it-safe.at

IT Sicherheitshandbuch

Datensicherheit schafft Vorsprung

3. Auflage

BMWA Bundesministerium für Wirtschaft und Arbeit

WKO Information · Consulting

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

Die Aktion wird unterstützt vom Bundesministerium für Wirtschaft und Arbeit, dem Unternehmerservice-Netzwerk der Wirtschaftskammern Österreichs, dem Zentrum für Sichere Informationstechnologie Austria (A-SIT), dem Bundesministerium für Unterricht, Kunst und Kultur und der IT-Security Experts Group.

IT Sicherheitshandbuch

Datensicherheit schafft Vorsprung

3. 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

3. Auflage, April 2007

Für den Inhalt verantwortlich: Mag. Bernhard Strilka, Mag. Jürgen Stöger, Friedrich Tuma
Basislayout: Birgit Altrichter, Michaela Köck – geschmacksache.at
Grafische Umsetzung: www.designag.at
Druck: Agentur Prokop

INHALT

VORWORT

Im geschäftlichen Alltag ist so gut wie jeder Unternehmer mit der Notwendigkeit konfrontiert, Daten elektronisch zu verarbeiten und zu speichern.

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 sind mit sensiblen Daten konfrontiert, die keinesfalls Dritten in die Hände fallen dürfen, sei es aus Gründen des Datenschutzes oder weil es sich um vertrauliche Unternehmensdaten zu neuen Produkten, Marktstudien oder Forschungsergebnissen handelt.

In all diesen Fällen ist es unerlässlich, dass die Unternehmensdaten geschützt werden. Sowohl vor dem Versuch Dritter, diese Daten auszuspionieren, als auch vor der Gefahr des Datenverlustes infolge von äußeren Einflüssen (z.B. Feuer, Blitzschlag, Wasser etc.) oder schadhaften Computersystemen.

Die Bundessparte Information und Consulting (BSIC) hat im Oktober 2005 die Aktion „it-safe.at“ ins Leben gerufen, um vor allem den kleinen Unternehmen Hilfestellung im Bereich IT-Sicherheit anzubieten. Oftmals ist ein Mehr an Sicherheit bereits durch einfache und rasch umzusetzende Maßnahmen zu erreichen. Viele Maßnahmen und Ratschläge finden Sie in diesem Buch. Weiterführende Informationen haben wir für Sie auf der Webseite www.it-safe.at zusammengestellt.

Nutzen Sie das Service der BSIC für die Sicherheit Ihres Unternehmens.

KommR Hans-Jürgen Pollirer
Bundesspartenobmann


30
35

Foto Fischer, Graz

EINLEITUNG

Die Bundessparte Information und Consulting (BSIC) will mit der Aktion „it-safe.at“ und vor allem mit diesem Handbuch – das nunmehr in der 3. Auflage vorliegt – jene Unternehmen ansprechen, die sich bisher noch nicht oder nur oberflächlich mit dem Thema IT- und Datensicherheit beschäftigt haben.

IT-Sicherheits-Maßnahmen können Zeit und Geld kosten, stehen aber in keinem Vergleich zu dem Schaden der bei einem Komplettverlust der Daten (z.B. aufgrund einer defekten Festplatte) eintritt. Oftmals resultieren die Maßnahmen auch in einem Komfort-Verlust. Natürlich ist es praktisch, wenn jeder Mitarbeiter als Administrator arbeitet und selbst Programme installieren kann. Sinnvoll ist es keinesfalls. Auch die Verwendung von USB-Sticks ist praktisch, auf der anderen Seite birgt sie aber ein Gefahrenpotenzial. Jedes Unternehmen muss für sich selbst entscheiden, welche Risiken bewusst in Kauf genommen und welche Risiken mit technischen und organisatorischen Maßnahmen minimiert bzw. vermieden werden.

Jedes Unternehmen hat auch individuelle Sicherheitsbedürfnisse. Daher finden Sie unter http://www.it-safe.at auch die Möglichkeit, ein für Sie individuell zusammengestelltes Sicherheitshandbuch zu generieren, das Sie dann als PDF herunterladen können.

Ganz wichtig ist auch die ständige Schulung und Sensibilisierung der Mitarbeiter. Zu diesem Zweck gibt es – ebenfalls aus der it-safe.at Reihe – ein eigenes „IT-Sicherheitshandbuch für Mitarbeiter“, das sich speziell an Computer-Anwender richtet und eine sinnvolle Ergänzung zum vorliegenden Handbuch für KMU darstellt.

Wir sind natürlich bemüht unsere Produkte laufend zu verbessern und freuen uns daher über jede Form der Kritik. Senden Sie uns Ihre Ideen und Anregungen an ic@wko.at.

Mag. Bernhard Strilka
Projektleiter

1. Datensicherung und Notfallwiederherstellung

Datensicherung und Notfallswiederherstellungsmaßnahmen helfen bei der Schadensbegrenzung nach Systemausfällen, dem Verlust einzelner Dateien oder im schlimmsten Fall der Zerstörung der gesamten IT-Infrastruktur. Verschiedene, miteinander verknüpfte Maßnahmen sind nötig, um sicherzustellen, dass die IT-Systeme innerhalb eines definierten Zeitraums wieder funktionsfähig sind.

Datensicherung

Voraussetzung für jede Notfallvorsorge ist die Planung und Durchführung regelmäßiger Datensicherungen. In vielen Fällen müssen auch die Mitarbeiter zur Einhaltung und Unterstützung der Datensicherungsmaßnahmen verpflichtet werden.

Heute werden oft Technologien eingesetzt, die bestimmte typische Einsatzzwecke von Datensicherungen abdecken: RAID-Laufwerke bieten Schutz vor dem mechanischen Ausfall einzelner Festplatten, Snapshot-Technologien ermöglichen das Wiederherstellen versehentlich gelöschter Dateien. Der Nutzen von Datensicherungen geht aber weit über diese begrenzten Einsatzbereiche hinaus: Sie ermöglichen die Wiederherstellung bestimmter Datenstände zu Beweisführungszwecken (Jahres-, Monatssicherungen) oder um Daten wiederherzustellen, die von Schadsoftware verfälscht wurden. Vor allem aber ermöglichen sie, die Daten nach schwerwiegenden Vorfällen, wie z.B. einem Brand im Serverraum oder dem Diebstahl von Rechnern, wiederherzustellen. Durch die geringe Größe der Sicherungsmedien ist auch die Auslagerung an einen sicheren Ort ohne großen Aufwand möglich.

DATENSICHERUNGSKONZEPT UND -PLANUNG

*In **schriftlicher Form** ist festzulegen, **welche Daten** von **wem** zu **welchem Zeitpunkt** gesichert werden.*

Folgende Punkte müssen dabei in jedem Fall behandelt werden:

- Umfang der zu sichernden Daten
- Sicherungstechnologie und -medien
- Zeitintervall und Zeitpunkt der Sicherungen
- Anzahl der aufzubewahrenden Sicherungen aus der Vergangenheit
- Zuständigkeiten für Durchführung, Überwachung und Dokumentation der Sicherungen
- Überprüfung der Datensicherungen, Wiederherstellungstests und -übungen

Vorrangig sollten selbst erstellte Daten (Produktionsdaten, z.B. Dokumente, Kundendatei, Buchhaltung etc.) gesichert werden, außerdem noch die Konfigurationsdateien der eingesetzten Software. Ob es sinnvoll ist, auch Systemdateien zu sichern (bis hin zur vollständigen Sicherung von Betriebssystem und installierter Software), hängt u.a. davon ab, wie dringlich die Wiederaufnahme des Betriebs nach einem Totalausfall erscheint.

Grundsätzlich sind alle Arten von Wechseldatenträgern als Sicherungsmedien geeignet. In einfachen Fällen kann es ausreichen, die Produktionsdaten wöchentlich auf eine CD-ROM oder DVD zu brennen. Auch Wechsel- oder externe Festplatten, eventuell auch USB-Sticks, können verwendet werden.

Allerdings erfordert diese Methode hohen Arbeits- und Zeitaufwand und lässt sich schlecht automatisieren. Ab einer bestimmten Datenmenge ist es daher sinnvoller, eine geeignete Sicherungssoftware und spezielle Wechsellaufwerke einzusetzen. Oft liegen dem Betriebssystem einfache Versionen von Backup-Software bei, die dazu bereits ausreichen können. Im Handel erhältliche Sicherungssoftware bietet dagegen oft Handlingvorteile und ist oft auch für Spezialfälle (Sichern von Datenbanken oder Mailservern) geeignet.

Als Sicherungshardware können Bandlaufwerke eingesetzt werden, die in den verschiedensten Ausführungen und Speicherkapazitäten erhältlich sind, alternativ dazu lassen sich auch Wechselfestplattensysteme verwenden. Voraussetzung für den Einsatz solcher Systeme ist die zentrale Speicherung der Daten auf einem eigenen Server (Fileserver), auf dem die benötigte Hard- und Software installiert werden kann. Diese Anordnung ist hinsichtlich der Datensicherheit ohnehin empfehlenswert. Die Benutzer müssen aber unbedingt dazu angehalten werden, ihre Daten auf dem Server und nicht auf den lokalen Festplatten ihrer Arbeitsplatzrechner zu speichern.

Für geringere Datenmengen lässt sich auch die Möglichkeit der **Online-Datensicherung** nützen. Dabei werden Daten über das Internet auf zentrale Server übertragen, von denen sie im Notfall wieder abgerufen werden können. Der Vorteil dieser Methode ist, dass die Daten außer Haus gespeichert werden und dadurch eine räumliche Trennung der Sicherungen von den Originaldaten gegeben ist. Für kleinere Datenmengen, eventuell auch, um nur die wichtigsten Daten zu sichern, ist diese Methode gut geeignet. Bei einer Online-Sicherung ist aber großes Augenmerk auf die Seriosität des Anbieters zu legen.

Verschiedene Datensicherungsmethoden sind möglich:

- **Volldatensicherung:**
  Bei dieser Methode werden sämtliche zur Sicherung vorgesehenen Dateien gesichert. Volldatensicherungen sind einfach durchzuführen und auch die Wiederherstellung der Daten funktioniert relativ einfach. Allerdings verbrauchen sie üblicherweise viel Speicherplatz auf den Sicherungsdatenträgern und dauern lange. Sie sind ideal für unbeaufsichtigte, in der Nacht oder am Wochenende durchgeführte Sicherungsläufe.

- **Inkrementelle Sicherung:**
  Bei inkrementellen Sicherungen werden nur die seit der letzten Sicherung geänderten Dateien gesichert. Dabei werden deutlich weniger Daten gesichert, die Sicherungen erfolgen also zeitsparender und verbrauchen weniger Platz. Der Nachteil besteht darin, dass eine einzige fehlgeschlagene Sicherung ausreicht, um alle darauf folgenden Sicherungen unbrauchbar zu machen. In regelmäßigen Abständen (z.B. wöchentlich) müssen daher zusätzlich Volldatensicherungen durchgeführt werden, auf denen die inkrementellen Sicherungen aufbauen. Auch die Wiederherstellung der Daten ist deutlich komplizierter: Der gesamte Sicherungssatz, d.h. die letzte Volldatensicherung sowie alle darauf folgenden inkrementellen Sicherungen, müssen dazu verwendet werden.

- **Datenträgerimages:**
  Datenträgerimages sind nicht eigentlich eine Datensicherungsmethode, sondern werden vorallem eingesetzt, um ausgefallene Computer rasch wiederherzustellen. Dazu wird von der Festplatte eines PCs ein „Image“, d.h. ein Abbild, erstellt und auf Datenträger gespeichert. Im Bedarfsfall kann dieser PC dann anhand des Images in wenigen Minuten wieder in den exakten Zustand zum Zeitpunkt der Imageerstellung versetzt werden. Alle seitdem veränderten Dateien gehen dabei allerdings verloren oder müssen von einer konventionellen Datensicherung wiederhergestellt werden.

Um sicherzustellen, dass die Datensicherung im Notfall ausreicht, muss **unbedingt** die Wiederherstellung der gesicherten Daten getestet werden. Besonders gilt dies für die Wiederherstellung komplexer Server (Datenbank-, Mailserver, Domänencontroller): Die Notfallwiederherstellung solcher Server, vom leeren System bis zur produktionsreifen Maschine, muss mindestens einmal durchgeführt und dokumentiert werden. Es ist **nicht** davon auszugehen, dass eine ungetestete Wiederherstellungsmethode im Notfall tatsächlich funktionieren wird.

SICHERUNGSVARIANTEN IM ÜBERBLICK

	Pro	Kontra	Fazit
ONLINE-SICHERUNG	Räumliche Trennung, Sicherheit (bei seriösen Anbietern)	Laufende Kosten, nur für kleine Datenmengen geeignet	vor allem für sehr wichtige Daten geeignet, kaum für Komplett-sicherungen
BANDSICHERUNG	Archivierung sehr einfach, räumliche Trennung leicht möglich, große Datenmengen, gut automatisierbar	Einrichtungs- und Bedienungsaufwand, teilweise störanfällig	sehr gut für Volldaten-sicherungen und Datenarchivierung geeignet
IMAGESICHERUNG	Sehr schnell, gut für Sicherung kompletter Systeme geeignet, schnelle Wiederher-stellung	Zusätzliche Sicherung veränderlicher Daten nötig, für regelmäßige Datensicherungen kaum geeignet, Beeinträchtigung des laufenden Betriebs	sehr gut zur Wiederher-stellung vollständiger Systeme und Konfigurationen geeignet
SICHERUNG AUF EXTERNE FESTPLATTEN, WECHSEL-FESTPLATTEN ODER USB-STICKS	kostengünstig, einfache Bedienung, für annähernd alle Datenarten möglich	Versionsmanagement und räumliche Trennung pro-blematisch, hoher Bedie-nungsaufwand, teilweise störanfällig	günstige Einsteigerlösung mit Abstrichen bei der Sicherheit

SCHRIFTLICHE AUFZEICHNUNGEN DER KONFIGURATIONSDATEN

Zusätzlich zur eigentlichen Datensicherung sollten verschiedene Konfigurationsdaten ausgedruckt und an sicherer Stelle aufbewahrt werden.

