

DIE SPARTE DER WACHSTUMSBRANCHEN



Datensicherheit schafft Vorsprung

08 09 10 11

wko.at/ic

014 | 015 | 016 | 017 |
100 200 300 400

it-safe.at



IT Sicherheitshandbuch

FÜR MITARBEITER

4. Auflage



it-safe.at



IT Sicherheitshandbuch

FÜR MITARBEITER

it-safe.at ist eine Aktion der Bundessparte Information und Consulting in der WKÖ (BSIC).



4. Auflage

it-safe.at – das IT-Sicherheitsprojekt für KMU

Impressum

Medieninhaber/Verleger:

Wirtschaftskammer Österreich, Bundessparte Information und Consulting, 1045 Wien,
Wiedner Hauptstraße 63; ic@wko.at, <http://wko.at/ic>

4. Auflage, November 2011

Für den Inhalt verantwortlich: Mag. Bernhard Strilka, Mag. Jürgen Stöger, Friedrich Tuma,

MMag. Peter Pfeifhofer, Mag. Martina Ertler

Basislayout: Birgit Altrichter, Michaela Köck – geschmacksache.at

Grafische Umsetzung: www.designag.at

Druck: Ing. H. Gradwohl GmbH, A-3390 Melk

Alle Rechte vorbehalten. Nachdruck – auch auszugsweise – nur mit Quellenangabe und nach vorheriger Rücksprache.

Trotz sorgfältiger Prüfung sämtlicher Beiträge in dieser Broschüre sind Fehler nicht auszuschließen und die Richtigkeit des Inhalts ist daher ohne Gewähr. Eine Haftung der Autoren oder der Wirtschaftskammer Österreich ist daher ausgeschlossen.

Alle personenbezogenen Bezeichnungen beziehen sich auf beide Geschlechter.

INHALT

1. Sicherer Umgang mit Computern und Informationen	6
Sicherer Umgang mit personenbezogenen Daten	6
Clear Desk Policy	7
Datenträger und Papierdokumente richtig entsorgen	8
Sicherer Umgang mit mobilen IT-Geräten	9
Wechselmedien richtig verwenden	10
Social Engineering	11
2. Passwörter – richtig auswählen und verwalten	14
Die richtige Auswahl	14
Der richtige Umgang	15
Passwort-Manager verwenden	15
3. Sicher unterwegs im Internet	16
Vorsichtsmaßnahmen	16
Verschlüsselte Datenübertragung	18
4. E-Mails und Spam	20
Umgang mit unerwünschten Mails	20
Phishing-Mails	22
Gefälschte Absenderadressen	23
Sparsamer Einsatz der eigenen Mail-Adresse im Internet	23
5. Gefährliche Schadprogramme	24
Wie können Sie erkennen, dass Ihr PC infiziert ist?	24
Maßnahmen richtig setzen	25
Vireninfektion: Was tun?	27
6. Glossar	29



VORWORT

IT-SICHERHEIT GEHT ALLE AN!

Daten-Sicherheit im Allgemeinen und IT-Sicherheit im Speziellen sind wesentliche Kriterien für den Erfolg eines Unternehmens. Praktisch jedes Unternehmen ist heute mit der elektronischen Verarbeitung und Speicherung von Daten konfrontiert.

Die Bandbreite reicht von Kundendaten über die computerunterstützte Buchhaltung bis hin zu Programmierern oder Grafikern, die ihre Produkte und Dienstleistungen mit dem Computer erstellen. Andere Unternehmen wiederum sind mit Daten konfrontiert, die keinesfalls in die Hände Dritter fallen dürfen – sei es aus Gründen des Datenschutzes oder weil es sich um vertrauliche Unternehmensdaten zu neuen Produkten, Marktstudien oder Forschungsergebnissen handelt.

Daher ist es unerlässlich, dass Unternehmensdaten bestmöglich geschützt werden. Sowohl vor dem Versuch diese Daten auszuspionieren, als auch vor der Gefahr des Datenverlustes oder durch schadhafte Computersysteme.

MITARBEITER SIND GEFORDERT!

Gerade in kleineren Unternehmen, die nicht über eine eigene IT-Abteilung verfügen, sind die Mitarbeiter gefordert. Deswegen können auch Sie zur Sicherheit und somit zum wirtschaftlichen Erfolg Ihres Unternehmens entscheidend beitragen! Jede nicht ordnungsgemäße Datenspeicherung und jeder Computervirus, der durch einen privaten USB-Stick an Firewalls vorbei in das Unternehmensnetzwerk gelangt, kostet Ihrem Unternehmen Zeit und Geld. Das kann – je nach Unternehmensart und Umfang des Datenverlustes – existenzbedrohend sein.

Das vorliegende Handbuch gibt wertvolle Hinweise zu vielen Fragen der IT-Sicherheit und fordert zum Handeln auf: Sprechen Sie mit Ihrer IT-Abteilung, Ihren Kollegen oder Vorgesetzten über mögliche Schwachstellen in Ihrem Unternehmen und tragen Sie dadurch zu mehr Sicherheit bei.

KommR Hans-Jürgen Pollirer
Bundesspartenobmann

1. Sicherer Umgang mit Computern und Informationen

Informationen sind das Kapital jedes Unternehmens. Jeder Mitarbeiter muss über den Wert der Information Bescheid wissen. Der Missbrauch von sensiblen Daten kann Wettbewerbsnachteile, Umsatzeinbußen, Imageverluste oder rechtliche Probleme zur Folge haben. Daher ist es besonders wichtig, Informationen und Computer vor unberechtigter Verwendung zu schützen.

Heute verfügen die meisten Unternehmen bereits über technische Sicherheitsmechanismen, die den Zugriff auf sensible Daten regeln. Allerdings gibt es in vielen Fällen keine klaren Regelungen, wie Daten verwendet werden sollen (z.B. deren Weitergabe, Vervielfältigung, Verarbeitung).

SICHERER UMGANG MIT PERSONENBEZOGENEN DATEN

Der Umgang mit personenbezogenen Daten – diese können natürlichen, aber auch juristischen Personen zugeordnet werden – wird durch das österreichische Datenschutzgesetz (DSG 2000) geregelt. Dieses Gesetz stellt u.a. „sensible personenbezogene Daten“ (wie etwa Rasse und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder Sexualleben) unter besonderen Schutz. Weiters legt es fest, dass alle personenbezogenen Daten nur zu festgelegten Zwecken und aufgrund einer ausdrücklichen Anordnung des Dienstgebers verwendet und weitergegeben werden dürfen.

Bitte beachten Sie als Mitarbeiter folgende Hinweise:

- Sie müssen personenbezogene Daten, die Ihnen aufgrund Ihrer beruflichen Tätigkeit anvertraut wurden, geheim halten.
- Ihr Arbeitgeber muss Ihnen klare Anweisungen geben, auf welche Weise diese Daten verarbeitet bzw. an welche andere Personen oder Unternehmen sie weitergegeben werden dürfen. Jede andere Nutzung oder Weitergabe personenbezogener Daten ist nicht erlaubt.
- Der Arbeitgeber hat Sie über Ihre Pflichten nach dem DSG 2000 sowie den internen Vorschriften zu belehren.
- Nach dem Ausscheiden aus dem Betrieb oder dem Wechsel der Arbeitsstelle dürfen Sie personenbezogene Daten, die Ihnen beruflich zugänglich gemacht wurden, nicht weitergeben oder für andere Zwecke nutzen.

Verstöße gegen das Datenschutzgesetz werden mit hohen Geldstrafen für Ihr Unternehmen geahndet und können auch für Sie als Mitarbeiter arbeitsrechtliche Konsequenzen haben. Zusätzlich können Geschädigte Schadenersatz einklagen. Dazu kommt noch der Vertrauensverlust bei Kunden und Geschäftspartnern.

Es ist daher empfehlenswert, bei der Verwendung personenbezogener Daten besondere Vorsicht walten zu lassen. Sensible Daten müssen so gespeichert werden, dass sie für unberechtigte Personen nicht zugänglich sind.

CLEAR DESK POLICY

Clear Desk-Policy bedeutet, dass jeder Mitarbeiter seine vertraulichen Unterlagen bei Abwesenheit verschließen sollte, sodass keine unberechtigten Personen (Besucher, Reinigungspersonal, aber auch unbefugte Mitarbeiter etc.) Zugriff dazu haben. Dies gilt insbesondere für Großraumbüros oder Räume mit Publikumsverkehr.

Folgende Hinweise sollten unbedingt beachtet werden:

- Achten Sie darauf, dass Computerausdrucke oder Fehlkopien mit sensiblen Informationen nicht für Unbefugte frei zugänglich herumliegen, z.B. neben dem Drucker oder im Kopierer. Solche Dokumente müssen sicher verwahrt oder zuverlässig vernichtet werden.
- Versperren Sie Schriftstücke oder Datenträger mit vertraulichen Inhalten an einem sicheren Ort (Schreibtisch, versperrbare Kästen, Datenträgersafe)!
- Bewahren Sie unter keinen Umständen Passwortnotizen an Ihrem Arbeitsplatz auf (unter der Schreibtischunterlage, als Post-it am Bildschirm)!
- Sperren Sie Ihren Computer, wenn Sie Ihren Arbeitsplatz für längere Zeit verlassen (unter Windows bspw. „Windows-Taste + L“)! Unbeaufsichtigte, nicht gesperrte Computer sind ein hohes Sicherheitsrisiko. Unbefugte könnten so Zugang zu vertraulichen Daten erhalten.
- Konfigurieren Sie einen Bildschirmschoner, der sich nach maximal fünf Minuten aktiviert und nur durch Eingabe eines Passworts aufzuheben ist. Falls bereits ein passwortgeschützter Bildschirmschoner installiert ist, deaktivieren Sie ihn nicht!

