

«Aus der Praxis - für die Praxis» KMU-Schriftenreihe

Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU)

Das erweiterte 10-Punkte-Programm schafft mehr Schutz

(Umschlag innen)

Konzept und Text:

Arbeitsgruppe KMU + Informationssicherheit des Vereins InfoSurance:

Ueli Brügger, *IBM, Zürich*

Christof Egli, *Ernst Basler + Partner, Zürich (Leiter Arbeitsgruppe)*

Hanspeter Feuz, *IT Projects, Thun*

Tiziana Giorgetti, *Symantec Switzerland AG, Bassersdorf*

René Hanselmann, *Microsoft GmbH, Wallisellen*

Peter Neuhaus, *Stiftung KMU Schweiz, Bern*

Niklaus Schild, *Trivadis AG, Zürich*

Die Arbeitsgruppe wurde unterstützt von:

Jürg Altenburger, *IBM, Zürich*

Chris Baur, *Trivadis AG, Zürich*

Diego Boscardin, *Symantec Switzerland AG, Bassersdorf*

Herbert Brun, *UPAQ Ltd, Küsnacht*

Roger Halbheer, *Microsoft GmbH, Wallisellen*

Andrea Müller, *Microsoft GmbH, Wallisellen*

Peter Kunz, *Omnisec, Dällikon*

Anton Lagger, *Bundesamt für wirtschaftliche Landesversorgung, Bern*

Marc Vallotton, *InfoGuard AG, Zug*

Christian Weber, *Staatsekretariat für Wirtschaft SECO, Bern*

Carlos Rieder, *Hochschule für Wirtschaft, Luzern*

Gestaltung und Druck:

Gisler Druck AG, Altdorf

Copyright:

Verein ISSS (Information Security Society Switzerland), Bollwerk 21, CH-3001 Bern, Tel. +41 31 311 5300, <http://www.iss.ch>

Die kostenlose Weiterverbreitung des Inhaltes dieser Broschüre ist unter Quellenangabe gestattet und im Sinn des Vereins.

Der Verein ISSS übernimmt keinerlei Haftung für allfällige Schäden, die aus der richtigen oder falschen Anwendung des erweiterten 10-Punkte-Programms entstehen.

Luzern, im Oktober 2008

Angepasst an ISSS im Mai 2016 aufgrund Auflösung InfoSurance und Übernahme der Assets durch ISSS im Mai 2016 (ohne inhaltliche Anpassung)

**Liebe KMU-Geschäftsleiterin,
lieber KMU-Geschäftsleiter**

Die Schweiz zählt im weltweiten Vergleich zu den Spitzenanwendern von Informations- und Kommunikationstechnologien. Niemand gibt weltweit mehr Geld pro Kopf aus für Informationstechnologie als Herr und Frau Schweizer.

Es ist klar, ohne IT läuft nichts – das gilt selbstredend auch für Sie, die kleinen und mittleren Unternehmen der Schweiz. Sie bilden die wichtigsten Stützen der Schweizer Wirtschaft und sie geniessen einen hervorragenden Ruf. Ihre Produkte und Dienstleistungen basieren auf Qualität, Flexibilität und Innovationskraft.

Schon früh hat sich der Verein InfoSurance mit den Risiken auseinandergesetzt, die den KMU beim Einsatz von Informationstechnologie drohen können. Daraus ist im August 2005 eine erste Broschüre entstanden, das **10-Punkte-Programm für einen wirkungsvollen IT-Grundschutz**. Die Broschüre unterstützt Sie bei der Einführung eines wirkungsvollen Grundschutzes.

Jetzt hat der Verein InfoSurance die Broschüre um zehn weitere Punkte ergänzt, die besonders diejenigen KMU unter Ihnen ansprechen, die einen erhöhten Bedarf nach Verfügbarkeit und Vertraulichkeit ihrer System und Daten haben.

Das **erweiterte 10-Punkte-Programm** ist wiederum einfach gehalten und Sie können die Massnahmen realisieren, ohne dass für Sie grosse Kosten entstehen. Wo das spezifische Fachwissen in einem KMU nicht verfügbar ist, lassen Sie sich von einem externen Experten unterstützen.

Schenken Sie bitte dem erweiterten 10-Punkte-Programm die gleiche Aufmerksamkeit, die schon das erste Programm erhalten hat.

Ich wünsche Ihnen und Ihrem Unternehmen viel Erfolg auf dem Weg zu mehr Informationssicherheit.

Nationalrat Edi Engelberger

Präsident des Schweizerischen Gewerbeverbandes

Mai 2016: Dieser Originaltext wurde nicht angepasst. InfoSurance wurde aufgelöst und ist an den Verein ISSS (Information Security Society Switzerland) übergegangen.

Das erweiterte 10-Punkte-Programm im Überblick

Zehn Massnahmen für einen **wirkungsvollen Grundschutz**

- Punkt 1 Erstellen Sie ein Pflichtenheft für IT-Verantwortliche!
- Punkt 2 Sichern Sie Ihre Daten regelmässig mit Backups!
- Punkt 3 Halten Sie Ihr Antivirus-Programm aktuell!
- Punkt 4 Schützen Sie Ihren Internetzugang mit einer Firewall!
- Punkt 5 Aktualisieren Sie Ihre Software regelmässig!
- Punkt 6 Verwenden Sie starke Passwörter!
- Punkt 7 Schützen Sie Ihre mobilen Geräte!
- Punkt 8 Machen Sie Ihre IT-Benutzerrichtlinien bekannt!
- Punkt 9 Schützen Sie die Umgebung Ihrer IT-Infrastruktur!
- Punkt 10 Ordnen Sie Ihre Dokumente und Datenträger!

Fünf weitere Massnahmen für **mehr Vertraulichkeit**

- Punkt 11 Erfüllen Sie die Vorgaben!
- Punkt 12 Regeln Sie den Zugriffsschutz auf Daten!
- Punkt 13 Verschlüsseln Sie mobile Datenträger und Übermittlung!
- Punkt 14 Behandeln Sie auch nicht elektronischen Daten vertraulich!
- Punkt 15 Sensibilisieren Sie Ihre Mitarbeitenden!

Fünf weitere Massnahmen für **mehr Verfügbarkeit**

- Punkt 16 Überprüfen Sie Ihre Systeme!
- Punkt 17 Sorgen Sie für eine unterbrechungsfreie Stromversorgung!
- Punkt 18 Halten Sie wichtige Elemente redundant!
- Punkt 19 Planen Sie die Notfallvorsorge!
- Punkt 20 Verteilen Sie das Know-how!

1

Erstellen Sie ein Pflichtenheft für IT-Verantwortliche!

Grundsätze **IT-Sicherheit beruht zu je einem Drittel auf technischen, organisatorischen und menschlichen Faktoren!**

Neben technischen Sicherheitslösungen und motivierten Mitarbeitenden muss auch die Geschäftsleitung ihren Beitrag zu einem wirkungsvollen Grundschutz leisten.

- Erläuterungen
- Jedes Unternehmen braucht einen EDV- bzw. IT-Verantwortlichen mit Stellvertreter. Das nötige Wissen dazu kann in entsprechenden Kursen erworben werden. Oft arbeiten kleine Unternehmen auch mit externen Spezialisten zusammen. Die Kosten hierfür sind wesentlich tiefer als die Folgen eines Datenverlustes oder eines Verstosses gegen das Datenschutzgesetz.
 - Die Geschäftsleitung delegiert Sicherheitsaufgaben an den IT-Verantwortlichen schriftlich und hält diese in einem Pflichtenheft fest (siehe unten).
 - Die Geschäftsleitung kontrolliert, ob der IT-Verantwortliche seine Aufgaben korrekt wahrnimmt.
 - Alle Mitarbeitenden, die an einem Computer arbeiten, erhalten Benutzerrichtlinien. Diese beschreiben, welche Aktionen auf dem Computer erlaubt und welche untersagt sind (siehe Punkt 8).
 - Bestimmen Sie den Ansprechpartner für alle Sicherheitsfragen, z.B. bei einem Verlust von Notebooks oder bei einem Virenbefall usw.