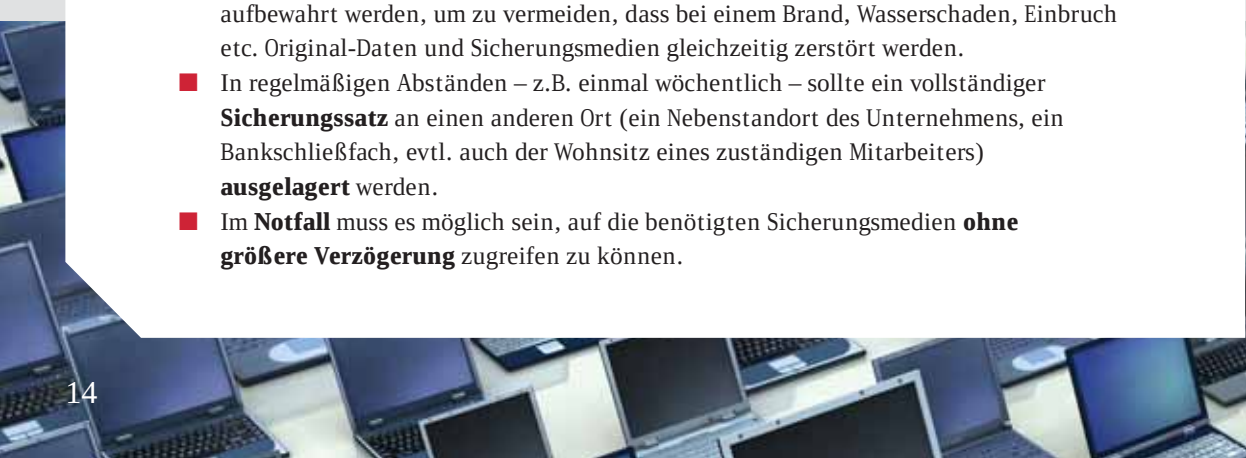
Selbst wenn sämtliche Konfigurationseinstellungen in elektronischer Form gespeichert werden können, ist es von Vorteil, in Notfällen auf Ausdrucke der wichtigsten Einstellungen zurückgreifen zu können. Die Zugangsdaten zum Internet-Provider, einschließlich der Konfigurationsdetails für den Netzwerkzugang und der Passwörter (z.B. für evtl. Mail-Accounts), sollten unbedingt gesondert zugreifbar sein. Auch für Konfigurationseinstellungen der Netzwerkrouter und Switches sind schriftliche Aufzeichnungen oder Bildschirmausdrucke bei der Wiederherstellung wichtig. Die Aufzeichnungen müssen an sicherer Stelle, d.h. vor Zerstörung und unbefugten Zugriffen geschützt, gelagert werden. Bei Änderungen an den Einstellungen oder Passwörtern müssen sie umgehend aktualisiert werden.

GEEIGNETE AUFBEWAHRUNG DER BACKUP-DATENTRÄGER

Bei der Aufbewahrung der Backup-Datenträger ist aus zwei Gründen besondere Sorgfalt angebracht: Die Entwendung eines Sicherungsmediums würde einem Angreifer den einfachen Zugriff auf die wichtigsten Unternehmensdaten ermöglichen. Und im Katastrophenfall, etwa nach der Zerstörung der IT-Systeme durch einen Brand, sind die Sicherungen die einzige Chance, den elektronisch gespeicherten Datenbestand zu retten.

Folgende Anforderungen sollten erfüllt sein:

- Der **Zugriff** auf Backup-Datenträger darf **nur befugten Personen** möglich sein. Sie sollten idealerweise in einem Safe, jedenfalls aber geschützt, gelagert werden. Auch die Sicherungslaufwerke sollten nur den zuständigen Mitarbeitern zugänglich sein, um zu verhindern, dass Medien unbemerkt ausgetauscht werden können.
- Die Backup-**Datenträger** müssen von den gesicherten Rechnern **räumlich getrennt** aufbewahrt werden, um zu vermeiden, dass bei einem Brand, Wasserschaden, Einbruch etc. Original-Daten und Sicherungsmedien gleichzeitig zerstört werden.
- In regelmäßigen Abständen – z.B. einmal wöchentlich – sollte ein vollständiger **Sicherungssatz** an einen anderen Ort (ein Nebenstandort des Unternehmens, ein Bankschließfach, evtl. auch der Wohnsitz eines zuständigen Mitarbeiters) **ausgelagert** werden.
- Im **Notfall** muss es möglich sein, auf die benötigten Sicherungsmedien **ohne größere Verzögerung** zugreifen zu können.



DATENSICHERUNG BEI MOBILEN IT-SYSTEMEN (NOTEBOOKS, PDAS ETC.)

Wenn Notebooks oder PDAs verwendet werden, um wichtige Daten „unterwegs“ zu erfassen oder zu bearbeiten, muss dafür gesorgt werden, dass auch die auf diesen Geräten abgelegten Daten gesichert werden.

Dazu bieten sich folgende Verfahren an:

- **Datensicherung auf externen Datenträgern (externe Festplatten, USB-Memory-Sticks, DVD-ROMs etc.)**
  Die Datenträger sollten getrennt von den zugehörigen IT-Systemen aufbewahrt werden, um den gleichzeitigen Verlust, etwa bei einem Diebstahl, zu verhindern. Nach Möglichkeit sollten die Daten verschlüsselt gespeichert werden, um Missbrauch beim Verlust eines Sicherungsdatenträgers zu verhindern.
- **Datensicherung über Fernverbindung zum Firmennetzwerk**
  Dabei werden Daten vom Standort des Mitarbeiters zu einem zentralen Server übertragen. Ausreichende Übertragungsgeschwindigkeit sowie die verschlüsselte Übertragung der Daten sind dafür unbedingte Voraussetzungen.
- **Datensicherung bei der Rückkehr ins Firmennetzwerk**
  Dieses Verfahren ist nur dann empfehlenswert, wenn der Mitarbeiter regelmäßig (z.B. wöchentlich) in das Unternehmen zurückkehrt und der mögliche Verlust der zwischenzeitlich geänderten Daten tragbar erscheint.

Die ersten beiden Verfahren bringen zusätzlichen Aufwand und zusätzliche Verantwortung für die Benutzer mit sich. Durch den Einsatz geeigneter Software-Tools ist es möglich, den nötigen Arbeitsaufwand zu verringern. Mitarbeiter mit mobilen IT-Systemen sollten aber besonders auf die Wichtigkeit regelmäßiger Datensicherungen und ihre Eigenverantwortung beim Schutz der Daten hingewiesen werden.

Notfallvorsorge und -wiederherstellung

Vor allem in Betrieben, in denen ein großer Teil der Wertschöpfung auf dem Funktionieren der IT-Infrastruktur beruht, ist es wichtig, rechtzeitig Überlegungen zum Abwenden und Bewältigen von Notfällen anzustellen. Notfälle sind kostspielig; ihre Kosten entstehen nicht nur durch Maßnahmen zu ihrer Behebung, sondern vor allem auch durch den Verlust an produktiver Arbeitszeit. Ein Notfallkonzept hilft, diese Ausfallszeiten zu minimieren und möglichst rasch zum normalen Produktionsbetrieb zurückzukehren.

ERHEBUNG DER WICHTIGSTEN ANWENDUNGEN

Erster Schritt jeder Notfallvorsorge ist das Festlegen von Prioritäten für die einzelnen Anwendungen.

Für die Notfallvorsorge ist es unerlässlich, die Anwendungen mit den höchsten Verfügbarkeitsanforderungen ausfindig zu machen. Im nächsten Schritt müssen jene Teile der IT-Systeme (wie z.B. Server, Daten, Datenleitungen), die für den Betrieb dieser Anwendungen nötig sind, identifiziert werden. Die Notfallplanung sollte sich vorwiegend auf diese zentralen Komponenten konzentrieren.

NOTFALLVORSORGE UND EINGESCHRÄNKTER ERSATZBETRIEB

Bei entsprechender Planung ist es oft möglich, mit relativ kleinem Aufwand Notfälle drastisch zu verkürzen: Ein einziger Ersatzrechner, z.B. ein Firmennotebook, das auch für andere Zwecke genützt werden kann, kann ausreichen, um den Ausfall einzelner PCs vollständig zu überbrücken.

Ersatzrechner müssen nicht den gleichen technischen Leistungsstandards entsprechen wie die Systeme, die sie ersetzen sollen. Daher können unter Umständen auch alte Rechner, die bereits durch neue Systeme ersetzt wurden oder auch weniger leistungsstarke und dadurch kostengünstigere Neu-Systeme für solche Aufgaben herangezogen werden. Auch für zentrale Netzwerkkomponenten können Altgeräte zurückbehalten werden: Als Ersatz für einen Breitband-Internetzugang bietet sich z.B. ein (ansonsten deaktiviertes) Modem an.

Für wichtige Serversysteme, deren Ausfall zu unmittelbaren finanziellen Einbußen führen kann (z.B. stark frequentierte Webshops), empfiehlt es sich dagegen, „gespiegelte“ Systeme mit möglichst gleicher Kapazität vorrätig zu halten, die bei Bedarf aktiviert werden können. In

solchen Fällen sind zusätzlich auch andere Überlegungen anzustellen: Es sollte überlegt werden, wo z.B. nach einem Brand im Serverraum diese Ersatzsysteme aufgestellt werden könnten, wie bei einem Ausfall der Netzanbindung vorgegangen werden kann etc. Grundsätzlich gilt: Je höher der durch einen Notfall zu erwartende Schaden ist, desto gründlicher sollte auch die Planung zur Notfallvorsorge durchgeführt werden.

Häufige Ursache für Notfälle sind Hardwareprobleme, wie z.B. Defekte an Netzteilen oder Festplatten. Für zentrale, wichtige Systeme sollten daher Wartungsverträge abgeschlossen werden, die den Ersatz defekter Komponenten innerhalb einer vereinbarten Zeitspanne sicherstellen. Oft sind derartige Wartungsverträge nur zum Zeitpunkt der Anschaffung der Komponenten günstig erhältlich. Diese Gelegenheit sollte daher möglichst genützt werden.

NOTFALLWIEDERHERSTELLUNG

Für die Rückkehr zum Normalbetrieb ist es notwendig, die ausgefallenen Systemkomponenten wiederherzustellen. Durch das Planen und Testen von Wiederherstellungsverfahren lässt sich dieser Prozess verkürzen und kalkulierbar machen. Vor allem kann dadurch aber vermieden werden, dass sich verschiedene Datenbestände erst beim Wiederherstellungsversuch als nicht mehr rekonstruierbar herausstellen.

Verschiedene Methoden der Notfallwiederherstellung sind möglich: Als erster Schritt werden zur Wiederherstellung eines PCs üblicherweise das Betriebssystem sowie die Sicherungssoftware installiert; das kann manuell, skriptgesteuert oder mit Hilfe eines Datenträger-Images erfolgen. Danach werden die Daten aus der letzten Datensicherung eingespielt, um den Rechner auf aktuellen Stand zu bringen.

Um Verzögerungen zu vermeiden, muss dafür gesorgt sein, dass alle benötigten Installationsdateien im Notfall greifbar und funktionsfähig sind. Am einfachsten geschieht das, indem Kopien der Installationsmedien erstellt und an gleicher Stelle wie die Sicherungsmedien gelagert werden. Auch an dem Ort, an den die Datensicherungsmedien ausgelagert werden (Bankschließfach o.ä.), sollten Kopien deponiert werden.

Verschiedene Backup-Programme ermöglichen auch eine vollständig automatisierte Notfallwiederherstellung, insbesondere von Serversystemen. Diese Methoden unterscheiden sich aber stark in Geschwindigkeit, Arbeitsaufwand und Zuverlässigkeit, sie müssen daher besonders gründlich getestet werden.

Häufig wird auch erst nach dem Test von Wiederherstellungsverfahren erkennbar, dass die bisher gesicherten Daten nicht für die vollständige Wiederherstellung ausreichen. Die Wiederherstellung hat also oft auch Rückwirkungen auf die Einstellungen der Datensicherung.

Um im Notfall sicher und rasch reagieren zu können, müssen die Backup/Restore-Methoden unbedingt detailliert und ausführlich dokumentiert werden. Die ausführliche Dokumentation des Wiederherstellungsverfahrens hilft u.a. in Fällen, in denen der ansonsten Verantwortliche nicht greifbar ist. Sie sollte ausreichend detailliert sein, um anderen technisch geschulten Personen die Durchführung des Verfahrens zu ermöglichen.

Das Know-how der SECUR-DATA auf dem Gebiet der Datensicherheit konzentriert sich auf die drei Säulen

- Datenschutz,
- Konzeption und
- Audit.

Der IT-Security Quick Check bedient sich dieses Wissens und untersucht bereichsübergreifend den Stand der IT-Sicherheit Ihres Unternehmens. In gestraffter Form werden die Ergebnisse zusammengefasst, um als fundierte Grundlage für weitergehende Maßnahmen zur Verbesserung des Sicherheitsniveaus zu dienen.

Trial and Error kann sich heute niemand mehr leisten. Die notwendigen Sicherheitsmaßnahmen müssen ***aus ganzheitlicher Sicht*** ausgewählt und eingeführt werden.

Der IT-Security Quick Check ist der erste Schritt.

Secur-Data

ist seit 1975 erfolgreich auf dem Gebiet der IT-Sicherheit in Österreich tätig.

Secur-Data
Betriebsberatungs-
GesmbH
Fischerstiege 9
A-1010 Wien

Tel 01 533 4207-0
Fax 01 533 4207-19
www.secur-data.at
office@secur-data.at

„Viele scheuen sich davor, das Thema IT-Security anzugehen, weil sie keine schlafenden Hunde wecken wollen. Andere haben nach und nach eine ganze Reihe von Sicherheitsmaßnahmen gesetzt, wissen aber nicht, wie diese gesamtheitlich zu werten sind. Mit dem IT-Security Quick Check haben sie nun erstmals eine kostengünstige Gelegenheit, eine objektive Darstellung zum Stand der IT-Sicherheit in ihrem Unternehmen zu erhalten, verbunden mit fundierten Empfehlungen zur weiteren Behandlung dieses oft überlebenswichtigen Themas."

KommR Hans-Jürgen Pollirer
CEO der Secur-Data Betriebsberatungs-Gesellschaft

„Zwei von fünf Unternehmen machen Pleite, wenn sie ihre Daten verlieren. Trotzdem will niemand in die notwendigen Schutzmaßnahmen investieren. Es ist höchste Zeit, das Thema auf Vorstandsebene aufzuhängen."

(„CIO - IT-Strategie für Manager", Münchener Computerwoche-Verlag)

Die drei Know-how-Säulen der Secur-Data im Rahmen der Datensicherheit und die angebotenen Produkte

2. Sicherheit des Internetzugangs

Durch eine Netzwerkverbindung zum Internet entstehen neue Gefahren: Werden keine zusätzlichen Schutzmaßnahmen eingerichtet, ist die Verbindung in beiden Richtungen offen, d.h. es kann nicht nur vom Firmenrechner auf das Internet, sondern auch von einem beliebigen Rechner im Internet auf das Firmennetz zugegriffen werden.

Auch der Zugriff auf das WWW ist nicht immer unproblematisch: Aktive Inhalte auf Webseiten gefährden die Sicherheit der lokalen Rechner und dadurch auch die Vertraulichkeit der Firmendaten. Weitere Gefahren gehen von Schadprogrammen (Viren, Würmer, Spyware, Adware etc.) aus.

FIREWALLS

IT-Systeme im Firmennetzwerk dürfen nur unter Verwendung ausreichender Sicherheitseinrichtungen mit dem Internet verbunden werden. Solche Einrichtungen werden als „Firewalls" bezeichnet.

Eine Firewall kontrolliert die Netzwerkverbindungen zwischen Firmennetzwerk und Internet und blockiert alle jene Verbindungen, die nicht explizit als „erlaubt" deklariert wurden. Firewalls sind in unterschiedlichsten Ausführungen und Preisklassen erhältlich, die Palette reicht von Breitband-Routern mit integrierter Paketfilter-Firewall bis zu hochleistungsfähigen Firewall-Appliances mit verschiedenen Schutzzonen. Sie unterscheiden sich stark in ihrer Leistungsfähigkeit und Schutzwirkung:

- Geräte mit **Paketfilter-Firewall** sind sehr einfache Firewalls, die nur eingeschränkten Schutz bieten und geringe Flexibilität aufweisen. Sie sind hauptsächlich für den Schutz privater PCs gedacht und für den betrieblichen Einsatz eher ungeeignet.
- **Multifunktions-Firewalls**, oft auch Sicherheits-Appliances o.ä. genannt, bieten zusätzlich zur Firewall-Funktion noch weitere Dienste an. Typischerweise können damit abgesicherte Zugänge für Telearbeit und Fernadministration hergestellt werden. Manche dieser Geräte können auch den Netzwerkverkehr auf Viren absuchen oder sogar Spam-Mails abwehren. Sie sind bei üblichen Anforderungen für kleine und mittlere Betriebsgrößen gut geeignet.
- **Traditionelle Firewallsysteme** kommen dagegen vor allem dann zum Einsatz, wenn es nötig ist, komplexe Unternehmensanwendungen – z.B. öffentlich zugängliche Web- und Datenbankserver – abzusichern, wenn eine große Anzahl von Benutzern auf hochleistungsfähige Internetverbindungen zugreifen muss oder wenn durch eine doppelte Auslegung der Firewall höchstmögliche Ausfallsicherheit erreicht werden soll.