DATENTRÄGER UND PAPIERDOKUMENTE RICHTIG ENTSORGEN

Computer, Datenträger und Papierdokumente mit vertraulichen oder personenbezogenen Inhalten, die defekt geworden sind oder nicht mehr benötigt werden, müssen auf sichere Art entsorgt werden. Sorglos weggeworfene Dokumente oder liegengelassene Kopien können ein ernstes Sicherheitsproblem darstellen, wenn diese Dokumente in falsche Hände geraten und missbräuchlich verwendet werden.

Bitte beachten Sie folgende Hinweise, wenn Sie Papierdokumente oder Datenträger wie z.B. USB-Sticks, Festplatten, CDs/DVDs, Mikrofiches und Sicherungsbänder entsorgen:

- Werfen Sie Datenträger auf keinen Fall in den Papierkorb! Sofern es sich um Inhalte handelt, die Außenstehenden nicht zugänglich gemacht werden sollen, müssen die Datenträger sicher entsorgt werden. Beachten Sie, dass diese Vorgehensweise auch bei Archivmaterial einzuhalten ist.
- Übergeben Sie die nicht mehr benötigten Datenträger einem Verantwortlichen Ihrer EDV-Abteilung bzw. einem eigens zu diesem Zweck bestimmten Verantwortlichen, der sie sicher entsorgt.
- Wenn Sie eine Festplatte verkaufen oder entsorgen wollen, müssen Sie vorher alle Inhalte mit einer geeigneten Löschoftware löschen. Das Formatieren der Festplatte ist nicht ausreichend! Verwenden Sie stattdessen ein Programm wie Eraser oder Wipedisk. Beide Programme sind kostenlos und bieten sichere Methoden zur endgültigen Bereinigung Ihrer Datenträger.
- USB-Sticks, Solid State-Disks und Speicherkarten können mit den oben genannten Programmen nicht sicher gelöscht werden! Derzeit gibt es keine in jedem Fall zuverlässige Methode zur vollständigen Löschung derartiger Medien. Die Datenträger dürfen daher nicht verkauft oder entsorgt werden, nachdem sie für das Speichern Ihrer sensiblen Daten verwendet wurden. Einzige Abhilfe ist derzeit, möglichst von Anfang an alle Daten auf diesen Speichermedien zu verschlüsseln: Ohne den Benutzerschlüssel bleiben sie – auch ohne Löschen – unlesbar.
- Optische Datenträger (CDs, DVDs) können nur „gelöscht“ werden, indem man sie physisch zerstört. Man kann sie also in möglichst kleine Teile zerbrechen oder die Beschichtung auf der Beschriftungsseite großflächig abkratzen. Meistens ist es aber einfacher, solche Medien zu sammeln und zum Shreddern an ein geeignetes Entsorgungsunternehmen zu übergeben. Beispiele für die korrekte Entsorgung finden Sie auf http://www.zendas.de/themen/vernichtung/beispiele_cddvd.html.

- Entsorgen Sie Papierdokumente mit sensiblen Informationen nicht mit dem Altpapier! Kleinere Mengen können Sie mit einem handelsüblichen Aktenvernichter (Shredder), größere Mengen über ein Entsorgungsunternehmen vernichten.
- Achten Sie darauf, dass bei Verlassen von Besprechungsräumen sämtliche sensiblen Informationen (z.B. auf Flipcharts) entfernt oder mitgenommen werden.
- Stellen Sie sicher, dass Sie nach dem Kopieren sämtliche Dokumente vom Kopiergerät entfernt haben und entsorgen Sie unbenötigte Dokumente mit vertraulichem Inhalt auf sichere Art.

SICHERER UMGANG MIT MOBILEN IT-GERÄTEN

Der Einsatz mobiler IT-Geräte (Notebooks, Smartphones, Tablet-PCs) birgt erhebliche Gefahren für das Unternehmen: Vertrauliche Unternehmensdaten werden außerhalb des Unternehmens gespeichert und verwendet. Portable Geräte sind für Diebe eine attraktive, leicht zu verkaufende Beute.

Wenn sie mobile IT-Geräte benutzen, sollten Sie Folgendes beachten:

- Sorgen Sie für eine diebstahlsichere Aufbewahrung Ihres Gerätes. Bewahren Sie es grundsätzlich nicht im Fahrzeug auf. Ist dies nicht zu vermeiden, decken Sie das Gerät ab oder schließen Sie es im Kofferraum ein.
- Lassen Sie das Gerät nicht unbeaufsichtigt und überlassen Sie es nicht anderen Personen! Sperren Sie es bei kurzen Arbeitspausen oder schalten Sie es ab. Stellen Sie es so ein, dass es nur nach Überwinden einer Zugriffsschutzfunktion (Passwort, PIN, Fingerprint, Erkennungsmuster, ...) bedient werden kann.
- Sorgen Sie für Sichtschutz, wenn Sie das Gerät in der Öffentlichkeit verwenden (z.B. am Flughafen) – das verhindert das Ausspähen von Unternehmensinformationen.
- Verschlüsseln Sie die Festplatteninhalte bzw. wichtige Dateien und verhindern Sie damit unbefugten Zugriff auf Firmendaten. Achten Sie auch bei Smartphones und Tablet-Computern auf die Verschlüsselung wichtiger Daten.

- Deaktivieren Sie alle nicht gerade benötigten Geräteschnittstellen (USB, WLAN, Infrarot, Bluetooth). Wenn diese Schnittstellen (z.B. WLAN für Internetverbindung) unbedingt notwendig sind, müssen entsprechende Schutzmaßnahmen (Personal Firewall, aktuelles Virenschutzprogramm usw.) vorgesehen werden.
- Schalten Sie den GPS-Empfänger auf Ihrem Smartphone immer ab, wenn er nicht gebraucht wird.
- Es gibt verschiedene Programme und Dienste, die es erlauben, alle Daten auf einem gestohlenen oder verlorenen Smartphone aus der Distanz zu löschen. Setzen Sie diese Apps unbedingt ein! Auch der Einsatz von Virenschutzprogrammen ist sehr zu empfehlen.
- Auf Smartphones oder Tablets, die Sie für berufliche Zwecke verwenden, dürfen Sie nie interne Sicherheitsmechanismen außer Kraft setzen (z.B. „Jailbreaks“ oder „Rooten“)! Durch diese Manipulationen entstehen zusätzliche Gefahrenquellen für die gespeicherten Unternehmensdaten.
- Installieren Sie nur Apps, die Ihnen als vertrauenswürdig und sicher bekannt sind! Fragen Sie im Zweifelsfall Ihre IT-Zuständigen oder recherchieren Sie im Internet, ob dazu Gefahren bekannt sind.
- Manche Apps fragen bei der Installation nach, auf welche Gerätefunktionen (WLAN, GPS-Empfänger, ...) sie zugreifen dürfen. In diesem Fall sollten Sie nur die unbedingt notwendigen Zugriffe zulassen.
- Bevor Sie ein Smartphone verkaufen, weitergeben oder entsorgen, müssen Sie sicherstellen, dass alle gespeicherten Daten gelöscht wurden. Am besten eignet sich dazu ein „Factory Reset“. Danach sollten Sie prüfen, ob noch Einstellungen oder Daten erhalten geblieben sind.
- Melden Sie einen Diebstahl oder Verlust sofort der IT-Abteilung! Möglicherweise müssen Fernzugänge zu Ihrem Unternehmen gesperrt oder Passwörter geändert werden, um unerlaubte Zugriffe zu unterbinden. Die rasche Meldung des Vorfalls kann helfen, weitere Sicherheitsverstöße zu verhindern.

WECHSELMEDIEN RICHTIG VERWENDEN

Wechselmedien sind externe Datenträger wie z.B. USB-Sticks, externe Festplatten, Fotospeicherkarten, CDs oder DVDs. Ihr Einsatz stellt für die meisten Unternehmen ein Sicherheitsrisiko dar: Einerseits können bei Missbrauch sensible Daten wie z.B. Kundenkarteien gelesen werden, andererseits können Programme mit Schadfunktionen auf Firmenrechner bzw. in das Firmennetzwerk eingeschleust werden.