Tipps & Tricks **Richtlinien für IT-Verantwortliche**

- Sichern Sie die Daten auf Servern, Arbeitsstationen, Notebooks, Laptops und anderen mobilen Geräten regelmässig (siehe Punkt 2).
- Halten Sie Betriebssysteme, Antivirus-Programme, Firewalls und sonstige Software aktuell (siehe Punkte 3, 4 und 5).
- Ändern Sie werkseitige Passworteinstellungen bei Geräten, Betriebssystemen und Anwendungsprogrammen sofort.
- Führen Sie eine Liste mit allen im Unternehmen vorhandenen Computern, mit den installierten Programmen sowie den ausgeführten Software-Aktualisierungen (siehe Punkt 5).
- Legen Sie die Zugriffsrechte fest: Welche Programme dürfen Mitarbeitende ausführen? Auf welche Daten haben Mitarbeitende Zugriff?
- Führen Sie eine Liste mit allen Personen, welche von aussen auf das Firmennetzwerk zugreifen, eventuell mit genauer Dauer der Berechtigung. Stellen Sie sicher, dass auch deren Schutzprogramme aktuell sind.
- Stellen Sie sicher, dass Datenschutz-Bestimmungen eingehalten werden, z.B. durch aktuelle Schutzprogramme und starke Passwörter (siehe Punkte 3, 4, 6).
- Kontrollieren Sie regelmässig, ob die Benutzerrichtlinien eingehalten werden.

2

Sichern Sie Ihre Daten regelmässig mit Backups!

Grundsätze Datenverluste entstehen auf verschiedene Arten: Daten werden versehentlich überschrieben, Informationen auf einer Harddisk werden durch einen Defekt unleserlich oder ein Brand beziehungsweise ein Wasserschaden zerstört Ihre Daten. Solche Verluste können Sie mit regelmässigen Datensicherungen (Backups) vermeiden.

- Erläuterungen**
- Grundsätzlich sind alle Daten mit geschäftsrelevantem Inhalt zu sichern. Softwarekonfigurationen sollten ebenfalls gesichert werden.
 - Die Häufigkeit der Datensicherung richtet sich nach Tätigkeit und Grösse Ihres Unternehmens. Mindestens einmal pro Woche sollte jedes KMU seine Daten sichern.
 - Ein Betrieb mit einem täglichen Backup sorgt für die gesetzeskonforme Archivierung Ihrer Daten gemäss Obligationenrecht und der „Verordnung über die Führung und Aufbewahrung der Geschäftsbücher“ (GebÜV) (*siehe unten*).
 - Regeln Sie schriftlich, wer für Datensicherungen zuständig ist und führen Sie eine Kontrollliste über die erfolgreiche Sicherung der Daten.
 - Sichern Sie die Daten immer auf mobilen Medien (Bandlaufwerk, auswechselbarer Datenträger).
 - Es lohnt sich, von wichtigen Daten, die nur in Papierform vorliegen (z.B. von Verträgen, Urkunden), Kopien anzufertigen und diese ebenfalls ausser Haus aufzubewahren.
 - Beachten Sie, dass die Bilanz, die Erfolgsrechnung, die Geschäftsbücher, die Inventare, die Buchungsbelege und die Geschäftskorrespondenz während 10 Jahren aufbewahrt werden müssen.

Tipps & Tricks **Richtlinien zum Thema Backup**

- Erstellen Sie von Montag bis Donnerstag je ein Tages-Backup auf einem eigenen Speichermedium. Die Tages-Backups werden jeweils am entsprechenden Wochentag in der folgenden Woche überschrieben. Bewahren Sie die Tageskopien ausserhalb des Serverraums auf.
- Erstellen Sie jeden Freitag ein Wochen-Backup auf einem separaten Speichermedium und bewahren Sie dieses ausserhalb des Betriebs auf. Das Wochen-Backup wird nach einem Monat wieder überschrieben.
- Erstellen Sie am Monatsende das Monats-Backup. Das Monats-Backup wird nicht mehr überschrieben und ausserhalb des Betriebs aufbewahrt.
- Erstellen Sie Ende Jahr das Jahres-Backup. Das Jahres-Backup wird nicht mehr überschrieben und ebenfalls ausserhalb des Betriebs aufbewahrt.
- Überprüfen Sie periodisch, ob sich die Daten von den Sicherungsmedien zurückspielen lassen. Jede Sicherung ist nutzlos, wenn die Daten nicht korrekt auf das Backup-Medium übertragen wurden.

3

Halten Sie Ihr Antivirus-Programm aktuell!

Grundsätze **Schädliche Programme, wie zum Beispiel Viren und Würmer, können Ihre IT-Infrastruktur lahm legen und damit die wirtschaftliche Existenz Ihres Unternehmens gefährden.**

- Erläuterungen**
- Computerviren können Daten und Programme verändern, manipulieren oder sogar vollständig zerstören. Bösertige Computerprogramme werden via E-Mail-Anhänge (Attachments) und Instant Messengers usw. übertragen. Im Internet sind Viren oft als nützliche oder unterhaltende Gratisprogramme getarnt und werden durch einen einfachen Mausklick aktiviert.
 - Unzureichend geschützte Computersysteme werden häufig zur Verbreitung von Viren und für gezielte Attacken gegen ein drittes Unternehmen missbraucht. Wer als Geschäftsleiterin oder Geschäftsleiter ungenügende Vorkehrungen zum Schutz seiner Computersysteme trifft, handelt fahrlässig und muss allenfalls mit Strafverfolgung rechnen.
 - Schutz vor bekannten Viren und Würmern bietet ein Antivirus-Programm. Es identifiziert Eindringlinge und macht sie unschädlich. Solche Programme können in Computerläden gekauft oder kostenlos aus dem Internet herunter geladen werden.
 - Da Hacker laufend neue Viren programmieren, muss das Antivirus- Programm immer wieder aktualisiert werden. Je nach verwendetem Produkt sucht das Programm auf der Homepage des Herstellers selbständig solche Aktualisierungen. Informieren Sie sich bei Ihrem Händler, ob dies bei Ihrem Programm der Fall ist. Die Aktualisierung sollte auf jeden Fall täglich durchgeführt werden.

Tipps & Tricks **Richtlinien zum Thema Virenschutz**

- Installieren Sie ein Antivirus-Programm auf sämtlichen Servern, Arbeitsstationen (Clients) sowie Ihren Notebooks und aktualisieren Sie den Schutz regelmässig, also mindestens täglich.
- Untersagen Sie ausdrücklich das Ausschalten oder zeitweise Deaktivieren des Antivirus- Programms.
- Fordern Sie die Mitarbeitenden auf, Warnmeldungen über Viren unverzüglich dem IT-Verantwortlichen zu melden.
- Führen Sie mindestens ein Mal wöchentlich einen vollständigen «Virus-Scan» von Festplatten durch. Damit werden bisher unerkannte Viren entdeckt und eliminiert.
- Untersagen Sie eigene Tests mit Viren ausdrücklich.
- Aktualisieren Sie bei grösseren Netzwerken Antivirus-Programme zentral und automatisch.

4

Schützen Sie Ihren Internetzugang mit einer Firewall!

Grundsätze **Gibt es in Ihrem Betrieb Brandschutztüren? Ja? Dann achten Sie bestimmt darauf, dass diese Türen auch stets geschlossen werden.**

In der Welt des Internets und des elektronischen Datenaustauschs erfüllt die Firewall diese Sicherheitsaufgabe.

- Erläuterungen**
- Ohne eine Firewall können Unbefugte auf Ihren Computersystemen Schaden anrichten. Sie können darauf unbemerkt Befehle ausführen oder Ihre Rechner zu illegalen Attacken auf Dritte missbrauchen. Zudem gelangen sie an Geschäftsdaten, die eventuell dem Datenschutzgesetz unterstehen.
 - Für grössere Firmennetzwerke ist eine eigenständige Firewall (spezielles Gerät), für einzelne PCs und mobile Geräte (Notebooks) eine integrierte Firewall (auf dem System selbst) zu empfehlen.
 - Im Handel sind Produkte erhältlich, die gleichzeitig eine Firewall und einen Virenschutz bieten. Gerade für kleinere Betriebe sind kombinierte Produkte sehr zu empfehlen.
 - Manche Betriebssysteme haben eine eigene Firewall eingebaut. Nutzen Sie auf jeden Fall auch diese Möglichkeit und aktivieren Sie diese Firewalls.
 - Wenn Sie in Ihrem Betrieb Wireless-LAN für Ihre Computer einsetzen, sorgen Sie dafür, dass diese richtig und sicher funktionieren. Falsch genutzte Wireless-LAN-Geräte machen den gesamten Firewall-Schutz zunichte.
 - Sämtliche Netzwerkübergänge müssen mit einer Firewall gesichert werden. Alle Verbindungen zwischen Lieferanten, Kunden, Outsourcern und Mitarbeitenden (auch mit Remote Access) und Ihrem Netzwerk müssen durch eine Firewall kontrolliert werden.