Häufig bieten auch Internet-Provider unter dem Schlagwort „Managed Security“ Firewall-Dienste an. Dabei stellt der Provider die Firewall zur Verfügung und übernimmt auch deren Einrichtung und Wartung. Insbesondere bei geringer Benutzeranzahl oder wenn kein ausreichendes Fachwissen vorliegt, sollte diese Variante in Betracht gezogen werden.

Weiters muss zwischen Firewalls im eigentlichen Sinn und Personal Firewalls unterschieden werden. Bei ersteren handelt es sich um Hardware-Geräte, die zwischen Internet und Firmennetz installiert werden und das gesamte Netzwerk (mehrere Rechner) schützen. Eine Personal Firewall ist dagegen ein Programm auf einem einzelnen Rechner, das den Datenverkehr dieses PCs kontrolliert und unerlaubte Verbindungen blockiert.

Jede Firewall muss richtig installiert und konfiguriert werden, um wirksam Schutz zu bieten. Sie muss außerdem laufend administriert werden; Folgende grundlegende Regeln müssen erfüllt sein:

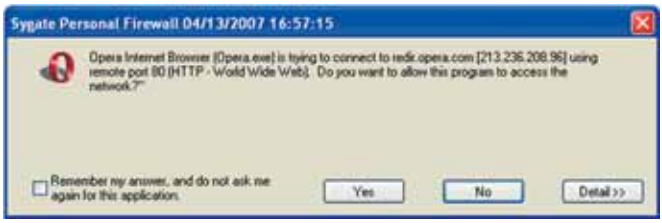
- Jede **Kommunikation** zwischen Firmennetz und Internet muss **ausnahmslos über die Firewall** geführt werden. Die Firewall darf nicht durch Modem- oder WLAN-Verbindungen umgangen werden können.
- **Sicherheitsrelevante Updates** der Firewall-Software müssen regelmäßig eingespielt werden, um zu verhindern, dass durch eine Schwachstelle der Firewall das gesamte Firmennetzwerk gefährdet wird.
- Die **Konfiguration und Administration** der Firewall darf nur über eine **sichere Verbindung** möglich sein. Angreifern aus dem Internet darf es nicht möglich sein, die Konfiguration der Firewall zu verändern oder auszulesen. Auch aus dem Firmennetzwerk darf der Zugang nur befugten Personen möglich sein.
- Die Konfiguration der Firewall muss in einer **Dokumentation** festgehalten werden, die nach jeder Änderung aktualisiert wird. Bei Konfigurationsänderungen sollten Grund, Zeitpunkt und der Name des durchführenden Mitarbeiters vermerkt werden.
- Eine richtig konfigurierte Firewall gestattet **nur die unbedingt notwendigen und tatsächlich gebrauchten Verbindungen**, alle anderen Verbindungen werden blockiert.

Die richtige Planung und Konfiguration einer Firewall ist komplex. Sie ist von höchster Wichtigkeit für die Sicherheit des Firmennetzwerkes und der verwendeten Daten und sollte in jedem Fall durch qualifiziertes Fachpersonal durchgeführt werden. Wenn im Unternehmen kein ausreichendes Fachwissen vorliegt, ist es am sichersten, die Grundkonfiguration durch einen spezialisierten externen Dienstleister vornehmen zu lassen. Nachträgliche Änderungen können dann eventuell durch die eigenen Mitarbeiter erfolgen, sobald diese sich das nötige Fachwissen erarbeitet haben.

PERSONAL FIREWALLS

In Fällen, in denen der Einsatz einer klassischen Firewall nicht möglich oder unangemessen erscheint, beispielsweise beim Betrieb eines einzelnen Rechners mit Internetanschluss, bieten Personal Firewalls grundlegenden Schutz gegen Fremdzugriffe. Bei korrekter Konfiguration können sie aber auch in Firmennetzen, die durch eine Hardware-Firewall geschützt sind, eingesetzt werden, um den Schutz vor unzulässigen Verbindungen zu verbessern.

Typischerweise funktioniert eine Personal Firewall so, dass nur Programme mit dem Internet kommunizieren dürfen, die dazu eigens autorisiert wurden. Oft „erlernt" sie zulässige Verbindungen aufgrund von Benutzereingaben: Beim ersten Verbindungsversuch eines Programms (z.B. des Internet-Browsers) mit dem Netzwerk wird der Benutzer gefragt, ob diese Verbindung gestattet sein soll. Erlaubt dieser die Verbindung, wird sie in Zukunft ohne weitere Abfrage zugelassen.



Bildschirmdialog einer Personal Firewall: Erst nach Erlaubnis des Benutzers darf das Programm (ein WWW-Browser) auf die Webseite im Internet zugreifen

Eine Personal Firewall kann den Schutz einzelner, mit dem Internet verbundener PCs verbessern. Es gibt allerdings auch einige Bedenken:

- Die Abfrage, welchen Programmen die Verbindung zum Internet gestattet werden soll, kann die **Anwender überfordern**. Einigen Programmen (insbes. jenen, die selbsttätig nach Produktaktualisierungen und Updates suchen, wie z.B Virenschutzprogramme) ist diese Verbindung zu erlauben, bei anderen Programmen (Schadprogramme wie Trojaner oder Spyware) ist der Verbindungsversuch als Alarmsignal zu werten. Diese Unterscheidung kann selbst gut ausgebildeten Administratoren manchmal schwer fallen.

- **Schadprogramme**, die den Computer befallen haben, können auch die Personal Firewall manipulieren oder sogar ausschalten. In diesem Fall ist der vermeintlich geschützte Rechner problemlos aus dem Internet angreifbar.

Personal Firewalls sind in verschiedenster Form erhältlich: Manche erfordern keine oder nur wenig Benutzereingriffe, andere können ohne ausgeprägtes Fachwissen kaum bedient werden. Der Schutz, den diese Programme bieten, ist ebenfalls sehr unterschiedlich.

Im Allgemeinen sollte eine Personal Firewall nur zum Schutz von Einzelplatzrechnern eingesetzt werden. Wenn mehrere Rechner geschützt werden müssen, ist der Einsatz einer Hardware-Firewall in jedem Fall vorzuziehen.

WIRELESS LAN (WLAN)

Drahtlose Netzwerke, sogenannte WLAN-Lösungen, ergänzen zunehmend traditionelle LANs, bei denen der Netzwerkanschluss über Kabelverbindungen realisiert wird. Zum einen bieten sie Flexibilität bei der Arbeitsplatzgestaltung, zum anderen sind für ihren Aufbau keine aufwändigen Verkabelungsarbeiten notwendig. Die steigende Zahl von mobilen Geräten (Notebooks, PDAs, etc.) fördert die Verbreitung von WLAN zusätzlich. Sicherheitstechnisch entstehen durch WLANs neue Gefährdungen und es sind einige Maßnahmen zu beachten, um nicht durch ihre Einführung die Sicherheit des gesamten lokalen Netzwerkes zu gefährden.

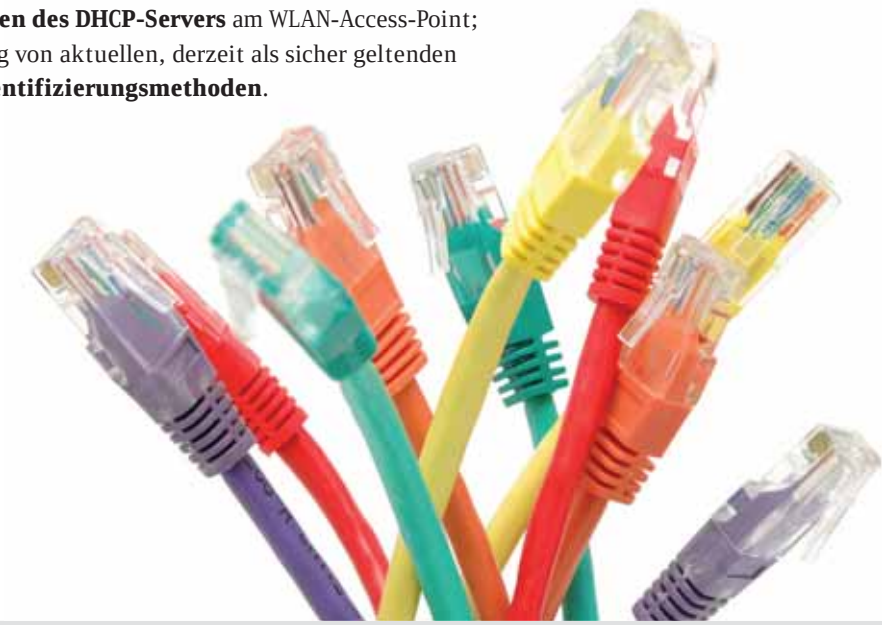
Sicherheitsmängel in WLAN-Netzwerken waren in letzter Zeit häufig die Ursache für erfolgreiche Attacken. Zum Teil lag das an Konfigurationsmängeln, zum Teil aber auch an Schwächen in den zugrundeliegenden Sicherheitstechnologien. Die Entwicklungen der letzten Zeit zielen u.a. auf die Behebung dieser Schwachstellen mittels neuer Technologien und Standards ab; sicherheitstechnisch ist es daher wichtig, möglichst nur aktuelle WLAN-Komponenten einzusetzen bzw. wenn möglich, ältere Geräte mittels Firmware-Updates zu aktualisieren.

An einem zufällig gewählten Standort verfügbare WLANs. Ungesicherte Netzwerke können jederzeit missbraucht werden.

Die Bedrohung durch WLAN-Angriffe darf nicht unterschätzt werden; mancherorts ist das „War-Driving“, d.h. das Aufspüren von Drahtlosnetzen, zu einer Art Sport geworden. Im Internet existieren Listen von WLAN-Zugängen, die nicht gesichert und für jedermann zugänglich sind. Die Nutzung eines solchen ungeschützten Netzes als kostenloser drahtloser Internetzugang ist noch die harmloseste Art des Missbrauchs, das Ausspionieren von Firmendaten die weitaus bedenklichere, aber nicht unbedingt kompliziertere Variante. Es besteht auch die Gefahr, dass Eindringlinge illegale Aktivitäten über das offene WLAN durchführen, für die dann der Betreiber verantwortlich gemacht wird.

Vor der Planung und Installation einer WLAN-Lösung bzw. zur besseren Absicherung bereits bestehender Anlagen sollten daher unbedingt die neuesten Entwicklungen und Sicherheitshinweise recherchiert werden. An dieser Stelle sind nur Hinweise auf einige Maßnahmen möglich, die von den zuständigen Administratoren beachtet werden sollten:

- **Geeignete Positionierung** und Ausrichtung der Zugriffspunkte und Antennen – außerhalb des Firmengeländes sollte der WLAN-Empfang möglichst verhindert werden;
- **Verschlüsselungsoptionen** aktivieren; ausschließlich WPA bzw. WPA2 sollten eingesetzt werden;
- Wird ein **Pre-Shared-Key** eingesetzt (WPA-PSK), sollte dieser **möglichst lang** sein und aus einer Folge zufälliger Zeichen bestehen;
- Ändern der **Standardeinstellungen** (insbes. Passwörter) am WLAN-Access-Point;
- Aktivieren der **MAC-Adressfilterung** am WLAN-Access-Point;
- **Deaktivieren des DHCP-Servers** am WLAN-Access-Point;
- Verwendung von aktuellen, derzeit als sicher geltenden **EAP-Authentifizierungsmethoden**.



FESTLEGUNG EINER WWW-SICHERHEITSSTRATEGIE

Eine WWW-Sicherheitsstrategie dient zur Klärung grundlegender sicherheitsrelevanter Fragestellungen, die noch vor Freigabe der Internetnutzung geklärt werden sollten.

Insbesondere folgende Fragen sollten behandelt werden:

- Wer erhält WWW-Zugang?
- Welche Bedingungen sind bei der WWW-Nutzung zu beachten?
- Wie werden die Benutzer geschult?
- Wie wird technische Hilfestellung für die Benutzer gewährleistet?

Das richtige Verhalten der Benutzer hat wesentlichen Anteil bei der Abwehr der Gefahren, die aus der Internet-Nutzung entstehen. Jeder Benutzer sollte daher bereits vor der Nutzung von Internet-Diensten durch entsprechende Anweisungen verpflichtet werden, die einschlägigen Sicherheitsrichtlinien des Unternehmens einzuhalten.

GEFAHREN BEIM WWW-ZUGRIFF

Einige typische Bedrohungen müssen bei der Planung der Sicherheitsmaßnahmen für den WWW-Zugriff berücksichtigt werden.

Beim Herunterladen von Dateien und/oder Programmen können eine Vielzahl von Sicherheitsproblemen auftreten, die bekanntesten sind Viren, Makro-Viren, Würmer und trojanische Pferde (Trojaner). Die Benutzer sollten immer die Möglichkeit in Betracht ziehen, dass heruntergeladene Dateien oder Programme Schadsoftware enthalten. Insbesondere das Installieren verschiedener Zusatzprogramme (Bildschirmschoner, Spaßprogramme ...) aus dem Internet sollte unterlassen werden, da diese oft Schadprogramme (insbes. Spyware) enthalten.

Firmendaten werden vor allem durch Programmfunktionen gefährdet, die ohne weitere Nachfrage auf dem lokalen Rechner ausgeführt werden. So können in heruntergeladenen Dokumenten oder Bildern Befehle enthalten sein, die automatisch beim Betrachten ausgeführt werden und Schäden verursachen können (z.B. Makro-Viren in Word- oder Excel-Dokumenten). Auf allen Rechnern mit Interzugang sollten daher aktuelle Virenschutzprogramme installiert sein, die diese Dateien bereits beim Download oder beim Zugriff prüfen.

Eine weitere Gefahr besteht in Phishing-Angriffen, bei denen ein Angreifer die Webseite einer Bank oder eines Webshops imitiert, um damit Benutzer zur Herausgabe von Passwörtern oder geheimen Daten zu bewegen. Solche Angriffe werden üblicherweise durch E-Mail-Aussendungen eingeleitet; ihre Anzahl hat in den letzten Jahren stark zugenommen. In diesem Zusammenhang ist besonders die Schulung der Benutzer wichtig: Als Grundregel muss dabei gelten, dass kein seriöses Unternehmen via E-Mail zur Eingabe von Passwörtern, PINs oder TANs auffordert; Aussendungen dieser Art müssen daher von den Mitarbeitern als Betrugsversuch erkannt und gemeldet werden; im Zweifelsfall sollte der Bankbetreuer kontaktiert werden.

SICHERHEIT VON INTERNET-BROWSERN

Verschiedene Sicherheitsprobleme beim WWW-Zugriff entstehen durch Schwachstellen in den eingesetzten Internet-Browsern.