Wenn Wechselmedien in Ihrem Unternehmen verwendet werden, sollten Sie folgende Hinweise (zusätzlich zu allfälligen Regelungen Ihres Unternehmens) beachten:

- Lassen Sie Wechseldatenträger wie z.B. USB-Sticks nie unbeaufsichtigt liegen!
- Setzen Sie unbedingt Verschlüsselungs- oder Sperrfunktionen ein! Häufig liegt dem USB-Stick eine Verschlüsselungssoftware bei, die gespeicherte Daten mittels Passwort schützt.
- Einige Verschlüsselungsprogramme bieten die Möglichkeit, den Inhalt des USB-Sticks nach mehrmaliger falscher Passwortheingabe automatisch zu löschen. Besonders bei sensiblen Inhalten sollten Sie diese Möglichkeit nutzen.
- Booten Sie Ihren Rechner nicht von einem Wechseldatenträger! Auch das Starten nicht freigegebener Programme von USB-Sticks (z.B.: Portable Versionen von Browsern oder E-Mail Clients) etc. ist unzulässig. Sie könnten damit Viren oder andere Schadsoftware in Ihren Computer einschleppen, die sich auf das gesamte Unternehmen ausbreiten können.

TIPP:

Die Installation privater Software kann einzelne PCs oder das gesamte Firmennetz bedrohen! Besonders Software aus dem Internet (z.B. Spiele oder „nützliche“ Tools) enthält oft Schadprogramme. Zudem könnte das Urheberrecht verletzt werden, wenn diese Programme nicht für den kommerziellen Einsatz lizenziert oder illegal kopiert wurden.

SOCIAL ENGINEERING

Social Engineering bezeichnet das Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten. Typisches Werkzeug des Social Engineers ist das Telefon. Persönliches Auftreten wird wegen des höheren Risikos zumeist gescheut, kommt aber ebenfalls vor.

STRATEGIE DES SOCIAL ENGINEERS

Ein „Social Engineer“ gibt sich beispielsweise als Mitarbeiter, wichtiger Kunde oder EDV-Techniker aus. Er täuscht sein Opfer durch firmeninternes Wissen oder Kenntnis des speziellen Fachjargons, die er sich zuvor durch Telefonate oder Insidergespräche erworben hat. Bei seinen Angriffen appelliert er als „gestresster Kollege“ an die Hilfsbereitschaft seiner Gesprächspartner oder droht als „Kunde“ mit dem Entzug eines Auftrages. Kommt er bei einem Mitarbeiter nicht an sein Ziel, wiederholt er den Angriff bei einem anderen.

Häufig verlaufen diese Angriffe mehrstufig:

- Durch gezielte Telefonate werden Insiderinformationen eingeholt, die an sich harmlos sind, deren Kenntnis dem Social Engineer aber hilft, seine Rolle überzeugend zu spielen.
- Oft wird über längere Zeit ein Vertrauensverhältnis aufgebaut, indem der Angreifer z.B. mehrere Telefonate mit seinem Opfer führt und unproblematische Anfragen stellt.
- Der eigentliche Angriff erfolgt nach diesen Recherchen: Wenn die Opfer den „Kollegen“ oder „Kunden“ gut zu kennen glauben, geht der Social Engineer zu seinem eigentlichen Ziel über – und bittet um den entscheidenden „Gefallen“.

Oft wird der Angriff vom Opfer nicht einmal registriert. Der Social Engineer bleibt unbemerkt und kann den Mitarbeiter bei anderer Gelegenheit erneut nach vertraulichen Informationen ausforschen.

WER BESONDERS GEFÄHRDET IST

Social Engineering-Attacken können sich gegen jeden Mitarbeiter richten. Am stärksten gefährdet sind

- neue Mitarbeiter, die mit den Verhältnissen noch nicht vertraut sind
- Mitarbeiter mit Kundenverkehr, da sie besonders kundenorientiert arbeiten. Hier finden sich außerdem häufig mehrere Mitarbeiter mit gleichen Zugriffsrechten, sodass der Social Engineer einen fehlgeschlagenen Angriff an einem anderen Opfer wiederholen kann.

MASSNAHMEN GEGEN SOCIAL ENGINEERING

Angriffe dieser Art können nie völlig unterbunden werden. Bitte beachten Sie aber folgende Vorsichtsmaßnahmen:

- Informieren Sie sich über den Wert und Vertraulichkeitsgrad der Informationen, zu denen Sie Zugang haben!
- Häufig ist Mitarbeitern infolge des dauernden Umgangs mit sensiblen Informationen nicht mehr bewusst, dass diese geheim sind. Auch fehlen oft klare Regelungen der Geschäftsführung. In jedem Unternehmen sollte – am besten in schriftlicher Form – festgelegt sein, welche Informationen vertraulich zu behandeln sind und welche weitergegeben werden dürfen. Sollte dies in Ihrem Unternehmen nicht der Fall sein, regen Sie eine solche Festlegung an oder klären Sie diesen Bereich zumindest mit Ihren Vorgesetzten.

- Bestehen Sie bei Anfragen zu vertraulichen oder geheimen Informationen auf schriftliche Form oder persönliche Vorsprache!
- Geben Sie über anonyme Kanäle (Telefon, E-Mail, Postfächer) grundsätzlich keine vertraulichen Informationen weiter!

Vertrauliche Informationen in diesem Sinn sind nicht nur Passwörter, Kontodaten oder ähnliche sensiblen Daten, sondern auch Firmeninterna wie z.B. Abläufe oder Fachwörter, die einem Angreifer helfen könnten.

Legen Sie im Vorhinein Methoden fest, wie Anfrager sicher authentifiziert werden können: Reicht z.B. die Kundennummer des Gesprächspartners oder ist ein zusätzliches Passwort nötig? So lässt sich Zeitdruck vermeiden, der gern als Hilfsmittel bei Social Engineering-Angriffen eingesetzt wird.

- Gibt der Gesprächspartner vor, Mitarbeiter eines Unternehmens zu sein, sollten Sie bei diesem Unternehmen anfragen, ob dieser Mitarbeiter existiert. Dazu muss aber die Telefonnummer aus öffentlichen Quellen (z.B. amtliches Telefonbuch) abgefragt werden – verwenden Sie nicht jene Telefonnummer, die der Anrufer angegeben hat.
- Wenn Sie sich bei einer Anfrage nicht sicher sind oder der Anfrager versucht, Sie unter Druck zu setzen, leiten Sie die Anfrage an den Vorgesetzten weiter! Einschüchterungsversuche dieser Art gehören zum Standardrepertoire des Social Engineering.

TIPP:

Besprechen Sie mit Ihren Kollegen auffällige oder unzulässige Anfragen und dokumentieren Sie diese Anfragen – so weiß man, ob der Anrufer es schon bei anderen Kollegen versucht hat. In solchen Gesprächen können auch neue Abwehrmethoden gefunden und ein Gefühl für den Wert der Firmeninformationen entwickelt werden.

2. Passwörter – richtig auswählen und verwalten

Passwörter dienen dem Schutz von IT-Geräten und Daten und verhindern unbefugte Zugriffe. Deswegen sind die richtige Auswahl und der richtige Umgang wichtig: Passwörter müssen komplex sein, um nicht erraten zu werden – aber auch einfach, damit sie nicht schriftlich notiert werden müssen.

DIE RICHTIGE AUSWAHL

Beachten Sie bei der Auswahl Ihres Passwortes:

- Ein gutes Passwort besteht aus mindestens acht verschiedenartigen Zeichen, im Idealfall aus Großbuchstaben, Kleinbuchstaben, Ziffern und/oder Sonderzeichen (Satzzeichen, Währungssymbole etc.).
- Niemals Namen, Vornamen, Geburtsdaten, Tel.-Durchwahlen, KFZ-Kennzeichen etc. verwenden. Diese werden von einem Angreifer zuerst ausprobiert.
- Verwenden Sie keine Begriffe aus einem Wörterbuch (auch nicht in einer anderen Sprache). Es gibt Programme, die Wortlisten mit mehreren tausend Begriffen sofort abrufen und so mögliche Passwörter finden. Auch sollten Sie Eigennamen, geografische Begriffe etc. vermeiden.
- Trivial-Passwörter (qwertz, aaaaa, 08/15, 4711 etc.) sind ebenfalls ungeeignet. Sie können bereits leicht beim Beobachten der Eingabe erkannt werden.

TIPP:

Bilden Sie Ihr Passwort aus den Wortanfängen und Satzzeichen einfacher Merksätze. Ein Satz wie „Ich kann mir nur ein Passwort merken!“ wird zum Passwort: „Ikmn1Pm!“.

DER RICHTIGE UMGANG

Geben Sie Ihre Passwörter – insbesondere das Passwort beim Anmelden am Computer – nicht an Mitarbeiter oder Vorgesetzte weiter. Sollte die Weitergabe unbedingt notwendig sein, ändern Sie Ihr Passwort anschließend sofort.

Setzen Sie für verschiedene Anmeldungen auch verschiedene Passwörter ein. Durch kleine Variationen – indem Sie z.B. zwei Buchstaben des Passworts ändern – ist dies leicht durchführbar.

Auf keinen Fall sollten Sie das gleiche Passwort für die Anmeldung am PC und Anmeldungen im Internet (z.B. das E-Mail-Konto beim Internet-Provider) verwenden. Wenn es in falsche Hände gerät, kann es gegen Ihr Unternehmen eingesetzt werden: Es gibt Fälle, wo Benutzer auf Webseiten gelockt und zur Angabe einer E-Mail-Adresse und eines Passworts aufgefordert wurden – in der (kriminellen) Hoffnung, dass das Opfer aus Bequemlichkeit keine unterschiedlichen Passwörter verwendet.

