAN-Passwort Ihres Routers. Das WLAN-Passwort müssen Sie nur selten eingeben (jeweils bei der ersten Verbindung eines neuen Geräts mit dem Router), sodass Sie ohne Komforteinbuße ein zufälliges, komplexes und längeres Passwort wählen können. Notieren Sie sich dieses Passwort und bewahren Sie es an einem sicheren Ort und nicht im unmittelbaren räumlichen Umfeld des PCs auf.

# Regelmäßiger Betrieb

## Backups

Bei einem defekten System ist die Gefahr eines unwiederbringlichen Verlusts Ihrer Daten sehr hoch. Regelmäßige Datensicherungen (Backups) auf externen Speichermedien (z.B. DVDs oder externe Festplatte) bieten Abhilfe.

Die mitgelieferten 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.

## Sicherheitsaktualisierungen

Wenn Sie während der Installation darauf geachtet haben, dass sowohl das System als auch alle installierten Anwendungen ein Auto-Update durchführen, brauchen Sie hierfür während des laufenden Betriebs nichts mehr zu tun.

In manchen Fällen werden Sie aufgefordert, die Installation eines Updates zu bestätigen. Andere Softwareprodukte, wie z.B. der Browser Google Chrome, installieren die Updates ohne eine weitere Nachfrage.

Falls Sie den Secunia Corporate Software Inspector (CSI) installiert haben, achten Sie im laufenden Betrieb regelmäßig auf dessen Meldungen. Sollte eine Anwendung veraltet sein, installieren Sie eine aktuelle Version.

## Überblick über die allgemeine IT-Sicherheitslage

Verschaffen Sie sich regelmäßig einen Überblick über die aktuelle IT-Sicherheitslage, z.B. durch ein kostenloses Abonnement der BSI-Meldungen des Bürger-CERT-Newsletters (<https://www.buerger-cert.de>).

So werden Sie über aktuelle oder neuartige Angriffsmethoden informiert, wie z.B. Betrugsmaschen beim Kauf von Waren oder die betrügerische Erschleichung von Kreditkartendaten durch geschickt formulierte E-Mails.

## Online-Banking

Setzen Sie beim Online-Banking ein sicheres, modernes Verfahren zur Freigabe von Überweisungen ein. Derzeit ist dies das ChipTAN-Verfahren, bei dem die Freigabe der Überweisung durch ein spezielles Lesegerät in Verbindung mit Ihrer Bankkarte erfolgt. Mindestens jedoch sollten Sie das mTAN-Verfahren einsetzen. Hier wird die Transaktionsnummer (TAN) zur Freigabe der Überweisung per SMS auf Ihr Mobiltelefon übermittelt. Wichtig dabei ist, dass die SMS nicht mit dem Smartphone empfangen wird, von dem aus auch das Bankgeschäft durchgeführt wird. Dies würde die Trennung der Kanäle Internetverbindung und Mobiltelefonieverbindung aufheben. Falls Ihre Bank eines der erwähnten Verfahren anbietet, sollten Sie auf den Einsatz papiergebundener TAN-Verfahren (z.B. TAN und iTAN) verzichten.

## Kommunikation

Kommunikation über das Internet findet in den meisten Fällen per E-Mail statt. Gegenwärtig werden jedoch über 95 Prozent aller E-Mails unverschlüsselt versendet und können daher wie eine Postkarte von jedem Unberechtigten abgefangen, mitgelesen und verändert werden. Bei höheren Anforderungen an die Sicherheit und Vertraulichkeit von E-Mails besteht künftig die Möglichkeit, De-Mail zu verwenden (<https://www.bsi.bund.de/De-Mail>)

Der De-Mail-Postfach- und Versanddienst gewährleistet eine zuverlässige und vertrauliche Kommunikation. Durch spezielle Versand- und Eingangsbestätigungen wird die Kommunikation nachweisbar und nachvollziehbar. Zusätzlich werden die Nachrichten gemäß der gewählten Versandoptionen durch die De-Mail-Diensteanbieter gegen Veränderungen des Nachrichteninhalts und der sogenannten Metadaten (z.B. Absenderadresse, Versandzeit, Versandoptionen) geschützt.