Übliche Ursachen dafür sind:

- Fehlbedienungen und falsches Benutzerverhalten
- unzureichende Konfiguration der benutzten Browser
- Sicherheitslücken in den Browsern

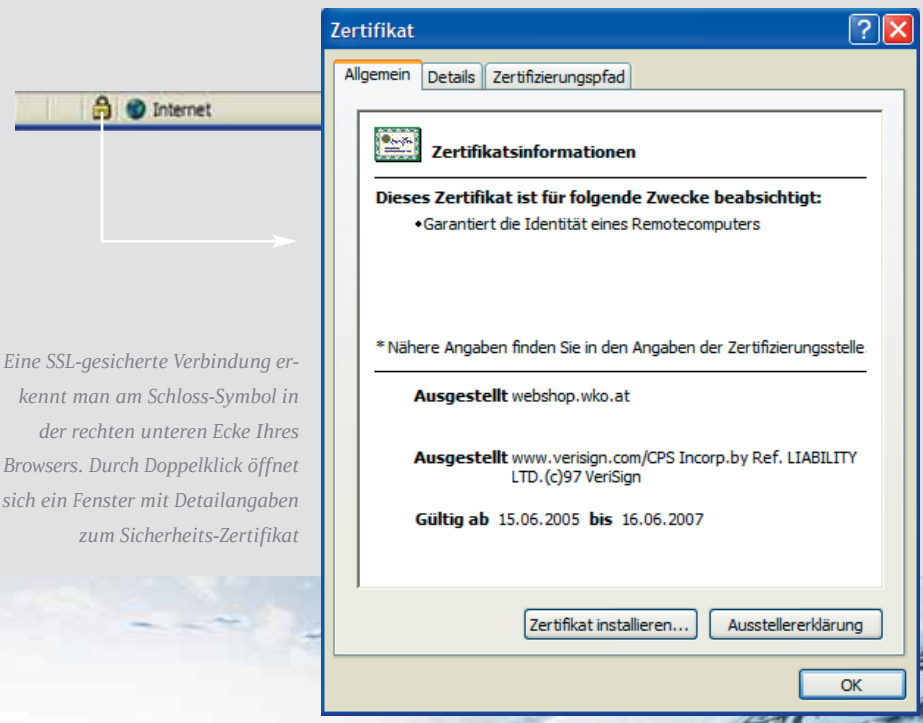
Sicherheit bei WWW-Zugriffen lässt sich nur dann erzielen, wenn jede dieser Problemquellen behandelt wird: Richtiges Benutzerverhalten ist mit Sicherheit der wichtigste Punkt; auch der bestgeschulteste Benutzer ist aber überfordert, bei den heute möglichen Angriffen immer richtig zu reagieren. Aktuelle Browser können durch Konfigurationsmaßnahmen weitgehend abgesichert werden, allerdings werden die Benutzer dann durch die umständliche Bedienung überfordert und eine Reihe von Webseiten lässt sich nur sehr eingeschränkt oder gar nicht nutzen. Auch die Auswahl eines „sicheren“ Browsers ist nicht möglich, da alle derzeit existierenden Programme gegen spezifische Angriffe anfällig sind und immer wieder neue erfolgreiche Angriffsmethoden gefunden werden.

Eine Abwehrstrategie gegen Sicherheitsprobleme beim WWW-Zugriff sollte daher drei Elemente enthalten:

- **Mitarbeiter** müssen **geschult** werden, um Fehlbedienungen zu vermeiden und Gefahren erkennen zu können. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen aus dem Internet und einzuhaltender Sicherheitsmaßnahmen sensibilisiert werden; sie sollten beispielsweise richtig auf Sicherheitsabfragen reagieren oder selbständig gesicherte Verbindungen erkennen können (SSL-Verschlüsselungen). Regelungen und Bedienungshinweise zur sicheren Internet-Nutzung sollten schriftlich fixiert werden.

- Die **Browser** müssen so **konfiguriert** werden, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann. Dazu sollten die sicherheitsrelevanten Einstellmöglichkeiten genutzt werden, die moderne Browser bieten: In Internet Explorer sind das insbesondere die Einstellungen des Zonenmodells, in Mozilla Firefox die Einstellungen zu JavaScript sowie verschiedene Add-Ons (NoScript, Flashblock ...). Die letzten Versionen dieser Browser (IE ab Version 7.0, Firefox ab Version 2.0) beinhalten zudem Schutzvorkehrungen gegen Phishing-Angriffe, die unbedingt eingesetzt werden sollten.

- **Internet-Browser** sollten immer **auf dem neuesten Stand** gehalten werden; häufig enthalten die Aktualisierungen Maßnahmen gegen neu gefundene Sicherheitslücken. Dazu muss u.a. auch überlegt werden, wie diese Updates im gesamten Unternehmen durchgeführt werden können, ob dazu der Eingriff eines Administrators nötig ist etc.



Eine SSL-gesicherte Verbindung erkennt man am Schloss-Symbol in der rechten unteren Ecke Ihres Browsers. Durch Doppelklick öffnet sich ein Fenster mit Detailangaben zum Sicherheits-Zertifikat

3. Virenschutz

Computer-Viren (in weiterer Folge einfach als Viren bezeichnet) gehören zu den „Schadprogrammen" („Malware"). Dies sind Programme, die verdeckte Funktionen enthalten und damit durch Löschen, Überschreiben oder sonstige Veränderungen unkontrollierbare Schäden an Programmen und Daten bewirken können. Sie verursachen zusätzliche Arbeit und Kosten und beeinträchtigen die Sicherheit von Daten oder Programmen.

Während früher Viren meist durch den Austausch verseuchter Datenträger verbreitet wurden, ist heute zunehmend die Verbreitung über Internet bzw. E-Mail das Problem. Bei den meisten über E-Mail verbreiteten „Viren" handelt es sich eigentlich um Würmer, die – unabhängig von der eigentlichen Schadensfunktion – schon durch ihr massenhaftes Auftreten und ihre rasante Verbreitung großes Aufsehen erregen und zu hohen Schäden führen.

Das nachfolgende Kapitel beschäftigt sich vorwiegend mit dem Schutz gegen Viren und Würmer. Die angeführten Maßnahmen sind großteils auch gegen andere Arten von Software mit Schadensfunktion, wie z.B. Trojanische Pferde, anwendbar.

TECHNISCHE VIRENSCHUTZMASSNAHMEN

Zur Abwehr von Vireninfektionen müssen alle Computer des Unternehmens mit Antivirus-Software ausgestattet werden. Zusätzlich sollten auch andere Einstellungen gesetzt werden, um Gefahren zu reduzieren, die aus noch unbekannter oder vom Virenschutz „übersehener" Schadsoftware entstehen können.

Der Betrieb von Antivirus-Programmen ist aus heutiger Sicht unerlässlich. Das gilt zumindest für alle Client- und Serversysteme, die unter Microsoft-Betriebssystemen betrieben werden, ist aber auch bei Linux- oder MacOS-Systemen anzuraten.

Bei der Auswahl der Virenschutzsoftware sind einige grundlegende Anforderungen zu beachten, die aber von allen modernen Lösungen erfüllt werden: Die Virensignaturdateien müssen laufend automatisch aktualisiert werden, alle infizierbaren Dateien müssen beim Dateizugriff (Zugriffs-, On-Access-Scan) geprüft werden, beim Auffinden von Viren muss der Benutzer verständigt und die infizierte Datei entweder gelöscht oder an eine sichere Stelle (Quarantäne) verschoben werden. Zusätzlich sollten noch automatisch gestartete Virensuchläufe über alle Datenträger des Computers eingestellt werden können, um regelmäßig eine genaue Prüfung des gesamten Datenbestandes durchzuführen.

Auch die beste Virenschutzsoftware erzielt nie eine hundertprozentige Trefferquote. Moderne Virentypen setzen verschiedene Methoden der Tarnung ein, gelegentlich kommt es auch vor, dass Viren sich schneller verbreiten, als die Hersteller der Antivirus-Software passende Signaturupdates erarbeiten können. Einige Maßnahmen können helfen, das Risiko einer Infektion weiter zu verringern:

- Die **Anzeige der Dateiendungen** sollte aktiviert werden, um potenzielle Schadprogramme, die als E-Mail-Attachment geschickt werden, leichter zu erkennen.
- In bestimmten Anwendungsprogrammen (MS Word, Excel, Powerpoint) sollte der **Makro-Virenschutz** aktiviert und auf entsprechende Warnmeldungen geachtet werden.
- In den **Sicherheitseinstellungen von Internet-Browsern** können aktive Inhalte (ActiveX, Java, JavaScript) und Skript-Sprachen (z.B. Visual Basic Script) deaktiviert werden.
- Das **Ausführen von aktiven Inhalten** in E-Mail-Programmen sollte durch entsprechende Optionen **unterbunden** werden.
- In verschiedenen E-Mail-Programmen gibt es die Option, Anlagen mit bestimmten Datei-Endungen nicht anzuzeigen. Sie sollte so gesetzt werden, dass **ausführbare Programme und Skripte unterdrückt** werden. Falls eine derartige Datei dennoch erwünscht ist, muss sie an einen technisch versierten Benutzer oder Administrator weitergeleitet werden.
- E-Mail-Clients sollten so eingestellt werden, dass **Attachments nicht automatisch geöffnet** werden. Als E-Mail-Editor dürfen keine Programme, die Makro-Sprachen (z.B. MS Word) oder Scripts unterstützen, eingesetzt werden. Auch beim Empfang von HTML-Mails ist Vorsicht geboten.
- Durch den Einsatz einer **Personal Firewall**, die Verbindungsversuche unbekannter Programme zum Internet blockiert, kann Angriffen gezielt entgegengewirkt werden. Eine zentrale Firewall kann durch derartige Software wirkungsvoll ergänzt werden.

VERMEIDUNG BZW. ERKENNUNG VON VIREN DURCH DEN BENUTZER

Die Sensibilisierung der Endanwender für die Virenproblematik ist eine wichtige Komponente aller Virenschutzmaßnahmen. Daher sollte in Schulungen regelmäßig auf die Gefahr von Viren, die Möglichkeiten zu ihrer Erkennung und Vermeidung sowie die notwendigen Handlungsanweisungen im Falle eines (vermuteten) Virenbefalls hingewiesen werden. Auch die laufende Information der Benutzer über aktuelle Bedrohungen ist empfehlenswert.

Alle Benutzer sollten folgende Verhaltensregeln beachten:

- Auch bei E-Mails von vermeintlich bekannten bzw. vertrauenswürdigen Absendern muss geprüft werden, ob der **Inhalt der Nachricht** zum Absender passt und ob das Mail bzw. das Attachment auch erwartet wurde. Englischsprachige Mails von deutschsprachigen Partnern sind ein klares Alarmsignal, aber auch unerwartete Inhalte oder der fehlende Bezug zu aktuellen Vorgängen sollten Vorsichtsmaßnahmen auslösen.
- Als Attachment gesendete **Programme oder Skripts** (d.h. Dateien mit den Endungen .com, .exe, .bat, .vbs etc.) dürfen nur ausgeführt werden, wenn sie vom Empfänger erwartet wurden und ihre Rechtmäßigkeit klar feststeht. Besondere Vorsicht ist bei doppelten, „merkwürdigen" Dateinamen-Endungen („.jpg.vbs" oder „gif.exe") geboten. Sie sollen dem Empfänger eine harmlose Datei vortäuschen, sind aber ausführbare Schadprogramme.
- Auch E-Mails im **HTML-Format** oder **Office-Dokumente** (*.doc, *.xls, *.ppt etc.) sowie Bildschirmschoner (*.scr) können Schadensfunktionen enthalten. Sie dürfen ebenfalls nur geöffnet werden, wenn der Absender vertrauenswürdig ist bzw. die Datei erwartet wurde.
- Mehrere **E-Mails mit gleichem Betreff** sind verdächtig, insbesondere wenn sie von verschiedenen Absendern stammen.
- **Phishing-Mails**, d.h. Mails, in denen zur Übermittlung von persönlichen Daten oder Passwörtern (z.B. PIN oder TAN) aufgefordert wird, dürfen auf keinen Fall beantwortet werden. Auch darin angegebene Webseiten dürfen nicht geöffnet werden. Bei Erhalt einer derartigen E-Mail sollten auch die anderen Mitarbeiter darauf hingewiesen werden, dass es sich dabei um einen Betrugsversuch handelt.
- Bei besonderen „Angeboten", für die nur ein **Link im E-Mail** angeklickt werden muss, ist besondere Vorsicht geboten: 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 mit der Seite übereinstimmen, die dann tatsächlich aufgerufen wird.

- **Spam-Mails**, Werbemails und andere unaufgefordert erhaltene Zusendungen sollte man **nie beantworten**. Auch die Aufforderung an den Absender, weitere Zusendungen zu unterlassen, ist sinnlos: 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.

NOTFALLMASSNAHMEN IM FALL VON VIRENINFEKTIONEN

Für Notfälle, die in Folge einer Virusinfektion auftreten können, sollten Vorkehrungen getroffen werden, um die weitere Ausbreitung der Viren zu verhindern und möglichst rasch die Rückkehr zum Normalbetrieb einleiten zu können.

Wie bei allen Notfällen sollte auch für den Fall einer massiven Vireninfektion rechtzeitig Vorsorge getroffen werden. Bei entsprechender Planung können Stillstände und Produktionsausfälle verhindert oder wenigstens eingeschränkt werden. Dabei sollten die folgenden Punkte behandelt werden:

- Den Benutzern sollte eine **Ansprechperson** bekannt sein, die sie in Notfällen erreichen können, um die weiteren Maßnahmen einzuleiten und zu koordinieren.
- Ein Programm an **Erstmaßnahmen**, die eine Weiterverbreitung von Viren verhindern, muss ausgearbeitet werden. Mögliche Inhalte sind z.B. das Herunterfahren des Mail-Servers und der betroffenen Clients oder das Trennen der Internetverbindung. Zu berücksichtigen ist dabei auch, wie vorgegangen werden soll, wenn keine Administratoren oder technisch sachkundige Mitarbeiter erreichbar sind.
- Es muss sichergestellt sein, dass bei Vorliegen eines neuen Virus die **Updates der Virenschutzprogramme** möglichst rasch auf allen Rechnern eingespielt werden. Entsprechende Maßnahmen müssen vorbereitet und getestet werden.
- Falls infizierte E-Mails an **andere Unternehmen** (Kunden, Partner) versandt wurden, sollten diese Unternehmen darüber rasch informiert werden, um die weitere Ausbreitung der Schadsoftware auf diese Unternehmen zu verhindern.
- **Wiederherstellungsstrategien** müssen erarbeitet werden, die festlegen, welche Rechner in welcher Reihenfolge in betriebsbereiten Zustand zu bringen sind, damit in kürzester Zeit eine zumindest eingeschränkte Funktionsfähigkeit hergestellt werden kann.
- Sollte der Virus Daten gelöscht oder verändert haben, so muss versucht werden, die Daten aus den **Datensicherungen** und die Programme aus den **Sicherungskopien** der Programme zu rekonstruieren.

4. Computersicherheit

AUSWAHL VON PASSWÖRTERN

Passwörter haben grundlegende Bedeutung beim Schutz der IT-Systeme und Daten. Die richtige Auswahl und der richtige Umgang mit Passwörtern können über die Sicherheit vor unbefugten Zugriffen und Manipulationen entscheiden.