PASSWORT-MANAGER VERWENDEN

Mit einem Passwort-Manager können mehrere, unterschiedliche Passwörter verwaltet und durch ein einziges Master-Passwort geschützt werden. Dieses Passwort sollte zumindest die obigen Kriterien erfüllen. Manche dieser Programme generieren auch auf Knopfdruck sichere Passwörter.

Wenn Sie in Ihrem Internet-Browser einen integrierten Passwort-Manager verwenden, aktivieren Sie bitte die Option „Master Passwort“. Dann können Sie ein sicheres Master-Passwort wählen.

Eine Übersicht über kostenlose Passwort-Manager und Websites, auf denen Sie den Sicherheitsgrad Ihrer Passwörter testen können, erhalten Sie auf unserer Webseite: <http://www.it-safe.at>



3. Sicher unterwegs im Internet

Ebenso wie im realen Leben ist man auch im Internet mit Kriminellen und Betrügern konfrontiert. Es liegt in Ihrer eigenen Verantwortung als Benutzer, solche Bedrohungen zu erkennen und auch entsprechend darauf zu reagieren.

VORSICHTSMASSNAHMEN

Einige einfache Verhaltensregeln reichen aus, um typische Gefahren zu minimieren:

- Gebrauchen Sie Ihren gesunden Menschenverstand: Websites, die von bekannten und angesehenen Anbietern ins Netz gestellt werden, ist eher zu vertrauen als unbekanntem Seiten.
- Websites, die mit dem Download kostenloser Zusatzsoftware oder unseriösen Gewinnspielen locken, ist grundsätzlich zu misstrauen. Natürlich gibt es auch seriöse Anbieter von kostenlosen Free- und Shareware-Programmen im Internet. Sollten Sie sich aber nicht sicher sein, fragen Sie bei Ihrem Vorgesetzten oder EDV-Verantwortlichen nach.
- Vor dem Download von Zusatzprogrammen – auch bei scheinbar ungefährlichen Dingen wie Bildschirmschonern, Klingeltönen oder Mauszeigern – ist grundsätzlich die Zustimmung des Vorgesetzten oder EDV-Verantwortlichen einzuholen.
- Das Herunterladen von Dateien kann – abgesehen von der Gefahr des Einschleppens von Schadsoftware – auch zu lizenz- und urheberrechtlichen Problemen führen. Das gilt auch für Software, die nicht installiert oder ausgeführt wurde und nur auf dem Bürorechner gespeichert ist. Holen Sie daher vorher die Zustimmung des Vorgesetzten oder des EDV-Verantwortlichen ein.
- Meiden Sie Hackerseiten und solche, auf denen kommerzielle Software, möglicherweise in gecrackter Form, zum Download angeboten wird (sogenannte „Warez“-Seiten). Die Wahrscheinlichkeit, dadurch Schadsoftware auf den Computer zu laden, ist naturgemäß deutlich höher als beim Aufsuchen der Website einer Bank oder eines bekannten Unternehmens. „Verdächtige“ Seiten sollten Sie am besten gar nicht aufrufen.
- Rufen Sie keine Websites mit pornografischen, gewaltverherrlichenden oder strafrechtlich bedenklichen Inhalten auf. Das kann gravierende rechtliche Probleme – auch für Ihr Unternehmen – nach sich ziehen.

Bei der Nutzung von Sozialen Netzwerken sind besondere Vorsichtsmaßnahmen zu berücksichtigen:

Soziale Netzwerke, wie Facebook, Xing oder MySpace, erfreuen sich immer größerer Beliebtheit. Immer mehr Plattformen bieten Netzwerke für spezifische Themenbereiche an. Leider haben aber auch Kriminelle diese Plattformen entdeckt und nutzen sie für ihre Zwecke. Daher sind mit der Benutzung sozialer Netzwerke auch Risiken verbunden. Neben dem Diebstahl persönlicher Daten und dem Verbreiten von Spam oder Schadsoftware sammeln immer mehr Angreifer Informationen, die Nutzer der Plattformen über sich und ihr Umfeld preisgeben. Diese Informationen erlauben es, gezielte Angriffe auf Unternehmen durchzuführen, indem etwa personalisierte Phishing-Mails an Geschäftsführung, Vertrieb oder Buchhaltung verschickt werden oder maßgeschneiderte Schadsoftware Firmengeheimnisse ausspioniert oder zerstört.

Bedenken Sie auch mögliche arbeitsrechtliche Konsequenzen: Wenn Sie vertrauliche Informationen des Unternehmens preisgeben oder das Unternehmen durch Ihre Aussagen in Verruf bringen, kann dies als Verletzung Ihrer Treuepflicht gedeutet und im schlimmsten Fall mit Entlassung geahndet werden. Wenn Sie das Sicherheitsrisiko bei der Nutzung sozialer Netzwerke minimieren wollen, sollten Sie einige grundlegende Sicherheitshinweise beachten:

- Informieren Sie sich, ob in Ihrem Unternehmen die Nutzung sozialer Netzwerke während der Arbeitszeit gestattet ist.
- Das Netz vergisst nie! Denken Sie immer daran, dass Informationen, die Sie auf sozialen Netzwerken preisgeben, öffentlich einsehbar sind und kaum oder gar nicht mehr gelöscht werden können.
- Vermeiden Sie es, vertrauliche Informationen über Ihr Unternehmen, Ihre berufliche Rolle oder Ihre geschäftliche Tätigkeit zu veröffentlichen. Alle diese Daten können von Angreifern genutzt werden, um Sicherheitsvorkehrungen zu umgehen.
- Unterscheiden Sie zwischen Ihrem geschäftlichen und Ihrem privaten Ich und verwenden Sie unterschiedliche Plattformen oder Profile. Private Daten haben auf Geschäftsprofilen nichts verloren und umgekehrt. Damit erschweren Sie potenziellen Angreifern den Missbrauch Ihrer Daten und schützen zudem noch Ihre Privatsphäre.
- Prüfen Sie unbedingt die Identität der anfragenden Person, bevor Sie diese zu Ihrem Netzwerk hinzufügen.
- Nutzen Sie die Sicherheits- und Datenschutzooptionen, die vom Plattformanbieter zur Verfügung gestellt werden und schränken Sie den Zugang zu Ihrem Profil ein. Kontrollieren Sie regelmäßig, ob der Betreiber Veränderungen vorgenommen hat, die unerwünschte Zugriffe ermöglichen.
- Vorsicht bei externen Links: Bedenken Sie, dass soziale Netzwerke oft genutzt werden, um Schadsoftware zu verbreiten.
- Verwenden Sie auch in sozialen Netzwerken ein sicheres Passwort!

VERSCHLÜSSELTE DATENÜBERTRAGUNG

Die Datenübertragung zwischen Servern im Internet und Ihrem PC erfolgt im Normalfall unverschlüsselt. Daher können übertragene Daten von Personen mit entsprechenden Zugangsmöglichkeiten problemlos abgehört oder manipuliert werden. Um dies bei der Übertragung sensibler Daten zu verhindern, wurde das Protokoll HTTPS mit dem Verschlüsselungsprotokoll TLS/SSL entwickelt. Dadurch sind folgende Sicherheitsmerkmale gewährleistet:

- Die übertragenen Daten werden verschlüsselt und sind für Außenstehende nicht lesbar.
- Die Identität des Webservers, der die Daten verarbeitet, wird anhand eines digitalen Zertifikats geprüft.
- Die übertragenen Daten werden durch verschiedene Rechenverfahren geprüft und vor Manipulationen geschützt.