Tipps & Tricks **Richtlinien zum Thema Firewall**

- Installieren Sie eine Firewall und aktualisieren Sie diese regelmässig.
- Wickeln Sie den gesamten Internetverkehr über die Firewall ab. Erlauben Sie keine anderen Zugänge zum Internet (z.B. via Modem).
- Setzen Sie keine privaten Laptops und Wireless-LAN-Geräte im Unternehmen ohne schriftliche Einwilligung des IT-Verantwortlichen ein.
- Schützen Sie die Konfiguration Ihrer Firewall mit einem starken Passwort.
- Sichern Sie die Konfiguration der zentralen Firewall regelmässig.

5

Aktualisieren Sie Ihre Software regelmässig!

Grundsätze Kontrollieren Sie bei Ihrem Auto regelmässig Ölstand und Reifendruck? Hoffentlich. So wie Sie Ihr Auto regelmässig warten, müssen auch Computerprogramme in einem Unternehmen gepflegt und auf den neuesten Stand gebracht werden.

- Erläuterungen**
- Heutige Software beinhaltet oft Millionen von Zeilen Code. Dabei schleichen sich trotz Kontrollen Fehler ein. Für den Hersteller ist es nahezu unmöglich, Anwendungen in jeder denkbaren Umgebung und möglichen Konfiguration zu testen. Die Hersteller bieten regelmässig sogenannte "Patches" also "Software-Flicken" an. Sie beheben die bekannten Fehler.
 - Wenn Sie Ihre Software nicht oder nur selten aktualisieren, können Angreifer bekannte Fehler ausnützen, um Daten zu manipulieren oder um Ihre Infrastruktur für böswärtige Zwecke zu missbrauchen.
 - Häufig sind Betriebssysteme und Anwendungen in der Lage, sich selbst über das Internet zu aktualisieren. Die Webseiten der Software-Hersteller und das Handbuch helfen hier weiter.
 - Minimieren Sie Ihre «Angriffsfläche», indem Sie nur Software installieren, die Sie tatsächlich benötigen, und unnötige Dienste, Netzwerkfreigaben und Protokolle deaktivieren. Was nicht vorhanden ist, kann nicht missbraucht werden und muss nicht gepflegt werden!
 - Wenn Sie selber Schwachstellen entdecken oder sich die Software unerwartet verhält, informieren Sie Ihren Software-Hersteller.

Tipps & Tricks **Richtlinien zum Thema Patches**

- Installieren Sie die neuesten «Patches» für Betriebssysteme und Anwendungsprogramme.
- Installieren Sie verfügbare «Sicherheits-Updates» so schnell wie möglich.
- Installieren Sie nur Aktualisierungen, für die Versionen einer Software, die Sie verwenden.
- Installieren Sie «Patches» auf sämtlichen Computern, d.h. auch auf Notebooks und Geräten von externen Mitarbeitenden!
- Führen Sie eine Liste darüber, welche «Updates» wo installiert sind.

Hier finden Sie die neuesten «Updates» für die Microsoft Produkte:
www.windowsupdate.com

6

Verwenden Sie starke Passwörter!

Grundsätze Wer den Benutzernamen und das Passwort eines Anwenders kennt, kann sich an einem System anmelden und übernimmt damit die (Computer-) Identität des entsprechenden Anwenders mit allen Zugriffsberechtigungen!

Durch Passwortdiebstahl können somit Unbefugte ohne grossen Aufwand an vertrauliche Geschäftsformationen gelangen. Verhindern Sie also, dass in Ihrem Betrieb der Identitätsdiebstahl möglich ist.

- Erläuterungen**
- Werkseitige Passworteinstellungen bei Geräten, Betriebssystemen und Anwendungsprogrammen müssen vom IT-Verantwortlichen sofort geändert werden (*siehe Punkt 1*).
 - Halten Sie Ihre Mitarbeitenden dazu an, nur starke Passwörter einzusetzen, die regelmässig geändert werden. Machen Sie allen bewusst, dass sie für Handlungen verantwortlich sind, die unter ihrem Benutzernamen ausgeführt werden.
 - Starke Passwörter sind mindestens 8 Zeichen lang, enthalten Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen
 - So können Sie starke Passwörter konstruieren:
Beispiel 1: Aus dem einfachen Wort «Sommer» leiten Sie das starke Passwort «So\$Mmer04» ab, indem Sie an der 3. Stelle «\$» einfügen, gross weiterfahren und am Ende noch die Ziffern «04» für den Monat April ergänzen.
Beispiel 2: Aus dem Satz «Letzten Sommer waren wir zu viert in Paris!» leiten Sie das starke Passwort «LSwwz4iP!» ab, indem Sie Anfangsbuchstaben und Ziffern aneinander reihen. Einen vernünftigen Satz kann man sich besser merken als ein kryptisches Passwort!

Tipps & Tricks **Richtlinien zum Thema Passwörter**

- Verwenden Sie *keine Passwörter*, die in Wörterbüchern zu finden sind.
- Verwenden Sie *keine Passwörter*, die Namen, AHV- und Passnummern und Geburtsdaten aus dem Familienumfeld enthalten.
- Prüfen Sie die Qualität eines Passwortes mit einem Passwort-Checker.
- Wechseln Sie das Passwort mindestens alle zwei Monate. Idealerweise wird dies vom System erzwungen.
- Schreiben Sie Passwörter *niemals* auf, ohne die Notiz sicher z.B. im Tresor zu verwahren. Viele Passwörter findet man aufgeschrieben im Umkreis von einem Meter beim Computer.
- Geben Sie Ihr Passwort *niemals* an Dritte weiter. Stellvertretungen funktionieren auch ohne Kenntnis des Passwortes. Falls Sie feststellen, dass Dritte Ihr Passwort kennen, ändern Sie es umgehend.

Hier können Sie die Qualität Ihres Passwortes überprüfen lassen:
<https://passwortcheck.datenschutz.ch/>

7

Schützen Sie Ihre mobilen Geräte!

Grundsätze **Mobiltelefone, Handheld-Computer und Notebooks mit Wireless-LAN sind ausgesprochen praktisch und vielseitig.**

Falsch eingesetzt, stellen diese Geräte aber ein Sicherheitsrisiko dar. Wer aus geschäftlichen Gründen gezwungen ist, sensible Daten auf mobilen Geräten zu speichern, muss spezielle Vorkehrungen treffen.

- Erläuterungen
- *Sämtliche* mobilen Geräte müssen mit einem starken Passwort geschützt werden (*siehe Punkt 6*). Beim Verlust des Geräts oder im Fall eines Diebstahls haben Unbefugte sonst ein leichtes Spiel, an Ihre Geschäftsdaten zu gelangen.
 - Auf mobilen Geräten sollten nur diejenigen Daten enthalten sein, die tatsächlich benötigt werden. Sichern Sie diese regelmässig (*siehe Punkt 2*).
 - Heikle Geschäftsdaten auf Notebooks müssen verschlüsselt gespeichert werden, damit sie bei Verlust oder Diebstahl nicht in die Hände Unbefugter geraten. Gute Verschlüsselungsprogramme sind im Handel erhältlich und können auch aus dem Internet herunter geladen werden (*siehe unten*).
 - Auch mobile Geräte müssen regelmässig auf Viren geprüft werden weil sie z.B. via E-Mail-Funktionen mit Ihren übrigen Computern synchronisiert werden.
 - Durch falsch konfigurierte Wireless-LAN-Geräte können Hacker innerhalb weniger Minuten aus Distanzen von über einem Kilometer in Ihr Firmennetzwerk eindringen! Die Nutzung von externen und öffentlichen Access Points (HotSpots) muss speziell geregelt werden.
 - Aktivieren Sie Bluetooth bei Ihren Geräten (Handy, Notebooks, Handheld-Computer) nur bei Bedarf und nicht erkennbar. Ihr Gerät reagiert sonst ohne Ihr Wissen auf Anfragen fremder Geräte (im Umkreis von bis zu 100 Metern).