Passwörter müssen ausreichend komplex sein, um nicht erraten werden zu können. Andererseits dürfen sie aber nicht so kompliziert sein, dass sie vergessen werden oder schriftlich notiert werden müssen. Dieser Kompromiss ist letztlich vom jeweiligen Benutzer abhängig, einige Grundregeln sollten dabei aber unbedingt beachtet werden:

- **Namen**, Vornamen, Geburtsdaten, tel. Durchwahlen, KFZ-Kennzeichen etc. dürfen **nicht** verwendet werden. Sie sind leicht ausfindig zu machen und werden bei Versuchen, ein Passwort zu erraten, mit Sicherheit getestet.
- Passwörter sollten **nicht** aus Begriffen bestehen, die in einem **Wörterbuch** (auch einer anderen Sprache) aufzufinden sein könnten. Programme, die zum Ausfindigmachen von Passwörtern verwendet werden, nützen Wortlisten mit mehreren tausend Begriffen, um Passwörter dieser Art innerhalb kürzester Zeit zu entschlüsseln. Auch Eigennamen, geografische Begriffe, etc. sollten möglichst vermieden werden.
- **Trivialpasswörter** (aaaaaa, qwertz, asdf,123456, 08/15, 4711 ...) dürfen nicht verwendet werden. Abgesehen davon, dass auch solche Passwörter in Wortlisten vorkommen können, sind sie meistens schon beim Beobachten der Passworteingabe zu erkennen.
- Das Passwort muss **ausreichend lang** sein. Für normale Benutzer muss es mindestens sechs, besser acht Zeichen lang sein, für Benutzerkonten mit besonderen Rechten (administrator, root, Dienstkonten etc.) sollte ein längeres Passwort gewählt werden.
- Ein Passwort sollte aus **verschiedenen Arten von Zeichen** zusammengesetzt sein. Im Idealfall besteht es aus Großbuchstaben, Kleinbuchstaben, Ziffern und/oder Sonderzeichen (Satzzeichen, Währungssymbole etc.).
- Passwörter – insbesondere das Passwort bei der Anmeldung am Computer – dürfen **nicht an andere Personen** weitergegeben werden. Auch an Kollegen oder Vorgesetzte dürfen Passwörter nur in absoluten Notfällen mitgeteilt werden; anschließend sollten sie sofort geändert werden.

Passwörter sollten in regelmäßigen Abständen geändert werden (z.B. alle 90 Tage). Sie sollten aber auch immer dann geändert werden, wenn der Verdacht besteht, dass sie von einem Unbefugten ausfindig gemacht wurden. Jeder Mitarbeiter sollte wissen, auf welche Weise er sein Passwort ändern kann.

Nach Möglichkeit sollten für verschiedene Anmeldungen auch verschiedene Passwörter gebraucht werden. Auf keinen Fall darf z.B. für die Anmeldung am PC und das E-Mail-Konto beim Internet-Provider das gleiche Passwort verwendet werden. In einfachen Fällen kann es ausreichen, kleine Variationen einzufügen, z.B. zwei Buchstaben zu ändern.

RECHTESTRUKTUR AUF ARBEITSPLATZRECHNERN

Zum besseren Schutz gegen Malware und Rechnerausfälle sollte darauf geachtet werden, dass administrative Rechte auf PCs nur dann genützt werden, wenn es tatsächlich nötig ist.

Moderne Betriebssysteme sehen Benutzerkonten mit unterschiedlichen Berechtigungen vor:

- Konten mit **Superuser- bzw. Administrator-Rechten** dienen zur Administration des Computers, zur Softwareinstallation, zum Ändern grundlegender Einstellungen, zum Anlegen neuer Benutzer etc.
- Konten mit **einfachen Benutzerrechten** werden für alltägliche Tätigkeiten, d.h. für die eigentliche Arbeitstätigkeit, verwendet.

Ein häufiger Fehler besteht darin, an alle Mitarbeiter Konten mit Superuser-Rechten zu vergeben. Durch diese Konfiguration entstehen aber verschiedene Probleme:

- Das Einschleppen und die Ausbreitung von **Schadsoftware** wird stark erleichtert;
- die Wahrscheinlichkeit von **Rechnerausfällen** ist deutlich erhöht, da Schutzmaßnahmen gegen das versehentliche Löschen von Systemdaten wegfallen;
- die Benutzer haben volle Rechte zur **unbefugten Installation** von Software;
- verschiedenste **Schutz- und Kontrollmaßnahmen des Betriebssystems** werden wirkungslos oder können von den Benutzern umgangen werden.

Für die tägliche Arbeit dürfen daher ausschließlich Konten mit einfachen Benutzerrechten verwendet werden. Superuser-Rechte sollten einigen wenigen Administratoren vorbehalten bleiben und auch von diesen nur dann genützt werden, wenn es für die betreffende Tätigkeit unbedingt nötig ist. Auch für Administratoren müssen daher eigene, einfach berechtigte Benutzerkonten eingerichtet werden.

GEFAHRENQUELLE WECHSELMEDIEN

Wechselmedien, wie z.B. Disketten, CD-ROMs, USB-Sticks oder externe Festplatten, ermöglichen den raschen und einfachen Transfer von Daten und Programmen, bringen aber auch eine Reihe von Risiken mit sich.

Derartige Risiken sind unter anderem:

- das **Booten fremder Betriebssysteme**, durch die Schutzmechanismen umgangen werden können;
- die **unbefugte Installation** unerwünschter Software oder Schadsoftware;
- das **unberechtigte Kopieren** von Unternehmensdaten auf Wechselmedien (Datendiebstahl, Verlust der Vertraulichkeit).

In vielen Fällen ist eine völlige Sperre der Wechselmedien entweder technisch nicht möglich oder aus betrieblichen Gründen nicht durchsetzbar. Hier sind zusätzliche personelle (Dienstanweisungen, Verbote) und organisatorische Maßnahmen (Kontrollen) erforderlich.

EINSATZ EINES VERSCHLÜSSELUNGSPRODUKTES FÜR ARBEITSPLATZSYSTEME

Wenn auf einem Computer, der in einer ungeschützten Umgebung betrieben oder aufbewahrt wird, besonders schutzwürdige Daten gespeichert werden, sollte der Einsatz einer Verschlüsselungssoftware überlegt werden.

Typischer Anwendungsfall für ein derartiges Verschlüsselungsprodukt sind Notebooks, auf denen wichtige Unternehmensdokumente gespeichert sind. Angesichts der hohen Diebstahls- und Verlustgefahr bei derartigen Geräten sollten diese Firmendaten nach Möglichkeit immer verschlüsselt werden, um sicherzustellen, dass sie nur von ihrem Eigentümer genutzt werden können. Auch bei gewöhnlichen Arbeitsplatzrechnern kann Verschlüsselung sinnvoll sein, z.B. wenn sensible Personendaten oder Dokumente der Geschäftsführung geschützt werden sollen. Dabei sind drei Möglichkeiten zu unterscheiden:

- **Transparente Verschlüsselung:** Dabei wird die gesamte Festplatte des Rechners verschlüsselt, alle Dateien sind geschützt. Der Benutzer bemerkt davon nichts, er muss nur beim Rechnerstart ein Verschlüsselungspasswort eingeben.

- **Online-Verschlüsselung:** Auf der Festplatte wird ein virtuelles Dateisystem erstellt, in dem Daten abgelegt werden können. Der Benutzer muss darauf achten, sensible Daten nur in diesem Dateisystem abzuspeichern, das nur nach Eingabe des Verschlüsselungspassworts geöffnet werden kann.
- **Offline-Verschlüsselung:** Einzelne Dateien werden verschlüsselt auf dem Datenträger gespeichert. Der Benutzer muss bei jeder einzelnen Datei entscheiden, ob sie verschlüsselt werden muss und gegebenenfalls beim Aufruf jeder einzelnen Datei ein Passwort eingeben.

Im Allgemeinen ist die transparente Verschlüsselung die benutzerfreundlichste und am wenigsten fehleranfällige Variante. Allerdings ist diese Lösung meistens teurer und beansprucht die Rechnerleistung stärker als die beiden anderen Verschlüsselungsarten.

Um zu vermeiden, dass auf wichtige Daten nicht mehr zugegriffen werden kann, weil das Passwort zu ihrer Entschlüsselung verloren gegangen ist, sollte festgelegt werden, dass Verschlüsselungspasswörter an sicherer Stelle hinterlegt werden. Das kann z.B. geschehen, indem sie in verschlossenen Kuverts im Firmensafe deponiert werden, die nur in Notfällen geöffnet werden dürfen.

REGELMÄSSIGE SOFTWARE-AKTUALISIERUNGEN

Durch Software-Updates können Schwachstellen beseitigt oder Funktionen erweitert werden.

Updates sind vor allem dann erforderlich, wenn Schwachstellen bekannt werden, die Auswirkungen auf die Sicherheit der Systeme haben oder wenn Fehlfunktionen wiederholt auftauchen. Vor dem Einspielen sollte die Zuverlässigkeit der neuen Komponenten und ihr Zusammenwirken mit bestehenden Programmen geprüft werden. Im Idealfall geschieht das auf einem eigenen Testsystem, alternativ dazu kann das Update auch auf einem einzelnen Rechner getestet werden, bevor es auf allen betroffenen Systemen eingespielt wird.

Aus sicherheitstechnischer Sicht besonders wichtig ist das regelmäßige Einspielen von Updates zu Betriebssystemkomponenten und Internet-Browsern, wie sie von deren Herstellern regelmäßig angeboten werden. Solche Aktualisierungen dienen fast immer der Behebung von aktuellen Sicherheitslücken. Werden sie nicht durchgeführt, ist kein Schutz gegen neuere Bedrohungen gegeben.

Meistens werden dazu auch Mechanismen angeboten, die für die automatische Durchführung sicherheitskritischer Updates sorgen und gleichzeitig sicherstellen, dass dabei ausschließlich vertrauenswürdige Quellen verwendet werden. Diese Einrichtungen ermöglichen es, bei geringem Administrationsaufwand die IT-Systeme auf dem aktuellen Sicherheitsstand zu halten.

NUTZUNGSVERBOT NICHT-BETRIEBLICHER SOFTWARE

Um sicherzustellen, dass keine unerwünschten Programme installiert werden und das System nicht über den vorgesehenen Funktionsumfang hinaus unkontrolliert genutzt wird, muss das Einspielen bzw. die Nutzung nicht-betrieblicher Software verboten und, soweit technisch möglich, verhindert werden.

Im Allgemeinen sollte auch die Nutzung privater Software (Programme, Daten) und Hardware (CD/DVD/Disketten, Wechselfestplatten, Notebooks, USB-Memory-Sticks etc.) untersagt werden. Der Einsatz jeder Hard- und Software, die nicht für den eigentlichen Betriebszweck benötigt wird, erhöht die Gefahr des „Einschleusens" von Schadprogrammen und verringert die Stabilität der Systeme.

Weitere Probleme können durch unlizenzierte Software entstehen, die von den Benutzern auf den Rechnern installiert wurde. Derartige Lizenzrechtsverletzungen können unter Umständen auch zu finanziellen Belastungen für das Unternehmen führen.

Folgenden Maßnahmen sollten umgesetzt werden:

- Ein **Nutzungsverbot nicht-betrieblicher Software** sollte schriftlich fixiert und allen Mitarbeitern mitgeteilt werden.
- Das **unautorisierte Einspielen** und/oder Nutzen von Software ist, soweit möglich, mit **technischen Mitteln** zu verhindern.
- In unregelmäßigen Abständen sollten die Rechner im Unternehmen **auf unzulässige Software überprüft** werden; wenn derartige Software gefunden wird, muss sie umgehend deinstalliert werden.
- Falls nötig, kann eine **Liste von Programmen, deren Nutzung explizit untersagt ist,** erstellt und an die Mitarbeiter ausgegeben werden. Beispiele dafür sind z.B. Instant Messaging-Clients (ICQ), Filesharing-Software (Kazaa, BitTorrent), Spiele oder Hacker-Tools.

5. Personelle Maßnahmen

IT-Sicherheit kann auch bei besten technischen Maßnahmen nur funktionieren, wenn die Mitarbeiter ausgeprägtes Sicherheitsbewusstsein besitzen und bereit und in der Lage sind, die Vorgaben in der täglichen Praxis umzusetzen. Schulung und Sensibilisierung für Fragen der IT-Sicherheit sind daher unbedingt notwendig.

REGELUNGEN FÜR MITARBEITER

Bei der Einstellung von Mitarbeitern sind diese zur Einhaltung einschlägiger Gesetze, Vorschriften und interner Regelungen zu verpflichten.

Es empfiehlt sich, Regelungen zu folgenden Bereichen zu treffen, die in Form einer Verpflichtungserklärung von allen Mitarbeitern zu unterzeichnen sind:

- Einhaltung der **PC-Benutzungsregeln**
- Einhaltung der **Regeln für die Benutzung von Internet und E-Mail**
- Einhaltung der **Verpflichtungserklärung auf das Datengeheimnis** (§ 15 DSG)

Neue Mitarbeiter müssen unbedingt auf interne Regelungen, Gepflogenheiten und Verfahrensweisen im IT-Einsatz hingewiesen werden. Ohne entsprechende Einweisung kennen sie ihre Ansprechpartner in Sicherheitsfragen nicht und wissen nicht, welche IT-Sicherheitsmaßnahmen einzuhalten sind.

In die Stellenbeschreibungen der Mitarbeiter müssen alle sicherheitsrelevanten Aufgaben und Verantwortlichkeiten explizit aufgenommen werden. Dies gilt besonders für Mitarbeiter mit speziellen Sicherheitsaufgaben (Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, Applikations- und Projektverantwortliche ...).

Bei der Einstellung von IT-Administratoren ist besondere Sorgfalt nötig: Sie haben weitgehende und umfassende Befugnisse, insbesondere sind sie in der Lage, auf alle Daten zuzugreifen, sie zu verändern und Berechtigungen so zu vergeben, dass erheblicher Missbrauch möglich ist. Das hierfür eingesetzte Personal muss sorgfältig ausgewählt werden und absolut vertrauenswürdig sein.

VERFAHREN BEIM AUSSCHEIDEN VON MITARBEITERN

Beim Ausscheiden von Mitarbeitern aus dem Unternehmen sollten folgende grundlegende Punkte beachtet werden:

- Sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (z.B. tragbare Rechner, Speichermedien, Dokumentationen) sind zurückzufordern.
- Sämtliche Zugangsberechtigungen und Zugriffsrechte müssen entzogen bzw. gelöscht werden, dies betrifft vor allem auch Berechtigungen für eventuelle Telearbeitszugänge.
- Wenn eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt wurde (z.B. mittels eines gemeinsamen Passwortes), muss nach Ausscheiden einer der Personen die Zugangsberechtigung sofort geändert werden. Wenn Administratoren oder andere Schlüsselpersonen ausscheiden, müssen auch alle anderen Passwörter geändert werden, die ihnen bekannt waren.
- Nach Möglichkeit sollte eine Neuvergabe des bestehenden Benutzerkontos an einen anderen Mitarbeiter vermieden bzw. ausgeschlossen werden.

REGELUNGEN FÜR DEN EINSATZ VON FREMDPERSONAL

Betriebsfremde Personen wie z.B. Reinigungspersonal oder Mitarbeiter von IT-Dienstleistern können leicht Zugang zu vertraulichen Unternehmensdaten erhalten und stellen unter Umständen eine erhebliche Bedrohung dar.