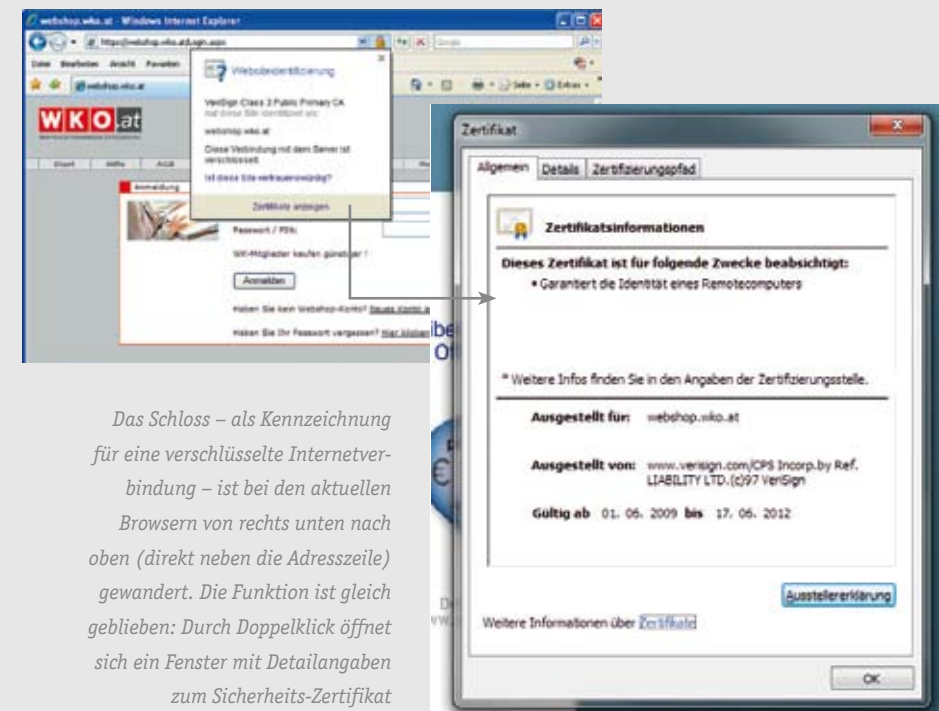
SICHERHEIT DURCH DIGITALE ZERTIFIKATE

Das wichtigste Element einer HTTPS-Verbindung ist das digitale Zertifikat des Website-Betreibers. Dieses Zertifikat wird vom Internet-Browser verwendet, um die Identität des Website-Betreibers festzustellen. Dadurch kann verhindert werden, dass eine gesicherte Verbindung zu einem Anbieter aufgebaut wird, der sich als jemand anderer ausgibt (z.B. kann ein Betrüger die Website einer Bank täuschend echt nachbauen, um Kunden PINs oder TANs zu entlocken).



Folgende Vorsichtsmaßnahmen sollten bei HTTPS-Verbindungen beachtet werden:

- Besondere Vorsicht ist geboten, wenn der Internet-Browser auf Schwierigkeiten mit dem Zertifikat hinweist. Auf diese Weise wird angezeigt, dass der Zertifikatsaussteller unbekannt ist oder der Name im Zertifikat nicht mit dem der Website übereinstimmt. Oft sind diese Meldungen nicht leicht zu interpretieren. Deswegen sollte ein EDV-Verantwortlicher oder besser ein kompetenter Mitarbeiter des Unternehmens, dessen Website aufzurufen versucht wurde, um Rat gefragt werden.



Das Schloss – als Kennzeichnung für eine verschlüsselte Internetverbindung – ist bei den aktuellen Browsern von rechts unten nach oben (direkt neben die Adresszeile) gewandert. Die Funktion ist gleich geblieben: Durch Doppelklick öffnet sich ein Fenster mit Detailangaben zum Sicherheits-Zertifikat

TIPP:

Kontrollieren Sie die Internet-Adresse genau, um kriminellen Methoden vorzubeugen. Es gab bereits Betrugsfälle, in denen die Opfer auf ähnlich aussehende URLs gelockt wurden (<http://ebanking.bawog.com> anstelle von <https://ebanking.bawag.com>, <https://www.mountain-america.net> statt <https://www.mntamerica.org>). Durch die Kontrolle der Adresszeile im Browser lassen sich solche Betrugsmethoden größtenteils ausschließen.

4. E-Mails und Spam

Sicherer Umgang mit unerwünschten Mails

Daten und Informationen werden immer häufiger per E-Mail ausgetauscht. Dadurch landen aber auch Spam-, Hoax- oder Phishing-Mails sowie mit Schadprogrammen verseuchte Nachrichten im Posteingangs-Ordner. Solche unerwünschte Nachrichten – mit mehr oder weniger gefährlichem Inhalt – machen mittlerweile über 90 Prozent des weltweiten E-Mail-Aufkommens aus.

UMGANG MIT UNERWÜNSCHTEN E-MAILS

Vor dem Öffnen eingehender E-Mails sollten Sie Folgendes beachten:

- Öffnen Sie niemals Dateianhänge, die Ihnen suspekt vorkommen. Auch bei vermeintlich bekannten bzw. vertrauenswürdigen E-Mail-Adressen ist zu prüfen: Passt der Text der Nachricht zum Absender (englischer Text von deutschem Partner, zweifelhafter Text oder fehlender Bezug zu konkreten Vorgängen etc.) und wird der Dateianhang auch erwartet.
- Kein „Doppelklick“ auf ausführbare Programme (.com, .exe) oder Scripts (.vbs, .bat etc.). Besondere Vorsicht ist bei doppelten, „merkwürdigen“ Dateinamen-Erweiterungen wie beispielsweise .jpg.vbs oder .gif.exe geboten. Sie sollen dem Empfänger eine harmlose Bilddatei vortäuschen. Tatsächlich handelt es sich jedoch um ein ausführbares Schadprogramm.
- Auch E-Mails im HTML-Format oder Office-Dokumente (.doc, .xls, .ppt etc.) sowie Bildschirm-schoner (.scr) können Skripte mit Schadensfunktion enthalten. Achten Sie hier auf die Vertrauenswürdigkeit des Absenders.
- Öffnen Sie auch keine E-Mails mit Spaßprogrammen, da die Programme ebenfalls Schadensfunktionen enthalten können.
- Öffnen Sie nur vertrauenswürdige E-Mail-Attachments! Oft ist die Art des Dateianhangs getarnt und über das Datei-Icon (z.B. das Word-Symbol) nicht sicher erkennbar.
- Vorsicht bei mehreren E-Mails mit gleich lautendem Betreff.
- So genannte Phishing-Mails, die zur Übermittlung von persönlichen Online-Banking-Daten oder Passwörtern (z.B. PIN oder TAN) auffordern, sind sofort zu löschen. Die angeforderten, vertraulichen Informationen dürfen Sie auf keinen Fall weitergeben.

- Oftmals muss in einem E-Mail nur ein Link angeklickt werden, um eine Webseite aufzurufen. Seien Sie vorsichtig: Beim Aufruf dieser URL wird möglicherweise Schadsoftware installiert oder eine gefälschte Phishing-Webseite aufgerufen. Im Fall von HTML-Mails muss die Adresse, die im Mail als Link angezeigt wird, nicht einmal mit der Seite übereinstimmen, die dann tatsächlich aufgerufen wird.
- Beantworten Sie keine Spam-Mails! Die Rückmeldung bestätigt dem Versender nur die Gültigkeit der Mail-Adresse, erhöht also nur das Risiko, weitere Zusendungen zu erhalten. Das Abbestellen von E-Mails ist nur bei seriösen Zustellungen sinnvoll.

Auch bei ausgehenden E-Mails sollte Folgendes beachtet werden (um nicht unabsichtlich Viren zu verteilen oder in Verdacht zu geraten, Spam-Mails zu versenden):

- Prüfen Sie, ob E-Mails im Ausgangs-Postfach stehen, die nicht von Ihnen verfasst wurden. Dies könnte auf Viren hindeuten.
- Versenden Sie keine E-Mails mit z.B. Scherz-Programmen, da diese Computer-Viren enthalten können.
- Folgen Sie nicht den Aufforderungen zur Weiterleitung von Warnungen, Mails oder Dateianhängen an Freunde, Bekannte oder Kollegen. Es handelt sich meist um Mails mit Falschmeldungen (Hoaxes, Kettenbriefe).
- Wenn Sie ein Mail an viele Empfänger schicken, die untereinander nicht bekannt sind, verwenden Sie „BCC“. Damit ist sichergestellt, dass keiner der Empfänger die E-Mail-Adressen der anderen Adressaten sehen und missbräuchlich verwenden kann.

TIPP:

Grundsätzlich dürfen Sie nach österreichischer Rechtslage keine E-Mails an mehr als 50 Empfänger (Massen-E-Mail) oder zu Zwecken der Direktwerbung (Werbe-E-Mail) versenden, ohne vorher die Zustimmung des Empfängers einzuholen.

Nähere Informationen dazu: http://portal.wko.at/wk/dok_detail_file.wk?angid=3&docid=1580694&stid=608901&dstdid=940

PHISHING-MAILS

Phishing ist eine spezielle Form des Social Engineering, bei der es darum geht, Zugangsdaten zu Online-Banking, Online-Zahlungssystemen, Web-Auktionsplattformen etc. zu „ergaunern“. Dies geschieht meist in Form von E-Mails, die dem Benutzer vorgaukeln, dass aufgrund von Wartungsarbeiten oder Sicherheitsüberprüfungen die Eingabe von Login/Passwort bzw. im Bankenbereich von PIN und TAN dringend erforderlich ist. Manchmal wird auch zusätzlich Druck ausgeübt, in dem die Schließung des Zugangs angedroht wird, sollte nicht binnen einer gewissen Frist der Aufforderung entsprochen werden. Ignorieren Sie grundsätzlich alle Mails, die diesem Muster folgen. Die Wahrscheinlichkeit, dass es sich dabei um ein echtes Mail handelt, ist verschwindend gering.