Tipps & Tricks **Richtlinien zum Thema Wireless-LAN**

- Ändern Sie den vom Hersteller vorgegebenen Namen für Ihr Wireless LAN (Service Set ID – SSID). Die neue Identifikation darf *keinesfalls* Ihren Firmennamen enthalten.
- Deaktivieren Sie die SSID-Ausstrahlung, damit Ihr AccessPoint für Dritte nicht sichtbar ist.
- Aktivieren Sie die Verschlüsselung der kabellosen Datenübermittlung (WPA2, Wi-Fi Protected Access 2). Ändern Sie das Standard-Passwort Ihres Access Points.
- Setzen Sie den MAC-Adressen-Filter ein, damit nur bekannte Geräte mit dem AccessPoint kommunizieren können.
- Übermitteln Sie hoch vertrauliche Daten nur über Verbindungen, welche zusätzlich mit einem Virtual Privat Network (VPN) geschützt sind.
- Zur Verschlüsselung können Sie das Produkt Pretty Good Privacy (PGP) verwenden. Sie finden PGP für kommerzielle Verwendungszwecke auf der offiziellen Website <http://www.pgp.com/de/index.html>.
- Für die Verwendung des freien OpenPGP-Standards besuchen Sie <http://www.gnupg.org/index.de.html>

8

Machen Sie Ihre IT-Benutzerrichtlinien bekannt!

Grundsätze Ohne verbindliche und verständliche IT-Benutzerrichtlinien können Ihre Mitarbeitenden nicht wissen, welche Handlungen erlaubt und welche verboten sind. Regeln werden nur ernst genommen, wenn sich auch Vorgesetzte daran halten. Handeln Sie in allen Sicherheitsaspekten als Vorbild.

- Erläuterungen**
- Definieren Sie schriftliche IT-Benutzerrichtlinien und lassen Sie diese von den Mitarbeitenden unterzeichnen.
 - Machen Sie Sicherheit in Ihrem Unternehmen immer wieder und auf unterschiedliche Weise zum Thema.
 - Führen Sie ein bis zwei Mal pro Jahr Sensibilisierungsaktionen durch. Diese lassen sich auch mit einfachen Mitteln realisieren: z.B. durch E-Mails an alle Mitarbeitenden, Rundschreiben in der internen Post, Plakate in der Kantine, Beiträge in der Firmenzeitung usw.
 - Organisieren Sie eine Basisausbildung für alle Mitarbeitenden (z.B. auf der Basis dieser Broschüre).
Die wichtigsten Lernziele sind:
 - der Nutzen der IT-Sicherheit
 - Bestimmen starker Passwörter
 - Sicherer Umgang mit Internet und E-Mail
 - Sicherer Umgang mit dem Virenschutz
 - Ablagestruktur von Dokumenten
 - Papier allein genügt nicht! Mitarbeitende müssen zum Thema Sicherheit regelmässig sensibilisiert werden.

Tipps & Tricks **Richtlinien für die IT-Benutzerinnen und -Benutzer**

- Regeln Sie die Installation und den Einsatz von eigenen Programmen und Hardware (Spiele, Bildschirmschoner, USB-MemorySticks, Modems, private Notebooks, Wireless-LAN, Handheld-Computer etc.).
- Regeln Sie den Gebrauch des Internets: Was dürfen die Mitarbeitenden herunterladen, was nicht (Informationen, Programme, etc)?
- Untersagen Sie den Besuch von Chatrooms, aber auch von Webseiten mit pornografischen, rassistischen und gewaltverherrlichenden Inhalten.
- Legen Sie die Art und Weise der Datensicherung fest, v.a. bei den Notebookbenutzerinnen und -benutzern (*siehe Punkt 2*).
- Legen Sie den Umgang mit Passwörtern fest (*siehe Punkt 6*).
- Regeln Sie den Umgang mit Sicherheits-Updates und Antivirus-Programmen (*siehe Punkt 3 und 5*).
- Regeln Sie den Gebrauch von E-Mail: keine vertraulichen Daten, kein Weiterleiten an die private E-Mail-Adresse, keine Kettenbriefe etc.
- Legen Sie den Umgang mit vertraulichen Informationen und Daten fest und richten Sie eine geschützte Dateiablage ein.
- Regeln Sie das Verhalten bei sicherheitsrelevanten Vorkommnissen, z.B. Viruswarnungen, Diebstählen und Verlusten von Notebooks und Passwörtern.
- Kündigen Sie Sanktionen bei einem Verstoss gegen die Benutzerrichtlinien an.

9

Schützen Sie die Umgebung Ihrer IT-Infrastruktur!

Grundsätze **Wissen Sie, wer in Ihrem Unternehmen tagsüber ein- und ausgeht? Einige wenige Vorkehrungen verhindern bereits, dass Unbefugte an wichtige Geschäftsinformationen gelangen.**

Gelebte, sichtbare Sicherheit ist heute ein Qualitätskriterium und schafft Vertrauen bei Kunden und Lieferanten. Was nützt die beste Firewall, wenn sich Fremde in die Büroräume einschleichen können?

- Erläuterungen**
- Alle Zugänge zum Gebäude resp. Firmenareal sind abzuschliessen oder zu überwachen. Falls dies nicht möglich ist, muss zumindest der Büroteil geschützt werden.
 - Lassen Sie Besucher, Kunden und Bekannte nicht unbeaufsichtigt in Ihrem Betrieb umhergehen.
 - Alle Drittpersonen werden am Empfang abgeholt, während ihres Aufenthaltes dauernd begleitet und beim Verlassen des Gebäudes am Ausgang wieder verabschiedet.
 - Wenn Sie nicht über einen Empfang verfügen, der den Eingangsbereich überblickt, sollten Sie die Eingangstüre schliessen und ein Schild «Bitte läuten!» anbringen.
 - Stellen Sie sicher, dass sämtliche Einstiegsmöglichkeiten (Fenster, Türen, usw.) über einen ausreichenden Einbruchschutz verfügen. Entsprechende Informationsblätter sind auf jedem Polizeiposten erhältlich.
 - Schlüssel und Badges müssen korrekt verwaltet und die entsprechenden Listen aktualisiert werden. Schlüssel mit Passpartout-Funktion sind restriktiv zu verteilen. Die entsprechenden Berechtigungen müssen mindestens jährlich auf ihre Notwendigkeit geprüft werden.
 - Mitarbeitende, welche aus dem Unternehmen austreten, geben ihre Schlüssel, Badges und andere Zugangsberechtigungen beim Austritt ab.

Tipps & Tricks **Richtlinien zum Thema IT-Umgebung**

- Stellen Sie Server in abschliessbare, klimatisierte Räume. Ist kein entsprechender Raum verfügbar, schliessen Sie die Server in einen Computerschrank (Rack).
- Lagern Sie brennbare Materialien wie Papier etc. nicht im oder unmittelbar vor dem Serverraum.
- Platzieren Sie im Serverraum einen gut sichtbaren CO₂-Feuerlöscher.
- Stellen Sie Netzwerkdrucker nicht in öffentlich zugängliche Räume, da Unbefugte Einblick in Dokumente erhalten können.
- Schliessen Sie Netzkabel, die durch öffentliche Räume führen, sowie Modems, Hubs, Router und Switches ein.

10

Ordnen Sie Ihre Dokumente und Datenträger!

Grundsätze **Hat Ordnung etwas mit Sicherheit zu tun? Mehr als man auf den ersten Blick vielleicht meinen möchte.**

Daten und Dokumente gehen auf einem ordentlichen Arbeitsplatz weniger verloren, als wenn die Arbeitsfläche mit Papieren, Handzetteln und Mäppchen übersät ist.