Einige einfache Regeln sollten beachtet werden, um vertrauliche Informationen zu schützen:

- Externe Mitarbeiter, die über einen längeren Zeitraum in einem Unternehmen tätig sind und Zugang zu vertraulichen Unterlagen und Daten erhalten könnten, müssen schriftlich (im Rahmen von **Geheimhaltungsverpflichtungen**) auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen verpflichtet werden.
- Für Fremdpersonal, das nur kurzfristig oder einmalig zum Einsatz kommt, gelten die gleichen Regeln wie für Besucher, d.h. dass etwa der Aufenthalt in sicherheitsrelevanten Bereichen **nur in Begleitung** von Mitarbeitern des Unternehmens erlaubt ist.

- Ist es nicht möglich, betriebsfremde Personen ständig zu begleiten oder zu beaufsichtigen, sollte zumindest der **persönliche Arbeitsbereich abgeschlossen** werden (Schreibtisch, Schrank; Abmeldung/Sperre am PC).

SICHERHEITSSENSIBILISIERUNG UND -SCHULUNG

Um die IT-Sicherheit zu verbessern, sollten alle Mitarbeiter über angemessene Kenntnisse im Umgang mit IT-Systemen und den Gefahren und Gegenmaßnahmen in ihrem eigenen Arbeitsgebiet verfügen. Es liegt in der Verantwortung der Geschäftsführung, durch geeignete Schulungsmaßnahmen die nötigen Voraussetzungen zu schaffen. Darüber hinaus sollte jeder Benutzer dazu motiviert werden, sich auch in Eigeninitiative Kenntnisse anzueignen.

Die überwiegende Zahl von Schäden im IT-Bereich entsteht durch Nachlässigkeit oder Bequemlichkeit. Das Aufzeigen der Abhängigkeit des Unternehmens von Informationen und vom reibungslosen Funktionieren der IT-Systeme ist ein geeigneter Einstieg in die Sensibilisierung der Benutzer für Sicherheitsanliegen.

Weitere mögliche Inhalte einer Benutzerschulung sind:

- Der richtige Umgang mit Passwörtern
- Richtiges Verhalten beim Auftreten von Sicherheitsproblemen
- Der Umgang mit personenbezogenen Daten
- Wirkungsweise und Arten von Schadprogrammen
- Erkennen eines Befalls mit Schadprogrammen
- Sofortmaßnahmen im Verdachtsfall und Maßnahmen zur Entfernung von Schadprogrammen
- Das richtige Verhalten im Internet
- Das richtige Verhalten bei unzulässigen Anfragen
- Risiken bei der Verwendung mobiler IT-Geräte und Datenträger
- Die Bedeutung der Datensicherung und ihrer Durchführung

Als Behelf für Benutzerschulungen und zum Selbststudium kann auch das bei der WKÖ erhältliche „IT-Sicherheitshandbuch für Mitarbeiter“ aus der it-safe-Reihe herangezogen werden.

ABWEHR VON SOCIAL ENGINEERING-ANGRIFFEN

Als Social Engineering bezeichnet man das Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten.

Die Angriffe werden meistens über das Telefon, unter Umständen aber auch durch persönliches Auftreten des „Social Engineers" geführt: Der Angreifer gibt sich als Mitarbeiter, Kunde oder IT-Techniker des Unternehmens aus und überzeugt einen Benutzer durch geschickte Täuschung von seiner Identität. Bei geeigneter Gelegenheit – oft erst nach mehrmaligen Telefonaten – erhält er Informationen, die der Firmenmitarbeiter einem Unbekannten nie zukommen lassen würde; er kann sein Opfer auch zu unerlaubten Handlungen bewegen etc.

Der Erfolg von Social Engineering-Angriffen kann nie ausgeschlossen werden. Ihre Gefährlichkeit liegt in der Ausnutzung menschlicher Eigenschaften und Schwächen: Hilfsbereitschaft und Höflichkeit, Kundenfreundlichkeit, aber auch Autoritätshörigkeit und Angst. Einige Maßnahmen können aber helfen, das Risiko zu verringern:

- **Schulungen** der Mitarbeiter über Social Engineering-Strategien und -Methoden helfen, sie auf Angriffe dieser Art vorzubereiten.
- Alle Mitarbeiter müssen regelmäßig auf den **Wert der** von ihnen **bearbeiteten Daten** hingewiesen werden, insbesondere auf den Schaden, den ein Angreifer damit verursachen könnte.
- **Schriftliche Festlegungen**, welche Informationen vertraulich behandelt werden müssen und welche auch an Unbekannte weitergegeben werden dürfen, können den Benutzern zur Orientierung dienen und dem Unternehmen auch als Argumentationshilfe nach Sicherheitsvorfällen nützlich werden.
- Auch Festlegungen zur **Anfragenform** sind sinnvoll: Das Anfordern einer Rückrufnummer oder einer schriftlichen Anfrage kann einen Social Engineer unter Umständen bereits zurückschrecken und gibt den Mitarbeitern Gelegenheit zu Nachfragen. Auskünfte zu sensiblen Daten sollten ohnehin nur bei persönlichem Erscheinen erteilt werden.
- Besonders neuen Mitarbeitern sollte empfohlen werden, **Anfragen**, bei denen sie unsicher sind, ob eine Beantwortung zulässig ist, an ihre Vorgesetzten oder andere erfahrene Personen **weiterzuleiten**.
- **Mitarbeiterkommunikation** ist wichtig: Bei „verdächtigen" Anfragen sollten auch die anderen Mitarbeiter informiert werden, um zu verhindern, dass ein abgewiesener Angreifer sein Glück bei anderen, zugänglicheren Kollegen versucht.

CLEAR DESK/CLEAR SCREEN-POLICY

In ungesicherten Arbeitsumgebungen hilft eine Clear Desk-Policy beim Schutz vertraulicher Dokumente und Daten vor unbefugten Zugriffen.

Jeder Mitarbeiter sollte bei Abwesenheit seine vertraulichen Unterlagen verschließen. Dies gilt insbesondere für Großraumbüros, aber auch in anderen Fällen ist dafür Sorge zu tragen, dass keine unberechtigten Personen (Kunden, Besucher, Reinigungspersonal, unbefugte Mitarbeiter etc.) Zugriff auf Schriftstücke oder Datenträger mit sensiblen Inhalten haben.

Ähnliches gilt auch für die Computer: Beim Verlassen des Arbeitsplatzes muss jeder Benutzer sich am PC abmelden. Wenn nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann der Computer stattdessen gesperrt werden. Zusätzlich sollte auch eine automatische Sperre bei Nicht-Nutzung, z.B. durch einen passwortgeschützten Bildschirmschoner, vorgesehen werden. Dabei sollte darauf geachtet werden, dass den Mitarbeitern ausreichende Möglichkeiten zum Versperren der sensiblen Arbeitsunterlagen zur Verfügung stehen. Alle Benutzer müssen außerdem über die Tastenkombinationen (z.B. „Windows-Taste + L“) zum schnellen Sperren des PCs informiert werden. Falls möglich, sollten besonders in der ersten Zeit auch Kontrollen und wiederholte Aufforderungen erfolgen, um die Durchsetzung dieser Anweisungen zu sichern.

NUTZUNG UND AUFBEWAHRUNG MOBILER IT-GERÄTE

Unter mobilen IT-Geräten sind alle für den mobilen Einsatz geeigneten Geräte zu verstehen, so etwa Notebooks, Personal Digital Assistants (PDA) und Smartphones.

Wenn mobile IT-Geräte außerhalb des Unternehmens eingesetzt werden, muss besonders auf die Sicherheit der Daten geachtet werden. Die Mitarbeiter sollten speziell geschult und für typische Gefahren sensibilisiert werden. U.a. sollten folgende Regeln befolgt werden:

- Bei der Speicherung firmeninterner, vertraulicher bzw. personenbezogener sensibler Daten ist ein **Zugriffsschutz** unbedingt notwendig, der Zugriff darf erst nach Eingabe eines Passworts o.ä. möglich sein. Der Einsatz von Festplatten- oder Dateiverschlüsselung ist empfehlenswert.
- Auch auf mobilen Datenträgern (USB-Sticks, Wechselfestplatten etc.) sollten diese Daten nach Möglichkeit **verschlüsselt** gespeichert werden; unverschlüsselte Datenträger dürfen keinesfalls unbeaufsichtigt (etwa im Hotel oder im Auto) zurückgelassen werden.

- Wenn ein mobiles Gerät in fremden Büroräumen genutzt wird, sollte dieser Raum auch beim kurzzeitigen Verlassen immer **verschlossen** werden. Wird der Raum für längere Zeit verlassen, muss zusätzlich das Gerät ausgeschaltet werden.
- Wird keine Festplattenverschlüsselung verwendet, sollte zumindest ein **Boot-Passwort** gesetzt sein, um die unerlaubte Benutzung zu erschweren.

TELEARBEIT

Unter Telearbeit versteht man Tätigkeiten, die räumlich entfernt vom Standort des Arbeitgebers durchgeführt werden und deren Erledigung durch eine kommunikations-technische Anbindung an die IT-Infrastruktur des Arbeitgebers unterstützt wird.

Bestimmte Anforderungen sollten möglichst noch vor der Einrichtung und Vergabe von Telearbeitszugängen überlegt und definiert werden. Z.B. sollte ein Telearbeitsplatz immer in einem eigenen, von der übrigen Wohnung getrennten Zimmer eingerichtet werden, Versperrmöglichkeiten für Datenträger und Dokumente müssen zur Verfügung stehen etc.

Für die verwendeten Computer sollten ebenfalls bestimmte Auflagen erteilt werden: Aktuelle Virenschutzsoftware ist unbedingt nötig, ebenso der Einsatz eines Zugriffsschutzes durch Benutzeranmeldung und Passworteingabe. Soweit das durchsetzbar erscheint, kann eine Liste von Software erstellt werden, die auf dem Telearbeit-PC aus Sicherheitsgründen nicht betrieben werden darf. Werden diese Auflagen nicht erfüllt, darf der Telearbeitszugang nicht vergeben oder muss wieder entzogen werden.

Oft ist es günstiger, den für die Telearbeit verwendeten PC vom Unternehmen bereitzustellen. In diesem Fall sollte schriftlich festgelegt werden, dass der Rechner ausschließlich für die berufliche Nutzung verwendet werden darf und dass andere Personen keinen Zugang erhalten dürfen. Auch die Festlegung der Softwareausstattung des Telearbeit-PCs und die Vereinbarung zusätzlicher Kontrollrechte des Arbeitgebers ist in solchen Fällen einfacher möglich.

Weitere Regelungen, z.B. zur Durchführung regelmäßiger Datensicherungen, zu Sicherheitsmaßnahmen bei sensiblen Daten oder zum Vorgehen bei Problemen, sollten zu einer schriftlichen Richtlinie zusammengefasst werden, die allen Telearbeitern übergeben wird.

6. Bauliche und infrastrukturelle Maßnahmen

Die in diesem Abschnitt beschriebenen Maßnahmen dienen dem Schutz von IT-Systemen mittels baulicher und infrastruktureller Vorkehrungen.

Baulich-organisatorische Maßnahmen

SCHÜTZENSWERTE GEBÄUDETEILE

Besonders schützenswerte Räume (Serverräume, Datenträgerarchive etc.) sollten nicht in exponierten oder gefährdeten Bereichen untergebracht sein.

Insbesondere ist zu beachten:

- Kellerräume sind durch Wasser gefährdet;
- Räume im Erdgeschoß – zu öffentlichen Verkehrsflächen hin – sind durch Vandalismus und höhere Gewalt (Verkehrsunfälle in Gebäudenähe) gefährdet;
- Räume im Erdgeschoß mit schlecht einsehbaren Höfen sind durch Einbruch und Sabotage gefährdet;
- Räume unterhalb von Flachdächern sind durch eindringendes Regenwasser gefährdet.

Im Allgemeinen sind schutzbedürftige Räume im Zentrum eines Gebäudes besser untergebracht als in dessen Außenbereichen; das ist bei der Planung neuer Räume für sensible oder betriebswichtige Komponenten zu berücksichtigen. Wenn die zentrale Anlage solcher Schutzbereiche aufgrund der bestehenden Bausubstanz oder Leitungsführung nicht möglich sein sollte, müssen zusätzliche Schutzmaßnahmen zur Abwehr der oben angeführten Gefährdungen eingerichtet werden (Wassermelder, Alarmanlagen, Fenstergitter etc.).

ZUTRITTSKONTROLLE

Die Überwachung des Zutritts zum Gebäude bzw. zu sensiblen Bereichen zählt zu den wichtigsten Schutzmaßnahmen. Ein Zutrittskontrollsystem vereinigt verschiedene bauliche, organisatorische und personelle Vorkehrungen.

In einem Zutrittskontrollkonzept sollten u.a. folgende Inhalte festgehalten werden:

- **Welche** Bereiche sind besonders **schützenswert** (Serverräume, Archive, Räume für Kommunikationseinrichtungen oder Haustechnik etc.)?
  Die einzelnen Bereiche können unterschiedliche Sicherheitsstufen aufweisen.
- **Welche internen und externen Personengruppen** haben Zutritt zu welchen Bereichen?
- **Welche Daten** müssen bei Zutritt und Verlassen von einem geschützten Bereich **protokolliert** werden?

Aus diesen Festlegungen lassen sich Anforderungen für Zutrittskontrollmaßnahmen ableiten, die z.B. bei der Auswahl einer Schließlösung, der Schlüsselvergabe, der Planung von Alarmanlagen oder der Führung von Zutrittslogbüchern beachtet werden müssen.

SCHLÜSSELVERWALTUNG

Alle Maßnahmen und Informationen, die in Zusammenhang mit der Schlüsselvergabe stehen, sollten in einem Schließplan dokumentiert werden.

Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln muss zentral geregelt werden. Reserveschlüssel sind vorzuhalten und gesichert aufzubewahren. Schlüssel dürfen nur an berechtigte Personen ausgegeben werden; es ist also ein ausgearbeitetes Zutrittskontrollkonzept nötig.

Über die Aus- und Rückgabe aller Schlüssel müssen schriftliche Aufzeichnungen geführt werden. Anhand dieser Listen sollte es jederzeit möglich sein, nachzuvollziehen, wer zu welchem Zeitpunkt Zutritt zu welchen Unternehmensbereichen hatte. Aus diesem Grund sollte es auch den Mitarbeitern verboten sein, ihre Schlüssel anderen zu überlassen; jede Schlüsselausgabe muss über die zentrale Ausgabestelle erfolgen.

Für den Verlust von Schlüsseln sollte ebenfalls vorgesorgt werden: Jedem Mitarbeiter muss bekannt sein, wer in diesem Fall zu verständigen ist. Eine Reihe von Maßnahmen – vom Ersatz des Schlüssels bis zum Austausch des Schlosses oder ganzer Schließgruppen – sollte von den zuständigen Verantwortlichen durchgeplant werden.

Das Gleiche gilt sinngemäß auch für alle anderen Zutrittskontrollmedien wie Magnetstreifen oder Chipkarten bzw. so genannte Multifunktionschipkarten.

EMPFANG

Die Einrichtung eines Empfangsdienstes (Portier, Front-Sekretariat etc.) hat weit reichende positive Auswirkungen gegen eine ganze Reihe von Gefährdungen.

Voraussetzung ist allerdings, dass bei der Umsetzung des Empfangsdienstes einige Grundprinzipien beachtet werden, die auch für vermeintlich vertrauenswürdige Personen (z.B. ehemalige Mitarbeiter) gelten müssen.