Phishing-Betrüger gehen auch in der zweiten Phase des Betrugs nach einem speziellen Muster vor: Sind sie im Besitz von PIN und TAN, können sie dennoch das Geld nicht einfach auf ihr Konto überweisen, denn das wäre leicht nachvollziehbar. Also werden sogenannte Finanz-agenten angeworben, und hier verbirgt sich die zweite Gefahr beim Phishing. Finanzagenten werden über Spam-Mails angeworben, in denen ein Gewinn über einen bestimmten Geldbetrag zugesagt wird. Reagiert der Malempfänger und gibt seine Kontodaten für die Überweisung bekannt, wird ihm ein Betrag überwiesen, der den Gewinn bei Weitem übersteigt (z.B.: USD 12.305,- statt „gewonnener“ USD 123,05). Kurz nach der Überweisung erfolgt wieder eine Kontaktaufnahme, in der auf diesen Fehler hingewiesen wird. Der Empfänger darf dann für die Unannehmlichkeiten einen zusätzlichen Betrag behalten, soll aber den restlichen Differenz-betrag abheben und per internationalem Bargeldtransfer (Western Union, Moneygram etc.) überweisen. Notfalls wird auch Druck ausgeübt und es wird suggeriert, dass der Versender aufgrund seines Fehlers seinen Job verliert oder Ähnliches. Das gleiche System wird auch angewandt, wenn Sie über ein Online-Auktionshaus eine Ware verkaufen und Ihnen der Käufer „irrtümlich“ einen zu hohen Betrag überweist.



Aktuelle Browser wie Internet Explorer 9 und Mozilla Firefox 7 verfügen über sogenannte Phishing-Filter, die beim Aufruf einer (bereits bekannten) Betrugsseite Alarm schlagen.

Als unwissend angeworbener Finanzagent verlieren Sie zwar nicht Ihr eigenes Geld, machen sich aber strafbar und können davon ausgehen, dass Sie zumindest sehr viel Ärger und Unannehmlichkeiten haben werden und möglicherweise sogar regresspflichtig sind. Ignorieren Sie also alle Aufforderungen, „irrtümlich“ auf Ihrem Konto geparktes Geld mittels Bargeldtransfer-Services zu versenden. Wenden Sie sich im Zweifelsfall an ihr Bankinstitut.

TIPP:

Phishing-Mails sind oftmals sehr gut gemacht und täuschen selbst Experten. Unter <http://www.it-safe.at> finden Sie einige Links zu Phishing-Tests, wo Sie anhand konkreter Mails testen können, ob es sich dabei um Originale oder Betrugsversuche handelt.

GEFÄLSCHTE ABSENDERADRESSEN

Wenn Sie Mails von bekannten Absendern, aber mit unpassenden Inhalten bekommen, muss der angezeigte Absender nicht unbedingt Urheber dieser Nachricht sein. Schadprogramme können auf das Adressbuch zugreifen und ohne das Wissen des Inhabers Mails an alle im Adressbuch gespeicherten Mail-Adressen versenden. Auch können die Mails im Namen einer im Adressbuch gespeicherten Person versendet werden.

Sollten Sie darauf angesprochen werden, dass Sie dubiose Mails versenden, sollten Sie sofort reagieren – vor allem dann, wenn Sie bisher keine entsprechenden Sicherheitsmaßnahmen (Virenschutz etc.) getroffen haben. Lassen Sie ein angeblich von Ihnen versandtes Mail von einem Experten prüfen, um zu klären, von wem das Mail wirklich stammt.

SPARSAMER EINSATZ DER EIGENEN MAIL-ADRESSE IM INTERNET

Vorsicht beim Ausfüllen von Webformularen: Häufig führt das Eintragen von Mail-Adresse oder persönlichen Daten zu einer Flut von Werbe- bzw. Spam-Mails. Der Handel mit Mail-Adressen wird in verschiedenen Ländern kaum kontrolliert. Hinterfragen Sie auch hier die Vertrauenswürdigkeit des Anbieters!

Sinnvoll ist es, bei einem Anbieter im Internet (<http://www.gmx.at>, <http://www.yahoo.at>, <http://www.gmail.com>, <http://www.hotmail.com> etc.) einen kostenlosen E-Mail-Account anzulegen, den Sie ausschließlich für derartige Registrierungen verwenden. Eine solche Adresse bietet außerdem die Möglichkeit, private und geschäftliche E-Mails zu trennen. So können auch Probleme beim Ausscheiden aus dem Unternehmen und der damit einhergehenden Deaktivierung Ihrer Mail-Adresse vermieden werden.

5. Gefährliche Schadprogramme

Schadprogramme wie z.B. Computer-Viren – enthalten verdeckte Funktionen, die durch Löschen, Überschreiben oder sonstige Veränderungen Schäden an Betriebssystemen, Anwendungsprogrammen und Daten erzeugen. Sie verursachen damit zusätzliche Arbeit und Kosten und haben einen negativen Einfluss auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten oder Programmen.

WIE KÖNNEN SIE ERKENNEN, DASS IHR PC INFIZIERT IST?

Typische Anzeichen einer Infektion sind:

- Sie können auf bestimmte Laufwerke oder Datenträger nicht mehr zugreifen und Dateien nicht mehr bearbeiten.
- Der Rechner arbeitet mit deutlich reduzierter Leistung (Systemauslastung zumeist auf 100 %), reagiert nicht oder startet in regelmäßigen Abständen neu. Auch der Zugriff auf Dateien dauert länger.
- Der Rechner startet nicht bzw. benötigt für das Hochfahren deutlich länger.
- Auf dem Bildschirm werden nicht vorhergesehene Bilder, Meldungen oder Dialogfenster angezeigt.
- Sie erhalten eine E-Mail-Nachricht mit Anhang. Beim Öffnen des Anhangs werden Dialogfenster angezeigt oder die Systemleistung nimmt sofort deutlich ab.
- Im Internet-Browser sind plötzlich zusätzliche Icons und Symbolleisten sichtbar. Als Startseite erscheint eine Homepage, die Sie nicht eingestellt haben.
- Es werden Warnungen angezeigt, dass bestimmte Programme eine Verbindung mit dem Internet herzustellen versuchen, obwohl dies nicht von Ihnen veranlasst wurde.
- Antiviren- und Antispywareprogramme sind deaktiviert und können nicht neu gestartet werden.
- Ohne Ihr Zutun verschwindet ein Programm von Ihrem Computer.
- Manche Viren greifen die zum Starten des Computers erforderlichen Dateien an. In diesem Fall erscheint nach dem Einschalten möglicherweise ein leerer Bildschirm.

Die angeführten Symptome können auch erst nach einer bestimmten Zeit auftreten. Sie können außerdem auch von Hardware- oder Softwarestörungen verursacht werden. Deswegen kann nur eine nähere Untersuchung des Rechners durch einen EDV-Fachmann Aufschluss über die tatsächlichen Ursachen geben.

MASSNAHMEN RICHTIG SETZEN

TECHNISCHE SCHUTZMASSNAHMEN

Jeder Rechner mit Internet-Anschluss benötigt einen aktuellen und aktivierten Schutz vor Schadsoftware:

- Betriebssysteme und einzelne Anwendungsprogramme wie z.B. der Internet-Browser können Sicherheitslücken aufweisen. Die Hersteller bieten meistens kostenlose Programmaktualisierungen (Updates oder sog. Hotfixes) an, die diese Fehler ausbessern sollen. Solche Aktualisierungen müssen unbedingt, möglichst ohne zeitliche Verzögerung installiert werden.
- Eine Firewall ist eine Sicherheitsschnittstelle zwischen Ihrem PC und dem Internet und verhindert unerlaubte Zugriffe. Sofern in Ihrem Unternehmen kein zentrales Firewall-System betrieben wird, sollte eine Personal-Firewall auf jedem Arbeitsplatz-rechner installiert werden. Diese Firewall darf auf keinen Fall deaktiviert werden.
- Ein Virenschutzprogramm mit aktuellen Signatur-Dateien ist unbedingt erforderlich. Die Signatur-Dateien müssen durch Updates regelmäßig aktualisiert werden, da sonst neu entwickelte Computerviren Ihren Computer ungehindert befallen können.

TIPP:

Melden Sie Ihrem EDV-Verantwortlichen unverzüglich, wenn Sie Warnhinweise erhalten, dass der Computer ungeschützt ist oder ein Sicherheitsproblem besteht. Vorsicht: Diese Hinweise können von Viren täuschend echt nachgestellt werden. Deswegen sollten Sie Maßnahmen erst nach Rücksprache mit dem EDV-Verantwortlichen setzen.

MASSNAHMEN BEI DER INTERNET-NUTZUNG

Daten und Programme, die aus dem Internet abgerufen werden, bergen die Gefahr von versteckter Schadsoftware in sich. Diese können Benutzerdaten ausspähen, weiterleiten, verändern oder auch löschen. Deswegen:

- Laden Sie Programme nur von vertrauenswürdigen Websites, wie z.B. von den Originalseiten des Herstellers. Dateien, die von Dritten über anonyme Webspaces-Provider angeboten werden, sind ein Sicherheitsrisiko.
- Daten und Programme von Hackerseiten, Gewinnspielseiten oder anderen dubiosen Homepages sind unbedingt zu meiden. Die Virengefahr ist überdurchschnittlich hoch.
- Überprüfen Sie immer die Größe von Dateien (evtl. wird auch die Prüfsumme angegeben) nach einem Download. Gibt es Abweichungen, besteht die Gefahr unzulässiger Veränderungen – meist durch Viren verursacht. Solche Dateien sollten Sie sofort löschen.
- Die heruntergeladenen Dateien müssen vor der Installation immer mit einem aktuellen Virenschutzprogramm überprüft werden.
- Gepackte (komprimierte) Dateien sollten Sie zuerst entpacken und auf Viren überprüfen. Die Entpackungsprogramme sind so zu konfigurieren, dass die zu entpackende Datei nicht automatisch startet.