- Erläuterungen**
- Eine klare Ordnungspolitik minimiert die Gefahr, dass sensible Dokumente im ungünstigsten Augenblick auftauchen oder von Unbefugten durch Zufall gelesen werden.
 - Ordnung ist auch eine Frage des Images: Kunden oder Lieferanten schliessen bei einem Unternehmen vom ordentlichen Äussern gerne auf die innere Haltung.
 - Ordnen Sie elektronische Daten und Papierdokumente in einem einheitlichen Ablagesystem, z.B. nach Kunde oder nach Projekt. Das System muss logisch aufgebaut und für die Mitarbeitenden gut verständlich sein.
 - Werden Speichermedien ausser Haus gegeben, sollten dafür neue und noch nie verwendete Datenträger einsetzen. Konventionell gelöschte Informationen können relativ leicht wieder hergestellt und von Unbefugten gelesen werden. Eine zuverlässige Löschung der Daten kann nur mit einem „Wipe“-Programm erreicht werden. Informationen dazu sind im Internet erhältlich.
 - Wenn Sie mit sensiblen Daten am Computer arbeiten, positionieren Sie den Bildschirm so, dass Kollegen und Besucher die Informationen nicht mitlesen können.

Tipps & Tricks **Richtlinien zum Thema Dokumente und Datenträger**

- Löschen Sie nicht mehr benötigte elektronische Daten auf Speichermedien wie CD's, DVD's, MemorySticks und Festplatten durch Überschreiben des gesamten Speicherbereichs. Der einfache Lösch-Befehl reicht nicht! Am besten werden Speichermedien vor der Entsorgung physisch zerstört.
- Halten Sie vertrauliche Unterlagen, sowie Dokumente mit Personendaten konsequent unter Verschluss.
- Vernichten Sie nicht mehr benötigte Papierdokumente und Notizen mit sensiblen Daten sicher (Aktenvernichter).
- Sperren Sie während Pausen und bei Abwesenheit vom Arbeitsplatz den Computer mit einem Passwort und schliessen Sie vertrauliche Dokumente ein.
- Lassen Sie ausgedruckte Dokumente nicht auf dem Drucker liegen. Dies gilt insbesondere für öffentlich zugängliche Bereiche (Empfang, usw.).

Brauchen Sie mehr Vertraulichkeit und mehr Verfügbarkeit?

Sie sind nicht sicher, ob Ihr Unternehmen erhöhte Sicherheitsanforderungen aufweist und weitergehende Sicherheitsmassnahmen benötigt?

Die folgenden Punkte helfen Ihnen, die Notwendigkeit weitergehender Sicherheitsmassnahmen abzuschätzen. Die Massnahmen finden Sie auf den folgenden Seiten.

Schützen Sie Ihr Unternehmen mit weitergehenden Massnahmen zur **Vertraulichkeit**, wenn

- gesetzliche Auflagen, Vorschriften oder Verträge die Vertraulichkeit explizit fordern (z.B. Datenschutzgesetz, Urheberrechtsgesetz);
- ein Missbrauch vertraulicher Daten zu hohen finanziellen Verlusten und zu breiter Ansehens- oder Vertrauensbeeinträchtigung führen würde wie z.B. Veröffentlichung von Geschäftsgeheimnissen oder Offerten;
- ein Missbrauch personenbezogener Daten erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen wie z.B. Veröffentlichung vertraulicher Kundendaten hätte.
- Ihr Unternehmen generell auf den Schutz der Vertraulichkeit angewiesen ist. Das trifft beispielsweise auf Personalberatungsunternehmen, Verbände, Spitäler, Treuhänder, Arzt- und Anwaltspraxen zu.

→ **Beachten Sie auf den folgenden Seiten vor allem die Punkte 11 bis 15.**

Schützen Sie Ihr Unternehmen mit weitergehenden Massnahmen zur **Verfügbarkeit**, wenn

- Ihr Unternehmen bei einem Ausfall Ihrer IT so stark beeinträchtigt wird, dass hoher Gesamtschaden entstehen kann (z.B. verspätete Lieferung aufgrund verzögerter Bearbeitung von Bestellungen);
- ein Ausfall der IT-Anwendung zu breiter Ansehens- oder Vertrauensbeeinträchtigung führt (z.B. Ausfall eines Buchungssystems einer Reisegesellschaft; Ausfall des Webservers für Kunden);
- der Ausfall der IT-Anwendung oder des IT-Systems unmittelbar die persönliche Unversehrtheit von Personen bedroht (z.B. Ausfall von Schliesssystem).
- Ihr Unternehmen generell auf den Schutz der Verfügbarkeit angewiesen ist. Das trifft beispielsweise auf Produktionsbetriebe, Handelsunternehmen, Druckereien oder Online-Shops zu.

→ **Beachten Sie auf den folgenden Seiten vor allem die Punkte 16 bis 20.**

11

Erfüllen Sie die Vorgaben!

Grundsätze Ein Unternehmen muss verschiedene Vorgaben bezüglich Vertraulichkeit einhalten. Neben rechtlichen Vorgaben können dies Verträge oder Vorschriften sein. Ein Nichteinhalten dieser Vorgaben kann zu rechtlichen Konsequenzen und einem Imageverlust für das Unternehmen führen.

- Erläuterungen**
- Besonders zu beachten sind das Datenschutzgesetz (DSG), das Urheberrechtsgesetz (URG) und das Obligationenrecht (OR).
 - Wo Daten von Personen, etwa Kunden- oder Mitarbeiterdaten auf irgendeine Art und Weise bearbeitet werden, gilt das Bundesgesetz über den Datenschutz. Gemäss Datenschutzgesetz müssen diese Daten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Auch die inhaltliche Richtigkeit der Daten muss sichergestellt sein.
 - Zu beachten sind auch Verträge mit Kunden und Partnern. Diese können besondere Vereinbarungen zum Thema Vertraulichkeit beinhalten.
- Tipps & Tricks**
- Machen Sie sich mit den Gesetzen und den Verordnungen vertraut. Treffen Sie entsprechende Vorkehrungen, um die Gesetze einzuhalten.
 - Achten Sie darauf, dass Daten rechtlich einwandfrei erhoben wurden und dass die gespeicherten Daten richtig sind.
 - Ermöglichen Sie den betroffenen Personen Auskunft über ihre gespeicherten Daten einzuholen.
 - Weitere Informationen finden Sie auf der Website des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (<http://www.edoeb.admin.ch/>) und auf der Website des Datenschutzbeauftragten des Kantons Zürich (<http://www.datenschutz.ch>).

12

Regeln Sie den Zugriffsschutz auf Daten!

Grundsätze **Auf Daten muss zugegriffen werden können. Doch nicht jeder soll Zugriff haben. Durch unbefugten Zugriff können Informationen missbraucht werden. Der Zugriff muss entsprechend geschützt werden, damit nur berechtigte Personen Zugang haben.**

- Erläuterungen**
- Wer unbefugten Zugriff zu Informationen hat, kann diese einsehen, kopieren, verändern oder löschen. Das kann gravierende Folgen haben. Stellen Sie sich vor, Ihre Offerte gerät in die falschen Hände, Ihre Kundendatenbank wird gelöscht oder Ihre Forschungsergebnisse gelangen in den Besitz Ihrer Konkurrenz.
 - Legen Sie fest, wer Zugriff auf bestimmte IT-Anwendungen oder Informationen hat. Dabei sollten die Zugriffsrechte rollenbasiert vergeben werden, z.B. Sekretariat, Verkauf, Buchhaltung, Personalwesen, Systemadministrator.
 - Es sind nur so viele Zugriffsrechte zu vergeben, die zur Durchführung einer Aufgabe benötigt werden («Need-to-know-Prinzip»).
 - Vergeben werden die Zugriffsrechte durch die Rechteverwaltung des IT-Systems oder durch eine übergeordnete Benutzeradministration..
- Tipps & Tricks**
- Führen Sie ein Klassifizierungssystem für Ihre Informationen ein.
 - Die Zugriffsrechte werden von der jeweils verantwortlichen Person festgelegt.
 - Die Rechteverwaltung muss dokumentiert werden. Festgehalten wird, welche Person welche Funktion wahrnimmt und welche Person Zugriff auf welche Applikationen und Daten hat. Überprüfen Sie diese Rechte regelmässig und passen Sie sie entsprechend an.
 - Benützen Sie eine starke Authentifizierung: Neben dem Benutzernamen und Passwort können Sie ein drittes Sicherheits-Element verwenden, z.B. eine Smart-Card.
 - Beim Austritt von Mitarbeitenden aus dem Unternehmen oder bei internem Wechsel sind deren Benutzerkonten und die Zugriffsrechte sofort zu sperren bzw. anzupassen.
 - Besonders zu beachten sind die Systembetreuer und die Administratoren. Sie verfügen in der Regel über sehr weitgehende Rechte.