- Die Mitarbeiter am Empfang beobachten und kontrollieren den Eingang zum Gebäude/Büro bzw. zum sicherheitsrelevanten Bereichen.
- Unbekannte Personen müssen sich beim Empfang anmelden und ausweisen.
- Die Empfangsmitarbeiter halten vor Einlass eines Besuchers beim Besuchten Rückfrage.
- Der Besucher wird zum Besuchten begleitet oder am Eingang abgeholt.

GEEIGNETE AUFSTELLUNG UND AUFBEWAHRUNG VON SERVERN UND ANDEREN BESONDERS SCHÜTZENSWERTEN IT-KOMPONENTEN

Aufgrund ihrer zentralen Funktion für das Unternehmen müssen Server besonders geschützt werden. Ähnliches gilt auch für zentrale Netzwerk- und Telekommunikationskomponenten (Router, Switches, Firewalls, Telefonanlage).

Um den Schutz solcher besonders betriebswichtigen IT-Komponenten sicherzustellen, ist es zwingend erforderlich, diese in einer gesicherten Umgebung aufzustellen.

Diese kann realisiert werden als:

- **Serverraum:** Raum zur Unterbringung von Servern, serverspezifischen Unterlagen, Datenträgern in kleinem Umfang sowie weiterer Hardware (etwa Drucker oder Netzwerkkomponenten). Im Serverraum ist im Allgemeinen kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten. Ein Serverraum muss Schutz vor unbefugtem Betreten bieten, spezielle Vorrichtungen wie z.B. Brandschutztüren können darüber hinaus im Fall eines Brandes die Sicherheit der Geräte und Daten erhöhen.
- **Serverschrank:** Versperrbare Serverschränke (Racks) dienen zur Unterbringung von IT-Geräten und schützen sie gegen unbefugten Zugriff. Der Schutz vor Schäden durch Feuer und Rauchgasen ist bei den meisten Serverschränken dagegen nicht gegeben.

Generell ist zu beachten:

- Der Zugang zu Servern und anderen schützenswerten Komponenten darf ausschließlich wenigen, befugten Personen möglich sein.
- Eine Vertretungsregelung muss sicherstellen, dass der Zugriff auch im Vertretungsfall geregelt möglich ist und nicht autorisierte Zugriffe auch in Ausnahmesituationen nicht vorkommen können.
- Für die sichere Verwahrung der Zugangsschlüssel muss gesorgt sein. Außerdem muss darauf geachtet werden, dass die entsprechenden Räume bzw. Schränke tatsächlich immer versperrt werden.

Brandschutz

Brandschutz stellt die Gesamtheit aller Maßnahmen dar, die die Entstehung und Ausbreitung von Bränden verhindern und die Bekämpfung von Bränden gewährleisten.

Bei systemkritischen Räumen (Serverräume, Verteilerräume) ist der Einsatz von Brandschutztüren zur Bildung eines eigenen Brandabschnitts sowie von Sicherheitstüren, die einen höheren Schutz gegen Einbruch bieten, vorzusehen.

Brandmeldeanlagen ermöglichen die Überwachung bestimmter, besonders gefährdeter Bereiche oder des gesamten Gebäudes. Brandmelder dienen zur Früherkennung von Brandgefahren und werden in automatische und nichtautomatische Melder unterschieden, welche an einer Brandmeldeanlage hängen oder als Einzelmelder fungieren.

In Räumen mit Computern oder Datenträgern, in denen Brände oder Verschmutzungen hohe Schäden verursachen können, sollte ein Rauchverbot erlassen werden. Dieses Rauchverbot dient gleichermaßen dem vorbeugenden Brandschutz wie der Betriebssicherheit. Die Einhaltung des Rauchverbotes ist zu kontrollieren.

Papier und andere leicht brennbare Materialien sollten unbedingt außerhalb der systemkritischen Räume (Serverraum, Verteilerraum) gelagert werden, um die Brandlast möglichst gering zu halten.

HANDFEUERLÖSCHER (MITTEL DER ERSTEN UND ERWEITERTEN LÖSCHHILFE)

Die meisten Brände entstehen aus kleinen, anfangs noch gut beherrschbaren Brandherden. Besonders in Büros findet das Feuer reichlich Nahrung und kann sich sehr schnell ausbreiten. Der Sofortbekämpfung von Bränden kommt also sehr hoher Stellenwert zu.

Eine Sofortbekämpfung ist nur möglich, wenn entsprechende Handfeuerlöscher in ausreichender Zahl und Größe im Gebäude – möglichst in räumlicher Nähe zu besonders schützenswerten Bereichen und Räumen – zur Verfügung stehen.

Dabei ist zu beachten:

- Die Feuerlöscher müssen **regelmäßig geprüft und gewartet** werden.
- Die Feuerlöscher müssen so angebracht werden, dass sie **im Brandfall leicht erreichbar** sind.
- Zur Brandbekämpfung bei IT-Geräten dürfen ausschließlich **CO_2-Löscher** eingesetzt werden; dabei muss auf die Gefahr der Sauerstoffverdrängung geachtet werden.
- Die Beschäftigten müssen über die Standorte der nächsten Feuerlöscher **informiert** und in deren Handhabung **unterwiesen** sein.

Im Brandfall geht von der damit verbundenen Rauchentwicklung sowohl für Mensch als auch für IT-Geräte eine erhebliche Gefahr aus. Ein umfassender Rauchschutz, z.B. durch rauchdichte Brandschutztüren, ist daher ebenfalls vorzusehen.

Stromversorgung und Klimatechnik

ANGEPASSTE AUFTEILUNG DER STROMKREISE

Eine unterdimensionierte Stromversorgung kann zu Computer-Abstürzen führen, die Datenverlust verursachen können.

Die Dimensionierung, für die eine Elektroinstallation ausgelegt wurde, stimmt erfahrungsgemäß nach einiger Zeit nicht mehr mit den tatsächlichen Gegebenheiten überein. Es ist daher anzuraten, bei Änderungen der Raumnutzung und Änderungen und Ergänzungen der technischen Ausrüstung (IT-Komponenten, Klimaanlage, Beleuchtung etc.) die Elektroinstallation zu prüfen und ggf. anzupassen.

LOKALE UNTERBRECHUNGSFREIE STROMVERSORGUNG (USV)

Die Überbrückung von Stromausfällen durch eine USV sowie das geordnete Herunterfahren der angeschlossenen Geräte beugt Datenverlusten vor, die in Folge von plötzlichem „Ausschalten" (Stromverlust) entstehen können.

USV-Anlagen können neben der Überbrückung von Totalausfällen der Stromversorgung und Unterspannungen auch dazu dienen, Überspannungen (z.B. durch Blitzschlag) zu glätten. Zumindest alle betriebswichtigen Server sowie die Sicherheits- und Alarmsysteme sollten an einer USV betrieben werden. Empfehlenswert ist auch der Anschluss eines Monitors für die betreffenden Server, um während eines Stromausfalls noch manuell eingreifen zu können.

Bei der Dimensionierung einer USV sollte man von einer Überbrückungszeit von mindestens 10 bis 15 Minuten ausgehen. In dieser Zeit kann die angeschlossene IT ohne externe Stromquelle betrieben oder geordnet heruntergefahren werden. Das Herunterfahren muss dabei von einer Softwarelösung automatisch ausgelöst werden. In regelmäßigen Abständen sollten außerdem Tests durchgeführt werden, bei denen die Funktion der USV-Anlage und der automatischen Serverabschaltung überprüft wird.

KLIMATISIERUNG

Insbesondere in kleinen Serverräumen muss für die ausreichende Abfuhr der Rechnerabwärme gesorgt werden.

Server sind für den Betrieb innerhalb eines engen Temperaturbereichs ausgelegt. Oberhalb ihrer maximalen Betriebstemperatur (meistens 30-35°C) besteht die Gefahr des Rechnerausfalls. Diese Temperatur kann gerade in kleinen, durch Brand- oder Zutrittsschutzmaßnahmen zusätzlich abgeschotteten Serverräumen leicht überschritten werden. In solchen Fällen ist der Einbau einer Klimaanlage zwingend erforderlich.

Bei der Auswahl des Klimageräts muss auf die ausreichende Kälteleistung geachtet werden. Dabei sollte auch die Möglichkeit der Anschaffung zusätzlicher Server mitbedacht werden, die zusätzliche Kühlung nötig machen. Oft ist eine Überdimensionierung empfehlenswert, um nicht bei zukünftigen Anschaffungen gleich auch die Klimaanlage wechseln zu müssen.

Zum Schutz der Serversysteme sollte außerdem eine Raumtemperaturüberwachung überlegt werden, die bei Überschreiten einer bestimmten Grenztemperatur per E-Mail oder SMS Alarmmeldungen aussendet.

7. Einhaltung rechtlicher Vorgaben

Eine Reihe von Gesetzen ist auch für den Informationssicherheitsbereich relevant: Das österreichische Unternehmensgesetzbuch und das GmbH-Gesetz, das Datenschutzgesetz etc. Verschiedene rechtliche Bestimmungen haben zusätzlich Auswirkungen z.B. auf die Festlegung von Aufbewahrungsfristen für Protokolle oder Daten.

BESTIMMUNGEN ZUR GESCHÄFTSFÜHRERHAFTUNG (UGB, GMBH-GESETZ)

Aus den Bestimmungen der oben angeführten Gesetze ergibt sich, dass die Verantwortung für Informationssicherheit grundsätzlich immer bei der Unternehmensführung verbleibt. Sicherheitsrelevante IT-Aufgaben können im Rahmen formeller Festlegungen (z.B. einer IT-Sicherheitspolitik) an einzelne Mitarbeiter delegiert werden; das Management trägt dennoch insbesondere für die Einhaltung gesetzlicher Bestimmungen die Letztverantwortung.

DAS ÖSTERREICHISCHE DATENSCHUTZGESETZ (DSG 2000)

Das Datenschutzgesetz regelt den Umgang mit personenbezogenen, schutzwürdigen Daten. Zu „Personen“ sind auch juristische Personen und Personengemeinschaften zu zählen; bei den Daten wird u.a. zwischen sensiblen (z. B. Gesundheitsdaten, religiöse oder politische Überzeugung) und nicht-sensiblen Daten (Adressen, Geburtsdatum, Kundendaten) unterschieden. Auch nicht-sensible Daten müssen – wenn auch in geringerem Ausmaß – geschützt werden.

Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke verwendet werden. Die Datenanwendungen, mit denen sie verarbeitet werden, müssen an das Datenverarbeitungsregister (DVR) gemeldet werden; allerdings zählt das DSG auch eine Reihe von Standardanwendungen auf, für die diese Meldung nicht nötig ist. Den Personen, deren Daten verwendet werden, stehen besondere Rechte (Auskunfts-, Richtigstellungs- und Löschungsrecht) zu.

Zu den wichtigsten Inhalten des DSG zählt die Festlegung bestimmter Datensicherheitsmaßnahmen: Die Daten müssen vor Zerstörung und Verlust und vor ordnungswidriger oder unrechtmäßiger Verwendung geschützt werden.

Folgende Punkte sind im § 14 DSG explizit angeführt:

- die ausdrückliche Festlegung der **Aufgabenverteilung** zwischen den Mitarbeitern;
- die Bindung der Datenverwendung an einen **gültigen Auftrag** z.B. eines Vorgesetzten;
- die **Information und Schulung** der Mitarbeiter über ihre Pflichten nach dem DSG und internen Datensicherheitsvorschriften;
- die Regelung der **Zutrittsberechtigungen** zu Räumen, in denen Daten verarbeitet werden;
- der Schutz der IT-Systeme und Datenträger vor **unbefugten Zugriffen**;
- der Schutz der IT-Systeme vor **unbefugter Inbetriebnahme**;
- die **Protokollierung** der Datenverwendung;
- die **Dokumentation** der oben angeführten Sicherheitsmaßnahmen in Form eines Datensicherheitshandbuchs.

Aus den Vorschriften des DSG ergeben sich einige typische Anforderungen für den Umgang mit personenbezogenen Daten: Alle Mitarbeiter müssen in Form einer Geheimhaltungsverpflichtung auf das Datengeheimnis verpflichtet werden. Sie müssen geschult werden, typischerweise in Form von Seminaren oder Richtlinien. Aufgaben und Kompetenzen müssen durch Stellenbeschreibungen, Organisationshandbücher und andere Anweisungen geregelt werden. Zutritts- und Zugriffsschutzmaßnahmen sowie Protokollierung müssen durch entsprechende, vorwiegend technische Einrichtungen gewährleistet sein.

Obwohl die Sicherheitsmaßnahmen des DSG an sich nur für die Verwendung personenbezogener Daten gelten, haben sie auch für die Verarbeitung anderer Daten Bedeutung erlangt. Sie bilden eine Art Mindeststandard, der auch im Umgang mit Finanzdaten, Geschäftsgeheimnissen u.ä. nicht unterschritten werden sollte.

DAS VERBANDSVERANTWORTLICHKEITSGESETZ (VBVG)

Das erst Anfang 2006 in Kraft getretene Verbandsverantwortlichkeitsgesetz regelt die Verfolgung juristischer Personen (auch Unternehmen) für Straftaten, die ihre Entscheidungsträger oder Mitarbeiter begangen haben. Es kommt zur Anwendung, wenn eine Straftat entweder zu Gunsten des Verbandes begangen oder wenn sie durch die Unterlassung bestimmter Sorgfaltspflichten ermöglicht oder wesentlich erleichtert wurde. Letzteres ist insbesondere der Fall,

wenn Straftaten von Mitarbeitern nicht durch technische, organisatorische oder personelle Maßnahmen verhindert wurden. Als Strafen sind Geldbußen vorgesehen, die je nach Ertragslage des Verbands und der Schwere des Vergehens bis zu 1,8 Millionen Euro betragen können. Aus dem VbVG ergeben sich auch verstärkte Anforderungen an die IT-Sicherheitsmaßnahmen eines Unternehmens: Wenn ein Mitarbeiter eine Straftat unter Verwendung der vom Unternehmen zur Verfügung gestellten IT-Systeme begeht und das Unternehmen die gebotene Sorgfalt zur Verhinderung dieser Tat außer Acht gelassen hat, kann das Unternehmen selbst verfolgt werden. Dazu kann es u.U. ausreichen, wenn ein Mitarbeiter seinen Internetzugang für den Bezug von Kinderpornographie verwendet und vom Unternehmen keinerlei Vorkehrungen gegen diese Verwendung getroffen wurden.