Irreführendes E-Mail: Im Text wird behauptet, dass der Empfänger Viren versenden würde. Tatsächlich wird mit dem Dateianhang der Wurm „Stration.C“ übertragen.

VIRENINFEKTION: WAS TUN?

Meist ist die Gefahr schon beseitigt, wenn der Computer Sie auf einen Virus oder ein anderes Schadprogramm aufmerksam macht. In diesem Fall ist der Virus bereits gelöscht oder isoliert bzw. unter Quarantäne gestellt. Dennoch sollten Sie Ihren EDV-Verantwortlichen oder Vorgesetzten darüber informieren.

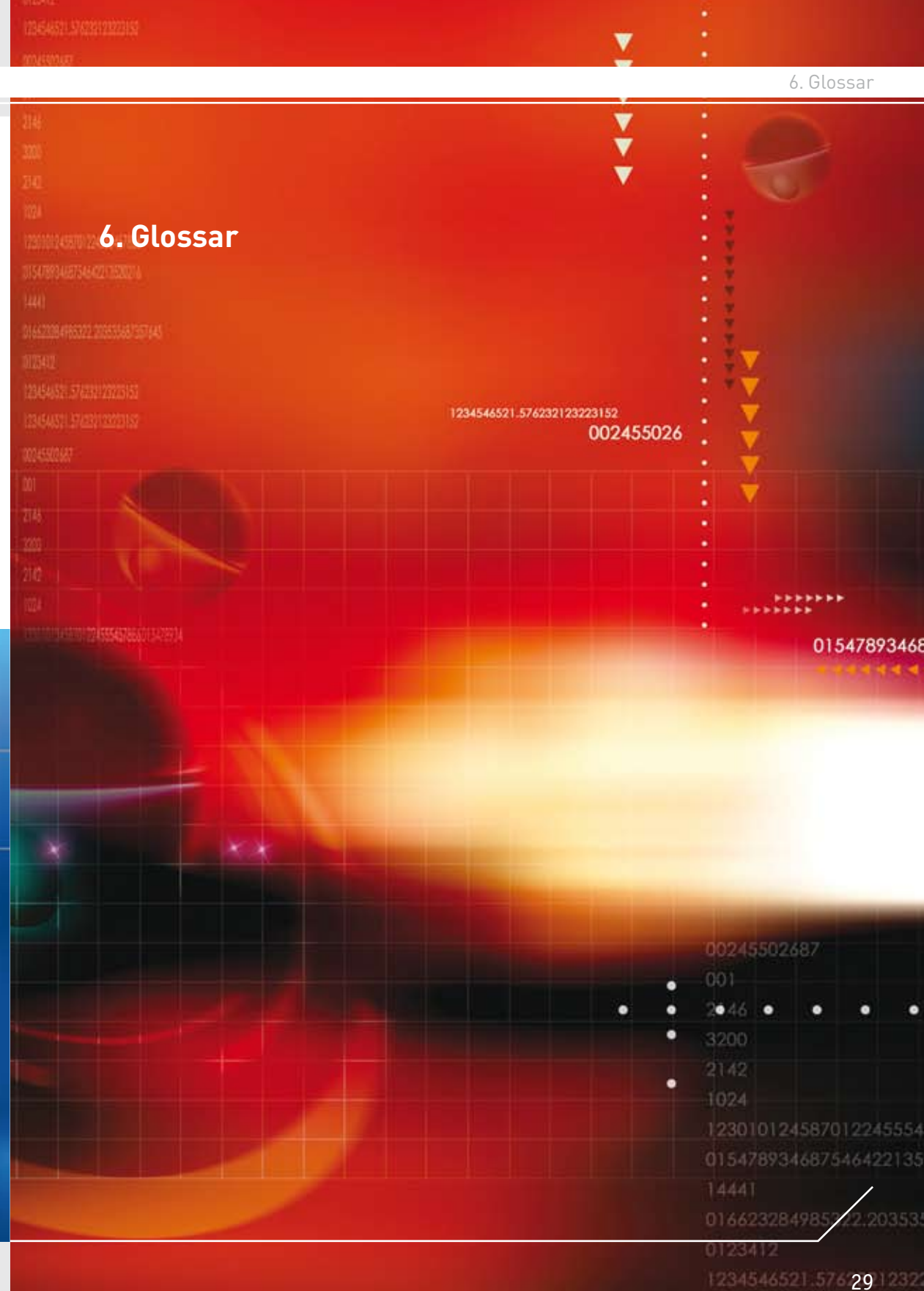
Wenn allerdings Ihr System das Problem nicht beseitigen kann oder der Verdacht einer Infektion besteht: Speichern Sie Ihre offenen Dateien ab und wenden Sie sich sofort an den zuständigen EDV-Verantwortlichen.

Name	Datum	Typ	Risikoausm...	An Symantec gesendet	Status
W32.Beagle@mm/zip	18.08.2006 20:38:39	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Beagle@mm/zip	16.08.2006 21:27:45	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Beagle@mm/zip	16.08.2006 21:21:00	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Bladnat.E@mm/lenc	04.07.2006 01:17:27	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Netsky.J@mm	16.02.2006 00:43:59	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Netsky.J@mm	16.02.2006 00:43:59	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Netsky.J@mm	16.02.2006 00:43:58	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Netsky.J@mm	16.02.2006 00:43:58	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Netsky.J@mm	16.02.2006 00:43:58	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Netsky.J@mm	16.02.2006 00:43:58	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Netsky.J@mm	16.02.2006 00:43:57	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Netsky.J@mm	16.02.2006 00:43:57	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
Trojan.Lodear.C	16.02.2006 00:43:53	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Sober.J@mm/zip	16.02.2006 00:43:51	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Sober.J@mm/zip	16.02.2006 00:43:51	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Netsky.C@mm	16.02.2006 00:43:12	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Sober.J@mm/zip	16.02.2006 00:43:08	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Sober.J@mm/zip	16.02.2006 00:43:08	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Sober.J@mm/zip	16.02.2006 00:43:07	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
Trojan.Lodear.C	16.02.2006 00:43:07	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Sober.J@mm/zip	16.02.2006 00:43:05	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Sober.J@mm/zip	16.02.2006 00:43:02	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Sober.J@mm/zip	16.02.2006 00:43:02	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
Trojan.Lodear.I	16.02.2006 00:42:58	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Sober.J@mm/zip	16.02.2006 00:42:56	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
Trojan.Lodear.B	16.02.2006 00:42:55	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
Trojan.Lodear.I	16.02.2006 00:42:55	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Beagle.AC@mm	16.02.2006 00:42:51	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei
W32.Myto.B@mm	16.02.2006 00:42:51	Virus	Hoch	Nicht gesendet	Backup-Kopie einer infizierten Datei

Auszug aus der Quarantäne-Liste eines Privat-Rechners

WAS TUN, WENN EIN KOMPETENTER VERANTWORTLICHER FEHLT?

- Speichern Sie Ihre offenen Dateien und schalten Sie den Rechner ab.
- Überprüfen Sie, ob die Rechner Ihrer Kollegen ähnliche Symptome zeigen.
- Recherchieren Sie von einem nicht befallenen Rechner aus im Internet. Verschiedene Websites, insbesondere von Herstellern von Antivirus-Software, enthalten Beschreibungen, wie Sie bestimmte Viren entfernen können.
- Verschiedene Antivirus-Programme enthalten bootfähige CDs. Mit diesen kann der befallene PC gefahrlos gestartet und auf Virenbefall geprüft werden. CDs mit derartigen Funktionen können auch aus dem Internet geladen und selbst gebrannt werden.
- Verschiedene Websites bieten Online-Virenprüfungen an. Bei Verdacht einer Infektion, d.h. wenn nicht währenddessen konkrete Schäden zu befürchten sind, kann der vermeintlich befallene PC getestet werden.