13

Verschlüsseln Sie mobile Datenträger und Übermittlung!

Grundsätze Vertrauliche Daten können bei ungeschützter Übertragung (z.B. E-Mail) von Dritten eingesehen werden. Mobile Geräte können verloren gehen und Ihre Daten geraten in falsche Hände. Um die Vertraulichkeit zu gewährleisten, ist eine Verschlüsselung der Daten auf den Geräten sowie der Übermittlung notwendig.

- Erläuterungen**
- E-Mails können von Dritten gelesen werden. E-Mails mit vertraulichem Inhalt sollten Sie deshalb verschlüsseln.
 -
 - Wenn Sie vertrauliche Daten speichern – insbesondere auf mobilen Geräten wie Notebooks, Smartphones oder digitalen Agenden – dann muss eine Verschlüsselung verwendet werden. Nur durch das entsprechende Passwort oder die Schlüssel kann die Information wieder entschlüsselt werden.
- Tipps & Tricks**
- Regeln Sie die Verschlüsselung. Legen Sie fest, welche Daten und welche Geräte in Ihrem Unternehmen zu verschlüsseln sind. Schulen Sie Ihre Mitarbeitenden im Umgang mit der Verschlüsselung. Regeln Sie auch die Entschlüsselung, damit etwa später immer noch auf archivierte Daten zugegriffen werden kann. Beachten Sie den Austritt von Mitarbeitenden, die Daten verschlüsselt haben.
 - Installieren Sie auf allen Geräten mit sensiblen Daten eine Verschlüsselungssoftware. Die Verschlüsselung muss mit einem sicheren Passwort geschützt werden (Siehe Punkt 6 des 10-Punkte-Programms).
 - Benutzen Sie eine Verschlüsselungssoftware für die E-Mail-Kommunikation mit sensiblen Daten.
 - Als einfache Lösung können Sie sensible Daten mit einem zip-Programm komprimieren und gleichzeitig verschlüsseln. Achten Sie darauf, dass Sie das Passwort nicht über den gleichen Kommunikationsweg übermitteln (z.B. zip-Datei per E-Mail, Passwort per SMS)
 - Sie können aber auch das Produkt *Pretty Good Privacy (PGP)* verwenden. Es ist weit verbreitet und verfügt über technisch ausgereifte Funktionalitäten für die Verschlüsselung, digitale Signatur und das sichere Löschen von Daten. Sie finden PGP für kommerzielle Verwendungszwecke auf der offiziellen Website <http://www.pgp.com/de/index.html>.
 - Für die Verwendung des freien OpenPGP-Standards besuchen Sie <http://www.gnupg.org/index.de.html>.

14

Behandeln Sie auch nicht elektronische Daten vertraulich!

Grundsätze **Was für elektronische Daten gilt, trifft selbstverständlich auch auf Daten in Papierform oder das gesprochene Wort zu: Lassen Sie Vorsicht walten, schützen Sie vertrauliche Daten und plaudern Sie nichts aus.**

- Erläuterungen
- Jedes Dokument hat einen Eigner und eine Ablage, Dokumente müssen klassifiziert werden, Dokument-Rechte müssen vergeben werden und bei Nichtgebrauch müssen Informationen korrekt entsorgt werden.
 - Vertrauliche Papierdokumente müssen sicher aufbewahrt werden. Sicher heisst: unter Verschluss.
 - Vertrauliche Papierdokumente müssen mit einem Aktenvernichter zerstückelt werden.
 -
 - Auch Gesprochenes muss vertraulich behandelt werden, z. B. bei Gespräch in der Öffentlichkeit. Weisen Sie Ihre Mitarbeitenden auf die Gefahren beim Ausplaudern vertraulicher Informationen im öffentlichen Raum hin.
 - Machen Sie Ihre Mitarbeitenden auf die Aspekte des *Social Engineerings* (Manipulation von Personen, mit dem Ziel, an geschützte Informationen zu gelangen) und der *Spionage* aufmerksam. Der Umgang mit vertraulichen Daten darf nie leichtfertig und unüberlegt geschehen.
- Tipps & Tricks
- Klassifizieren Sie auch Ihre Papierdokumente.
 - Wo mit vertraulichen Daten gearbeitet wird, soll ein Aktenvernichter zur Verfügung stehen.
 - Schaffen Sie Möglichkeiten zur sicheren Aufbewahrung von Dokumenten, z.B. separat abschliessbare Aktenschränke.
 - Bewahren Sie vertrauliche Dokumente in einem abschliessbaren Schrank oder Tresor auf. Das gilt für Dokumente in Papierform wie auch für mobile Datenträger.

15

Sensibilisieren Sie Ihre Mitarbeitenden!

Grundsätze Nur sensibilisierte Mitarbeitende setzen Sicherheitsmassnahmen um. Erläutern Sie Ihren Mitarbeitenden die Notwendigkeit der Massnahmen und den korrekten Umgang mit vertraulichen Daten. Schliessen Sie gegebenenfalls eine Vertraulichkeitsvereinbarung ab.

- Erläuterungen**
- Eigene und externe Mitarbeiter bearbeiten oft vertrauliche Daten. Diesen Personen muss bewusst sein, dass sie entsprechende Massnahmen ergreifen müssen, um die Vertraulichkeit zu gewährleisten.
 - Fügen Sie eine Vertraulichkeitsklausel in den Arbeitsvertrag ein. Dies gilt auch für externe Mitarbeiter oder Partner. Diese Vertraulichkeitsvereinbarung definiert, wie mit vertraulichen Informationen umgegangen werden muss. Machen Sie auf die Konsequenzen bei Nichteinhalten der Vereinbarung aufmerksam.
 - Machen Sie die betroffenen Personen auf die rechtlichen Grundlagen (z.B. das Datenschutzgesetz) aufmerksam.
- Tipps & Tricks**
- Sensibilisieren Sie die neuen Mitarbeiter bereits bei deren Einstellung für die Belange der IT-Sicherheit.
 - Sensibilisierung ist ein stetiger Prozess. Führen Sie deshalb regelmässige Sicherheitskampagnen durch. Das können Schulungen, Umfragen, Merkblätter, Broschüren usw. sein.
 - Nutzen Sie dazu das Angebot von Dritten, z.B. des Vereins ISSS <http://www.iss.ch>

16

Überprüfen Sie Ihre Systeme!

Grundsätze **Das reibungslose Funktionieren der IT-Systeme muss jederzeit gewährleistet sein. Deshalb müssen IT-Systeme überprüft und regelmässig gewartet werden. Eine korrekte Wartung vermindert Störungen und verhindert Schäden an der Informationstechnologie.**

- Erläuterungen**
- Prüfen Sie regelmässig die Funktionstüchtigkeit Ihrer IT-Systeme: Funktioniert das Backup-System? Sind die Backup-Daten tatsächlich lesbar? Funktioniert die unterbrechungsfreie Stromversorgung (USV)? Enthalten die automatischen Systemprotokoll-Dateien Fehlermeldungen?
 - Beachten Sie auch organisatorische Aspekte: Werden gesetzliche und andere Richtlinien eingehalten? Ist die Notfallvorsorge überprüft worden?
 -
- Tipps & Tricks**
- Erstellen Sie ein Wartungsliste: Was muss wann durch wen geprüft und gewartet werden? Stellen Sie die Kontrolle und die Nachvollziehbarkeit der Wartung sicher.
 - Die Überwachung von Systemen kann bis zu einem gewissen Grad automatisiert werden. So kann z.B. eine Software automatisch eine Warnmeldung an den Administrator versenden, falls ein kritischer Wert überschritten wird.
 - Sie können Geräte und Systeme selber warten oder die Arbeit durch Partner (z.B. Hersteller) durchführen lassen. Achten sie bei externen Partnern auf vertrauenswürdige Personen und gewähren Sie nur beschränkte Zugangs- und Zugriffsrechte.
 - Überwachung und Wartungsarbeiten muss in regelmässigen Abständen durchgeführt werden.
 - Lassen Sie die externen Wartungstechniker eine Vertraulichkeitsvereinbarung unterzeichnen.
 - Der Zugriff auf Daten und Informationen durch Externe ist soweit wie möglich zu vermeiden.
 - Informieren Sie die betroffenen Personen über die anstehenden Wartungsarbeiten.