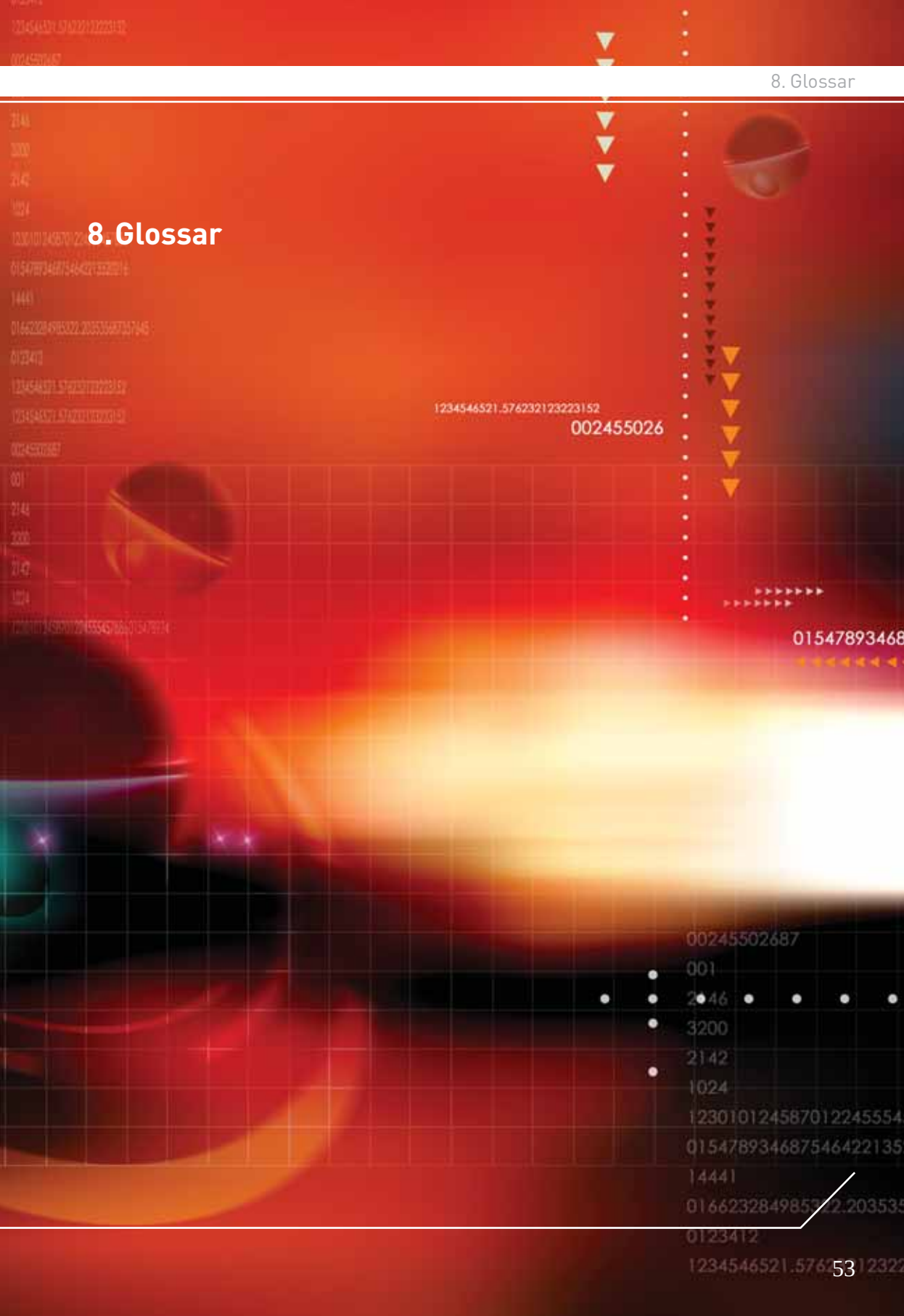
Zur Abwehr einer strafrechtlichen Verfolgung muss das Unternehmen nachweisen, dass es seinen Sorgfaltspflichten nachgekommen ist. Das ist insbesondere durch die Einführung einer straffen, gut dokumentierten Unternehmensorganisation möglich. Für typische Unternehmensrisiken sollten eigene Verantwortliche eingesetzt und ein Risikomanagement eingeführt werden. Für IT-Risiken bedeutet das im Wesentlichen die Bestellung eines IT-Sicherheitsbeauftragten und die Erstellung von IT-Sicherheitsrichtlinien bzw. einer IT-Sicherheitspolitik.

BESTIMMUNGEN ZU AUFBEWAHRUNGSFRISTEN (DSG, BAO)

Bei der Archivierung von Daten müssen verschiedene gesetzliche Vorschriften zu Aufbewahrungsfristen beachtet werden. Z.B. schreibt das DSG vor, dass Protokolle, die die Nachverfolgung von Datenzugriffen ermöglichen, drei Jahre aufbewahrt werden müssen. Die Bundesabgabenordnung verlangt, dass Bücher, Aufzeichnungen und Belege sieben Jahre aufbewahrt werden; dies gilt auch für deren Aufbewahrung in elektronischer Form (Buchhaltungsdaten, elektronische Rechnungen, gegebenenfalls auch E-Mails).

Die Verantwortung für die sichere Aufbewahrung und Wiedergabe dieser Daten liegt dabei beim Unternehmen, d.h. eine derartige Langzeitarchivierung muss gut geplant werden: Über den Datenträgerbestand sollte ein Bestandsverzeichnis geführt werden; die archivierten Datenträger müssen regelmäßig geprüft werden; günstigerweise sollte eine Kopie vorliegen, falls das Original unlesbar wird. Vor allem aber muss bei der Planung der Langzeitarchivierung darauf geachtet werden, dass die Daten in einigen Jahren noch nutzbar sind. Bei einem Wechsel oder einer neuen Version der Buchhaltungssoftware muss geprüft werden, ob die alten Datenbestände verwendet werden können. Andernfalls müssen die Installationsmedien der alten Software aufbewahrt oder besser noch eine betriebsfähige Installation des alten Programms, eventuell auf einem älteren Rechner, beibehalten werden.

8.Glossar


1234546521.576232123223152
002455026
01547893468
00245502687
001
2146
3200
2142
1024
14441

AKTIVE INHALTE:

Als aktive Inhalte werden von einem Webserver an den Internet-Browser übermittelte Programme/Skripte bezeichnet, die auf dem PC des Benutzers lokal ausgeführt werden. Bekannte Vertreter sind ActiveX, Javascript und Java. Üblicherweise dienen sie zur Erleichterung der Webseitenbedienung oder steigern die Attraktivität durch spezielle Effekte. Sie können aber auch eingesetzt werden, um Schadroutinen auszuführen und sind als Sicherheitsrisiko anzusehen.

DIALER:

Einwahl-Programme, die eine Internetverbindung über 0190-Mehrwertnummern aufbauen. Der User bleibt weiterhin online und bemerkt möglicherweise gar nicht den Wechsel der Internetverbindung. Die Kosten für die Dialer-Verbindung betragen dabei mehrere Euro pro Minute. Betroffen sind ausschließlich Benutzer von Einwahlverbindungen über Analog- oder ISDN-Modems, für Internetzugänge über ADSL, XDSL, Kabelmodem oder andere Breitbanddienste entstehen keine Mehrkosten.

PDA:

Als PDA (Personal Digital Assistant) bezeichnet man kleine, tragbare Geräte, die insbesondere zur Kalender- und Adressverwaltung verwendet werden. PDAs können oft auch Computerdaten speichern oder E-Mails empfangen. Verschiedene moderne Handys besitzen ebenfalls PDA-Funktionalität.

PHISHING:

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. Üblicherweise 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 einzugeben. Diese Webseiten sind ebenfalls gefälscht und sehen den Originalen zum Verwechseln ähnlich. Die eingegebenen Daten landen auf den Servern von Betrügern, die mit den Nutzerdaten Transaktionen zum Schaden des Users durchführen.

QUARANTÄNE:

In Analogie an den medizinischen Begriff bezeichnet man damit jenen „Ort“, wo mit Schadprogrammen infizierte Daten aufbewahrt werden. Anti-Virenprogramme verlagern Dateien in die Quarantäne, um die Schadroutine eventuell zu einem späteren Zeitpunkt zu entfernen.

RAID:

Ein RAID-System ist ein Zusammenschluss mehrerer Festplatten zu einem logischen Laufwerk, das wie eine einzelne Festplatte genutzt wird. Verschiedene RAID-Typen sind gebräuchlich, die unterschiedliche Vor- und Nachteile aufweisen. Die v.a. bei Servern gebräuchlichen RAID 1- und RAID 5-Systeme schützen gespeicherte Daten vor Defekten einzelner Festplatten.

ROOTKITS:

Rootkits sind Schadprogramme, die in der Lage sind, sich auf einem Rechner vollständig unsichtbar zu machen. Sie verbergen sich vor Antivirusprogrammen und Benutzereinblicken und werden oft erst durch den entstandenen Schaden auffällig, z.B. wenn der Provider den Internetzugang sperrt, weil Spam-Mails verschickt wurden. Häufig dienen sie auch zum Verstecken von „Hintertüren“, mit deren Hilfe das Fernsteuern des Rechners möglich ist, um ihn für Hack-Angriffe auf andere Rechner zu missbrauchen. Rootkits werden durch Computerviren oder durch die Installation zweifelhafter Software eingeschleppt. Ihre Entdeckung und Entfernung ist schwierig; im Internet findet man aber verschiedene (häufig kostenlose) Anti-Rootkit-Programme, die dazu in der Lage sind.

SNAPSHOT:

Snapshot-Technologien dienen zur Aufbewahrung älterer Versionen eines Datenbestands. Bekanntestes Beispiel dafür ist der Volumeschattenkopie-Dienst von Windows 2003 Server, mit dessen Hilfe eine versehentlich überschriebene Datei ohne großen Aufwand wieder hergestellt werden kann. Snapshots können aber auch von ganzen Datenträgern gemacht werden. Insbesondere größere Speichersysteme (Storage Area Networks) nutzen diese Möglichkeit, um Datensicherungen zu beschleunigen.

SPAM:

Als Spam werden unerwünschte Werbemails bezeichnet, die mittlerweile einen Großteil des weltweiten 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, er kostet allerdings Arbeitszeit und Internet-Bandbreite. Mittels eigener Spam-Filter können bereits auf Provider/Mailserver-Ebene oder auch erst am lokalen Rechner unerwünschte Mails gefiltert und gelöscht werden.

SPYWARE:

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.

SSL/HTTPS:

HTTPS ist die Abkürzung für HyperText Transfer Protocol Secure, das durch die Verwendung des Verschlüsselungsverfahrens SSL ausreichende Sicherheit für die Übertragung sensibler Daten bietet. Mit Hilfe dieses Verfahrens werden einerseits die übertragenen Daten verschlüsselt und abhörsicher gemacht, andererseits wird durch die Verwendung von digitalen Zertifikaten die Identität des Webservers 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.

TROJANISCHE PFERDE:

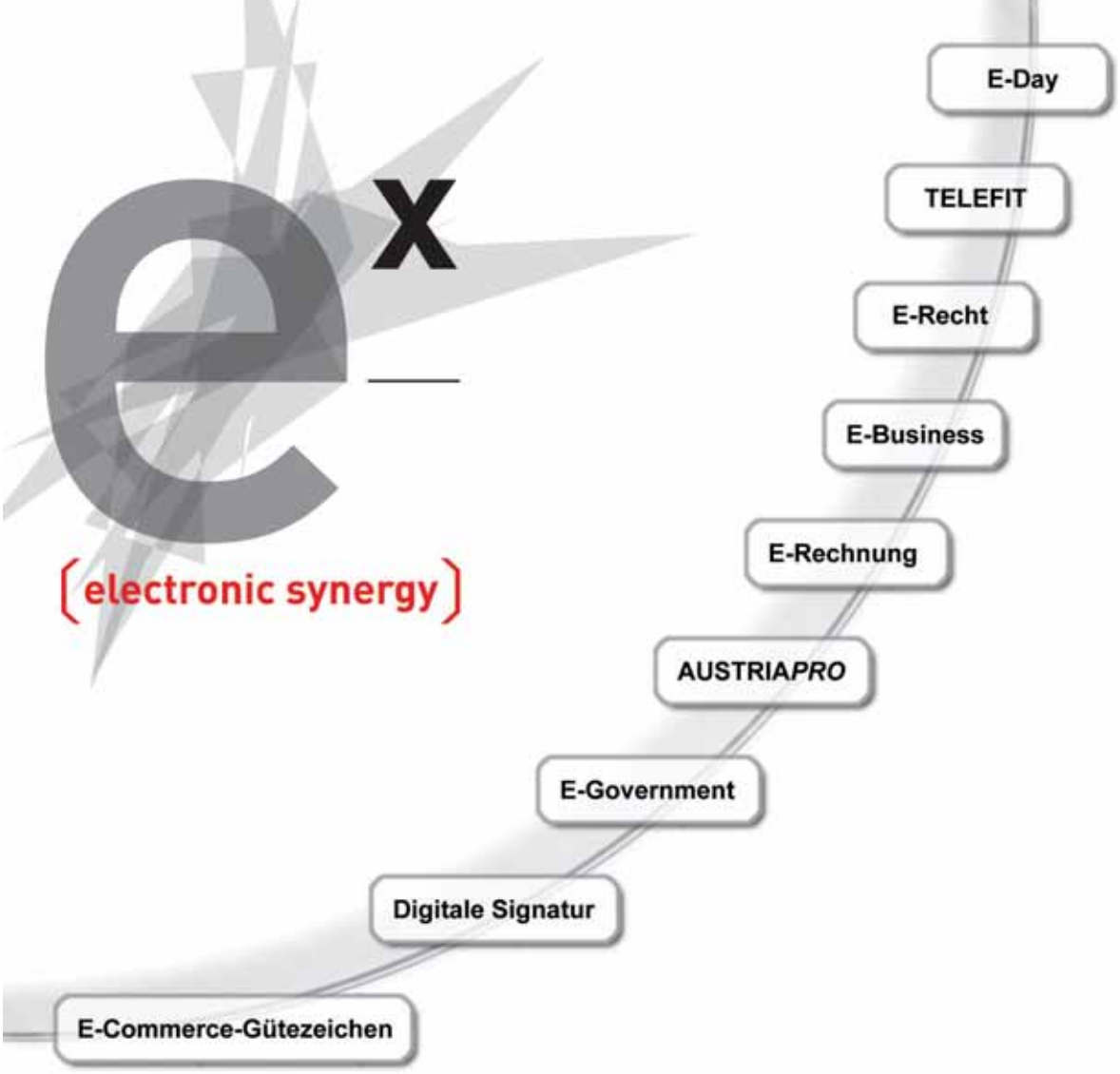
Selbständige Programme mit verdeckter Schadensfunktion, ohne Selbstreproduktion. Trojaner tarnen sich als nützliche, gutartige Programme: Ein Programm, das zum Zweck der Viren-Entfernung aus dem Internet heruntergeladen wird, kann so unter Umständen genau das Gegenteil bewirken. Daher sollte immer die Seriosität der Quelle, von der ein Programm bezogen wird, überprüft werden.

VIREN:

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:

Selbständige, selbst reproduzierende 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 Infizierung führen.



e^x ...steht für „electronic synergy"

WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

Unter dieser Marke werden sämtliche E-Aktivitäten der Wirtschaftskammer Österreich im neu eingerichteten E-Center konzentriert. „e hoch x" symbolisiert auch die zahlreichen Themen und Tätigkeitsbereiche, die im E-Center zusammenlaufen.

Als Schnittstelle zwischen Wirtschaft und Verwaltung ist das E-Center erster Ansprechpartner für Multiplikatoren in diesen Bereichen. Zudem koordiniert das E-Center inhaltliche Positionen der Wirtschaftskammer und stimmt diese mit den Praktikern der betroffenen Experts Groups des Fachverbandes UBIT ab.

http://wko.at/electronic-synergy

DIE SPARTE DER WACHSTUMSBRANCHEN

WKO
INFORMATION · CONSULTING

Datensicherheit schafft Vorsprung

06 07 08 09

wko.at/ic

Microsoft

Schützen Sie jetzt Ihren PC!

Am besten durch drei einfache Schritte.

Firewall

Software Updates

Antiviren Software

Bestellen Sie noch heute kostenfrei

> das Microsoft Windows XP Service Pack 2
> den Sicherheits-Newsletter

www.microsoft.com/austria/PC-Schutz

Fragen zum Thema Sicherheit beantwortet Ihnen auch das Microsoft Infoservice unter:

> austria@microsoft.com > 08000 123-345 (gebührenfrei)

Ihr Microsoft Österreich Sicherheitsteam