Wenn Sie De-Mail nicht nutzen möchten, können Sie Ihre E-Mails auch mithilfe zusätzlicher Software selbst verschlüsseln und signieren, um individuell einen Schutz der Vertraulichkeit zu erreichen und die Authentizität und Integrität Ihrer E-Mails zu sichern. Die hierfür notwendigen Anwendungen, wie z.B. Gpg4win (GNU Privacy Guard for Windows, <http://gpg4win.de>) sind kostenfrei erhältlich.

## Passwörter

Der Zugang zu Online-Services im Internet erfolgt häufig über Benutzername und Passwort. Wenn Sie verschiedene Online-Dienste nutzen, dann verwenden Sie dafür jeweils unterschiedliche Passwörter. Um komplexe, nicht erratbare Passwörter zu nutzen, sollten Sie Merkhilfen verwenden, etwa die Anfangsbuchstaben eines längeren Satzes, oder Ihre Passwörter notieren und an einem sicheren Ort aufbewahren. Hinweise zur Passwort-Sicherheit finden Sie bei „BSI für Bürger“ (<https://www.bsi-fuer-buerger.de/Passwoerter>).

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

## Verhaltensweisen im Internet und in sozialen Netzwerken

Lassen Sie in der Online-Welt stets ein gesundes Misstrauen walten. Wenn Ihnen im Internet etwas merkwürdig erscheint, halten Sie inne und brechen Sie lieber einen Vorgang ab. Wenn Zweifel bestehen, geben Sie keine persönlichen

Daten oder gar Ihre Kreditkartennummer an.

In sozialen Netzwerken wie z.B. XING, Facebook oder Google+ sollten Sie sich immer so verhalten, wie Sie es auch in der realen Welt tun würden. Teilen Sie nur Informationen, die Sie auch sonst einem beliebigen anderen mitteilen würden.

Stellen Sie die Einstellungen zur Privatsphäre in sozialen Netzwerken nach Ihren Bedürfnissen so restriktiv wie möglich ein. Fragen Sie regelmäßig Freunde oder Familienmitglieder, wie Sie aus deren Sicht im virtuellen sozialen Netzwerk erscheinen. Versehentlich geteilte private Informationen werden in der Regel zunächst andere und nicht Sie selbst bemerken. Bitten Sie Ihr Umfeld, Sie darauf aufmerksam zu machen, wenn in Ihrem Profil im virtuellen sozialen Netzwerk etwas unpassend erscheint oder ungewöhnliche Online-Kommunikation erfolgt, die unter Umständen auf Spamnachrichten von Ihrem Profil schließen lässt.

## Notfallmaßnahmen

Bereiten Sie sich auf potentielle Notfälle vor und überlegen Sie sich Ihre Reaktion in folgenden Situationen:

- Das Virenschutzprogramm meldet eine Schadsoftware, ist aber nicht in der Lage, sie selbständig und automatisch zu entfernen
- Der Rechner startet nicht mehr
- Sie bemerken eine nicht von Ihnen vorgenommene Überweisung von Ihrem Konto
- Sie können sich nicht mehr in Ihr E-Mail-Postfach einloggen
- Sie können keine Verbindung mehr mit dem Internet herstellen

Microsoft gibt Ihnen für solche Situationen unter <http://windows.microsoft.com/de-DE/windows7/help/system-repair-recovery> verschiedene Hilfestellungen.

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

## PC-Entsorgung

Wenn Sie Ihren PC eines Tages entsorgen wollen, 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.

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

Wollen Sie die Festplatte dennoch erhalten, 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 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 Ausgaben der Kommandozeile achten. Sie können Ihre Festplatte auch mit BitLocker Drive Encryption oder TrueCrypt, siehe Verschlüsselung der Festplatte, verschlüsseln und lediglich das Schlüsselmaterial vernichten.

Mit den „BSI-Empfehlungen zur Cyber-Sicherheit“ veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik Lösungsvorschläge und Handlungsempfehlungen zur Cyber-Sicherheit. Die Inhalte werden mit größtmöglicher Sorgfalt und nach bestem Wissen und Gewissen recherchiert und zusammengestellt. Kommentare und Hinweise richten Sie bitte an: [cs-info@bsi.bund.de](mailto:cs-info@bsi.bund.de). Bitte beachten Sie, dass bei Systemkonfigurationen die Möglichkeit eines Datenverlustes besteht. Daher sollte vor jeder Systemänderung eine Datensicherung vorgenommen werden.