17

Sorgen Sie für eine unterbrechungsfreie Stromversorgung!

Grundsätze Wenn Sie auf eine hohe Verfügbarkeit Ihrer Daten und Systeme angewiesen sind, können Sie sich keinen Ausfall leisten. Eine unterbrechungsfreie Stromversorgung (USV) schützt Ihre Systeme vor einem Stromausfall und Spannungsspitzen (z.B. Blitzeinschlag) und verhindert Datenverluste.

- Erläuterungen**
- Die unterbrechungsfreie Stromversorgung (USV) wird zwischen der normalen Stromversorgung und den zu schützenden Geräten geschaltet.
 - Bei einem Stromausfall versorgt die Batterie der USV die Komponenten so lange mit Strom, dass sie geregelt abgeschaltet werden können.
 -
 - Zusätzlich kann eine USV als Filter wirken und Ihre Systeme vor Spannungsschwankungen schützen.
 - Neben dem Server müssen auch weitere wichtige Peripherie-Geräte an der USV angeschlossen werden. Dazu gehören beispielsweise wichtige Rechner im Netzwerk, Router, Backup-Systeme usw.
- Tipps & Tricks**
- Erstellen Sie eine Liste mit den Komponenten, die an die USV angeschlossen werden müssen. Aus dieser Zusammenstellung wird die benötigte Leistungsfähigkeit der USV bestimmt.
 - Kontrollieren Sie regelmässig die Leistungsfähigkeit der Batterien der USV und ersetzen Sie schwache Batterien sofort (siehe Punkt 16).

18

Halten Sie wichtige Elemente redundant!

Grundsätze Ein Ausfall eines kritischen Elements in Ihrem Netzwerk wie beispielsweise eines Servers kann viel Geld kosten und stört den Betrieb. Viele Unternehmen sind sich nicht bewusst, wie abhängig sie von kritischen System sind. Um nach einem Ausfall möglichst schnell wieder den Betrieb aufzunehmen, empfiehlt es sich, kritische IT-Systeme (z.B. Harddisk, Netzteile, Netzwerkkomponenten oder ganze Server) redundant halten.

- Erläuterungen**
- Redundanz heisst, dass mindestens ein identisches Ersatzgerät oder -system vorhanden ist, welches das beschädigte Gerät oder System bei einem Ausfall ersetzt.
 - Um den Ausfall einer Festplatte zu verhindern, kann eine sogenannte Festplattenspiegelung benützt werden. Falls eine Festplatte ausfällt, übernehmen automatisch andere Festplatten deren Aufgabe, ohne dass der Betrieb unterbrochen wird.
 - Schliessen Sie mit Ihren Lieferanten Serviceverträge für Hardware- und Software-Interventionen (Reaktionszeiten, Lieferfristen, usw.) ab.
 - Erarbeiten Sie eventuell mit Ihrem Lieferanten Notfallpläne für Ausfallszenarien (siehe Punkt 19).
- Tipps & Tricks**
- Benutzen Sie nur Komponenten von namhaften Herstellern. Diese sind in der Regel von guter Qualität und wurden intensiv getestet.
 - Denken Sie nicht nur an redundante IT-Systeme, sondern auch an eine redundante Internet-Anbindung.
 - Wichtig ist, dass die Ersatzgeräte identisch sind und bereits vorkonfiguriert sind, damit sie im Ereignis sofort eingesetzt werden können.

19

Planen Sie die Notfallvorsorge!

Grundsätze Ein existenzbedrohender Notfall tritt meistens plötzlich ein. Besonders höherer Gewalt ist man schutzlos ausgeliefert. Durch das richtige Verhalten kann in einer Notfallsituation der Schaden in Grenzen gehalten werden. Es muss deshalb im Voraus festgelegt werden, wie man sich bei einem Notfall verhält und welche Aktionen auszulösen sind.

- Erläuterungen**
- Überlegen Sie sich, welche Notfallsituationen in Ihrem Unternehmen eintreten können und wie darauf reagiert werden soll. Setzen Sie sich mit folgende Ausfallszenarien auseinander: Ausfall der IT, Ausfall von Personal, Ausfall der Arbeitsplätze oder des Gebäudes und Ausfall externer Partner und Dienstleistungen.
 - Bei einem Notfall muss schnell alarmiert und gehandelt werden. Jede Person muss genau wissen, wer alarmiert werden muss und wer verantwortlich ist. Erstellen Sie dazu einen Alarmierungsplan und eine Verantwortlichkeitsregelung.
 - Erstellen Sie einen Notfallvorsorgeplan. Dazu gehören Sofortmassnahmen zur Einleitung des Notfallbetriebs, Regelungen für den Ablauf des Notfallbetriebs und Massnahmen zur schnellen Wiederherstellung des Normalbetriebes.
 - Instruieren Sie die Mitarbeitenden, wie sie sich in Notfallsituationen zu verhalten haben und welche Sofortmassnahmen eingeleitet werden müssen.
 - In Stress-Situationen handelt der Mensch oft intuitiv. Das richtige Verhalten im Ereignisfall muss deshalb geübt werden.
 - Eventuell lohnt es sich, für grosse Risiken IT-Versicherungen abzuschliessen, z.B. Anlagenversicherung oder Zusatzversicherung für Datenträger- und Wiederherstellungskosten.
- Tipps & Tricks**
- Dokumentieren Sie alle IT-Komponenten ordnungsgemäss. Bewahren Sie diese Dokumentation extern auf.
 - Organisieren Sie Ausweichmöglichkeiten für die IT-Systeme mit der höchsten Verfügbarkeitsanforderung, damit schnell ein Weiterbetrieb gewährleistet werden kann.
 - Überprüfen Sie die Reaktionszeit des Supports mit Ihren Verfügbarkeitsanforderungen. Kann z.B. ein Serverausfall wirklich in der benötigten Zeit behoben werden?
 - Erarbeiten Sie mit dem Lieferanten und den Herstellern Notfallpläne für Ausfallszenarien (siehe Punkt 18).

20

Verteilen Sie das Know-how!

Grundsätze Gerade in kleineren KMU steckt das entscheidende Wissen über die IT-Systeme oft nur bei einer Person. Fällt sie aus oder verlässt sie das Unternehmen, dann gerät das Unternehmen in Schwierigkeiten.

- Erläuterungen**
- Das Schlüsselwissen steckt in der Konfiguration, im Betrieb und im Unterhalt der IT-Systeme des Unternehmens.
 - Krankheit, Unfall, Todesfall oder der Austritt aus dem Unternehmen können zum Verlust des Schlüsselwissens führen.
 -
- Tipps & Tricks**
- Damit das Wissen bei einem Ausfall nicht verloren geht, sollten wichtige Systeme und Prozesse dokumentiert werden. Das erleichtert auch den Nachfolgern und neuen Mitarbeitenden, sich schnell zurechtzufinden.
 - Zu einer Dokumentation gehören beispielsweise eine Liste der Benutzer, Gruppen und Rechte (siehe Punkt 12), das Netzwerklayout, die Konfigurationen der Systeme, Installationsbeschreibung, Konzepte, Arbeitsabläufe und Stellenbeschreibungen für sicherheitsrelevante Stellen. Führen Sie diese Dokumentationen regelmässig nach.
 - Versuchen Sie das Wissen von Personen zu verteilen und damit die Anzahl Schlüsselpersonal zu reduzieren.
 - Benutzen Sie eine einheitliche Namensgebung bei der Dokumentation und beschriften Sie die Dokumentation mit Versions-Nummer, Datum, Revisionsgrund und Name des Autors.
 - Erstellen Sie einen Netzwerkplan mit Ihren Servern und Netzwerkkomponenten.
 - Bewahren Sie wichtige Passwörter im Doppel in einem Safe auf.
 - Sichern Sie die geschäftsrelevanten Daten von ausgeschiedenen Mitarbeitenden.

Glossar

ADSL Schneller Anschluss ans Internet. Mit ADSL ist ein Computer permanent mit dem Internet verbunden und kann jederzeit angegriffen werden. Als Mindestschutz sollte eine *Firewall* eingesetzt werden.