**6. Glossar**

BEGRIFFSERLÄUTERUNGEN:

- Als **AKTIVE INHALTE** werden bestimmte Funktionen von Websites bezeichnet, die die Bedienung einfacher, attraktiver oder bequemer machen sollen. Gemeinsam ist allen diesen Funktionen, dass sie am PC des Benutzers ausgeführt werden und nicht direkt sichtbar sind. Typische Beispiele für solche aktiven Inhalte sind Java-Applets, JavaScript, VBScript und ActiveX-Controls. Aktive Inhalte sind in der Standardeinstellung der Internet-Browser meistens aktiviert, da ohne sie die Bedienung vieler Websites nicht vollständig funktioniert. Sie stellen aber ein hohes Sicherheitsrisiko dar, da es mit ihrer Hilfe u.a. möglich ist, Schadprogramme zu installieren oder Daten aus dem PC auszulesen und an unbefugte Empfänger zu übertragen.
- **COOKIES** werden eingesetzt, um Informationen zu früher aufgerufenen Websites in kleinen Dateien auf dem Computer zu speichern. Sie ermöglichen beispielsweise, persönliche Einstellungen aus früheren Sitzungen wiederherzustellen oder Informationen aus Online-Shops ohne explizite Benutzeranmeldung zu speichern. Im Allgemeinen sind Cookies ungefährlich, allerdings können sie dazu missbraucht werden, das Surfverhalten von Benutzern auszuforschen oder Benutzerprofile anzulegen, die für zielgruppenorientierte Werbung genutzt werden.
- **DIALER** sind Einwahl-Programme, die eine Telefonverbindung über kostenpflichtige Mehrwertnummern aufbauen. Die Kosten für die Dialer-Verbindung betragen dabei mehrere Euro pro Minute. Die Aktivierung eines Dialers erfolgt in der Regel durch den User selbst, der dem Download oder der Installation eines Programms zustimmt. Betroffen sind insbesondere Benutzer von ungeschützten Smartphones.
- **DIGITALE ZERTIFIKATE** bilden die Grundlage für die Authentifizierung von Webservern beim Einsatz von HTTPS. Sie werden außerdem auch zur Verschlüsselung und zum Signieren von E-Mails genutzt. Zertifikate werden von einer Zertifizierungsstelle herausgegeben und weisen die Identität des Zertifikatsinhabers aus. Diese Zertifizierungsstellen können wieder durch andere Stellen zertifiziert sein; insgesamt bildet sich so eine Zertifizierungskette oder Zertifikatshierarchie, die bis zu einer obersten Stammzertifizierungsstelle reicht.

- **FTP** ist die Abkürzung für File Transfer Protocol, ein Verfahren zur Übertragung von Dateien zwischen Kommunikationspartnern. Die Datenübertragung ist in beide Richtungen möglich, mittels FTP-Client können Daten vom Server zum Client oder vom Client zum Server übertragen werden. Ähnlich wie bei HTTP werden dabei die Daten (auch Passwörter) unverschlüsselt übertragen. In Zusammenhang mit dem Internet wird FTP vor allem dazu verwendet, Softwareinstallationsdateien von FTP-Servern auf Clients zu übertragen oder neue Webseiteninhalte auf Servern einzuspielen.
- Als **HOAXES** bezeichnet man Warnungen über angebliche neue Computer-Viren, sensationelle Einkunftsöglichkeiten udgl., die in der Regel über E-Mail verbreitet werden und den Empfänger zur Weiterleitung auffordern. Bei diesen Warnungen handelt es sich in der Regel um Falschmeldungen oder Kettenbriefe, die den Empfänger verunsichern und zu unüberlegten Handlungen verleiten sollen. Hoax-Mails und Kettenbriefe sollten daher am besten sofort gelöscht und keinesfalls weitergeleitet werden. Nähere Informationen sind auf der Hoax-Liste der TU-Berlin unter <http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml> zu finden.
- **HTTP** ist die Abkürzung für HyperText Transfer Protocol, dem typischen Übertragungsprotokoll für Webseiten. Über HTTP werden Webseiten, d.h. Texte und Bilder von Servern im Internet an den jeweiligen Browser übertragen. Es können aber auch in Gegenrichtung Daten vom Browser an den Server gesendet werden, z.B. um eine Suchanfrage oder Daten in einem Webformular zur weiteren Verarbeitung an den Webserver zu schicken. HTTP ist ein relativ unsicheres Protokoll, das Daten unverschlüsselt überträgt und keinen Schutz vor dem Abfangen oder Umleiten von Daten bietet. Zur Übermittlung sensibler Daten ist es daher nicht geeignet.
- **HTTPS** ist die Abkürzung für HyperText Transfer Protocol Secure, das durch die Verwendung des Verschlüsselungsprotokolls SSL/TLS ausreichende Sicherheit für die Übertragung sensibler Daten bietet. Mit Hilfe dieses Protokolls werden einerseits die übertragenen Daten verschlüsselt und abhörsicher gemacht, andererseits wird durch die Verwendung von digitalen Zertifikaten die Identität des Servers gesichert. Einem Angreifer sollte es – richtige Handhabung vorausgesetzt – nicht möglich sein, sich z.B. als E-Banking-Server auszugeben, um dem Benutzer Passwörter, PINs oder TANs zu entlocken.

- **PHISHING** ist ein Kunstwort aus den beiden Begriffen „Password“ und „Fishing“ und bezeichnet den Versuch mittels gefälschter E-Mails an fremde Nutzerdaten (Login, Passwort, TAN etc.) zu gelangen. Normalerweise wird der Empfänger eines solchen Mails unter Vorspiegelung falscher Tatsachen (Userdaten gingen verloren, Neuidentifikation ist notwendig ...) aufgefordert, die Webseite einer Bank (Online Shop, Kreditkarteninstitut, Auktionshaus etc.) aufzusuchen und dort seine Zugangsberechtigungen einzutippen. Diese Webseiten sind ebenfalls gefälscht und sehen den Originalen zum Verwechseln ähnlich. Die dort eingetippten Daten landen natürlich nicht bei der eigenen Bank, sondern auf den Servern von Betrügern, die dann mit den Nutzerdaten Transaktionen zum Schaden des Users durchführen. Grundsätzlich fordert kein seriöses Unternehmen seine Kunden auf, seine Userdaten über das Internet zu bestätigen. Es sind also alle diesbezüglichen Mails zu ignorieren. In Zweifelsfällen sollte man sich telefonisch mit dem (vermeintlichen) Absender in Verbindung setzen.
- Als **ROOTKIT** bezeichnet man Software bzw. eine Softwaretechnik, mit der ein System manipuliert werden kann, sodass bestimmte Dateien, Prozesse, Netzwerkverbindungen, Speicherbereiche nicht mehr angezeigt werden. Damit ist es möglich, das Rootkit selbst und damit verborgene Schadsoftware vor Virencannern und Anwendern zu verstecken.
- **SOZIALE NETZWERKE** sind Netzgemeinschaften, die meist über Internetportale zugänglich sind. Über das Portal können Benutzer eigene Inhalte erstellen und austauschen. Typische soziale Netzwerke bieten Benutzern die Möglichkeit, Profile über die eigene Person, Vorlieben und Interessen anzulegen sowie Kontakte zu anderen Benutzern herzustellen und mit diesen zu kommunizieren.
- Als **SPAM** bezeichnet man unerwünschte Werbemails, die mittlerweile rund 90 Prozent des gesamten E-Mail-Verkehrs ausmachen. Auch bei kleineren Unternehmen ist es durchaus möglich, mehrere hundert Spam-Mails pro Tag zu erhalten. Gefährlich ist Spam grundsätzlich nicht, allerdings geht beim Löschen der Werbe-Mails wertvolle Arbeitszeit verloren. Mittels spezieller Spam-Filter können entweder bereits auf Provider-/Mailserver-Ebene oder auch erst am eigenen Rechner unerwünschte Mails gefiltert und gelöscht werden.
- Als **SPYWARE** bezeichnet man Programme, die den User und/oder sein Surfverhalten ohne sein Wissen ausspionieren. Diese Daten werden an den Hersteller der Software oder auch an Dritte, meist mit dem Zweck, personalisierte Werbung und Pop-ups einzublenden, weitergeleitet. Mittels Spyware können aber auch sensible persönliche Daten an Unbefugte übertragen werden.
- **TROJANISCHE PFERDE (TROJANER)** sind selbständige Programme mit verdeckter Schadensfunktion, ohne Selbstreproduktion. Trojanische Pferde dienen vor allem dazu, Computer auszuspionieren. Der Trojaner verdankt seinen Namen dem Umstand, dass die Schadensroutinen oft in scheinbar nützlichen Programmen versteckt sind. Ein Programm, das zum Zweck der Viren-Entfernung aus dem Internet heruntergeladen wird, kann unter Umständen genau das Gegenteil bewirken. Es ist daher immer auch notwendig, die Seriosität der Quelle, von der man Programme bezieht, zu überprüfen.
- **URL** ist die Abkürzung für Uniform Resource Locator, sie ist gewissermaßen die Adressangabe für einen Dienst in einem Computernetzwerk. Die URL für die Website von it-safe ist z.B. <http://www.it-safe.at>. Eine URL besteht aus der Zugriffsmethode auf diesen Dienst – im Web üblicherweise http oder https, für Datenübertragungen auch ftp – und dem Ort des Dienstes. An die URL kann noch, durch ein Fragezeichen getrennt, ein weiterer Textteil angeschlossen werden, um z.B. eine Anfrage an den verarbeitenden Server zu übertragen.
- **VIREN** sind nicht-selbständige, in andere Programme oder Dateien eingebettete Programmroutinen, die sich selbst reproduzieren und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung, vornehmen.
- **WÜRMER** sind selbständige, selbstreproduzierende Programme, die sich in einem System (vor allem in Netzen) ausbreiten. Zu diesem Zweck verwenden viele Würmer das Adressbuch des infizierten Rechners und versenden Mails mit gefälschten Absenderadressen. Das Öffnen solcher Mails kann bei einem ungeschützten System zu einer Infektion führen.