Anti-Virus Software Auch Virens Scanner genannt. Programm, welches den Computer vor *Viren*, *Würmern* und *Trojanischen Pferden* schützt.

Attachment (Anhang). An eine E-Mail angehängte Datei. Viele bösartige Programme (*Malware*, *Crimeware*) werden so verbreitet und durch das Öffnen der Nachricht oder das Öffnen des Anhangs aktiviert. Anhänge sollten deshalb nur geöffnet werden, wenn man *Anti-Virus Software* einsetzt und den Absender der Nachricht kennt.

Backup Vorgang, bei dem durch Speicherung der Daten auf externen Speichermedien deren möglicher Verlust verhindert wird.

Benutzername (Username) Wird meist in Verbindung mit einem Passwort zur Anmeldung an einem Dienst (z.B. Internet) oder einem Programm verwendet. Betriebssystem Systemsoftware, in der englischen Kurzform als «OS» (Operating System) bezeichnet. Es handelt sich um eine Sammlung von speziellen Programmen, welche den Computer und die Anwendungsprogramme (z.B. Microsoft Word oder Excel) nutzbar machen.

Bluetooth Kurzstreckenfunk, welcher von mobilen Computern und Mobiltelefonen zum Datenaustausch genutzt werden kann.

Browser Programm, das man benutzt, um im Internet Informationen abzurufen. (z.B. Internet Explorer, Opera oder Firefox)

Client Computer, der an einem Netzwerk angeschlossen ist und mit anderen Computern in Verbindung steht.

Cracker Ein *Hacker*, der sein Wissen und seine Erfahrung nutzt, um anderen Schaden zuzufügen.

Crimeware Sammelbegriff für Programme, die von *Crackern* und anderen kriminellen Computerbenutzern eingesetzt werden, um anderen Computerbenutzern Schaden zuzufügen. Meist zielt *Crimeware* darauf ab, Geld oder wertvolle Information (z.B. Kreditkarten-Nummer) zu stehlen. Eine weniger aggressive Form wird als *Spyware* bezeichnet.

Download (Herunterladen) Vorgang, bei dem von einem entfernten Computer (z.B. im Internet) Daten und Programme auf dem eigenen Rechner gespeichert werden.

Firewall (Feuerwand, Brandschutzmauer) Gerät oder Computerprogramm, das Computer oder Netzwerke vor unerlaubtem Zugriff von Extern (z.B. *Cracker*) schützt.

Hacker Spezialist, der über ein enormes Wissen über Computer und Netzwerke verfügt und vorhandene Fehler erkennt und ausnutzt. Im Gegensatz zum *Cracker* haben Hacker keine illegalen Absichten.

Hub Gerät, an dem mehrere Computer angeschlossen werden können und so ein kleines Netzwerk bilden.

Instant Messenger Programm, mit dem in Echtzeit kurze Textnachrichten ausgetauscht werden können.

IP-Adresse Numerische Adresse, das Geräte in einem Netzwerk (z.B. Internet) eindeutig identifiziert.

ISDN Digitales Fernmeldenetz zur Übertragung von Sprache und Daten mit höherer Geschwindigkeit und Sicherheit im Vergleich zur analogen Technik.

Junk-Mail (Abfall-Mail) Unerwünschte elektronische Post, meist Werbung, wird auch als *Spam* bezeichnet.

Kabelmodem Gerät für Zugang zum Internet über das Kabelfernsehtz. Login Anmelden an einen Dienst, erfolgt in der Regel mit *Benutzername* und Passwort.

Malware Auch Malicious Code genannt. Sammelbegriff für bösartige und schädliche Programme, wie z.B. *Viren*, *Würmer* oder *Trojanische Pferde*.

Modem Gerät, das elektrische Signale in Töne umwandelt und umgekehrt. Wird benutzt, um über analoge Telefonleitungen mit digitalen Netzwerken (z.B. Internet) Verbindung aufzunehmen. Auch als *ADSL-Modem* oder *Kabelmodem* bekannt.

Patch (Pflaster) Aktualisierung von Programmen, bei welchen Fehler entdeckt wurden. Siehe auch *Update*.

PGP (Pretty Good Privacy), deutsch: «ziemlich gute Privatsphäre») Programm zur Verschlüsselung von Daten.

Pharming Erweiterter *Phishing*-Angriff, der den Computer des Opfers so manipuliert, dass der Angriff nur noch von professionellen Sicherheits- oder Netzwerkspezialisten erkennbar ist. In Anbetracht dieser Angriffsmethode ist der Einsatz eines Virens Scanners, einer *Firewall* und

das tägliche *Patchen* des Computers höchst empfohlen.

Phishing Angriffsmethode, die ein Opfer dazu verleiten will, *Login*-Angaben zu finanzrelevanten Diensten (z.B. eBanking) an einen Angreifer zu übermitteln; entweder via E-Mail oder den Besuch auf einer als Original getarnten Internet-Seite.

Port (Pforte, Tor) Numerische Angabe, die einen Dienst auf einem Rechner adressierbar macht. Damit ist die eindeutige Unterscheidung von verschiedenen Datenpaketen im Netzwerk möglich.

Provider Anbieter eines Zuganges zu Netzwerken (z.B. Internet). Bekannte Provider sind Bluewin, Sunrise oder Cablecom.

Remote Access Entfernter Zugriff auf ein Netzwerk oder einen Computer, in der Regel über das Internet. Solche Zugriffe sollten nur unter Zuhilfenahme von Sicherheitstechnologien wie *Firewalls* und *VPN* ermöglicht werden.

Router Gerät, das Netzwerke miteinander verbindet. Auch als *ADSL-Router* bekannt.

Server Computer, der in einem Netzwerk anderen Rechnern (*Clients*) Dienste zur Verfügung stellt. (z.B. Mail-Server)

Signatur, digitale Digitale Unterschrift mit verbindlichem Charakter.

Smart Card Plastic-Karte mit einem Chip, der Daten speichern kann, die über die Eingabe eines Codes (PIN) freigegeben werden können.

Spam Unerwünschte Massen-E-Mails, die als Kettenbrief oder Werbung für dubiose oder spezielle Produkte oder Dienste verschickt werden. Mit dem Spamfilter kann man sich dagegen schützen und einen grossen Teil des Spam aus der regulären Post herausfiltern.

Spyware Eine Art von *Malware*, welche eingesetzt wird, um Computeranwender auszuspionieren. Dabei werden das Verhalten, vor allem im Internet, beobachtet oder sogar die Eingaben auf der Tastatur mitgelesen (Passwortklau!). Als Schutz davor sollte regelmässig ein *Spyware*-Scanner eingesetzt werden.

Switch Gerät, das Computer oder Netzwerke miteinander verbindet. Wird in lokalen Netzwerken (LAN) eingesetzt.

Trojanisches Pferd Gefährliches *Malware*-Programm, welches meist unerkannt und unerlaubt auf dem eigenen Computer gespeichert und ausgeführt wird. Es meldet sich meist bei einem Angreifer (*Cracker*) und erlaubt die totale Kontrolle des Computers durch den Angreifer. Als Mindestschutz sollte ein *Virens Scanner* eingesetzt werden.

Update Aktualisierungsroutine, welche fehlerhafte Programme (z.B.: *Betriebssysteme*) repariert. Siehe auch *Patch*.

URL Adresse einer Seite im Internet, z.B. www.infosurance.ch

USB-Stick Auch «Memory Stick» genannt. Speichermedium, das am USB-Anschluss des Computers angeschlossen wird. Wird aufgrund seiner kleinen Ausmasse und grossen Speicherkapazität auch von Datendieben genutzt.

USV Steht für *unterbrechungsfreie Stromversorgung*. Gerät, das zwischen Stromversorgung und Verbraucher angeordnet wird und bei Stromausfall als Stützbatterie für den Verbraucher wirkt sowie als Filter den Verbraucher vor Spannungsschwankungen schützt.

Virus Meist schädliches Programm (*Malware*), das Daten zerstört oder die Nutzung des Computers verhindert. Kann durch jede Form der Datenübertragung (Internet, Diskette, CD-ROM, USB-Stick, E-Mail, etc.) verbreitet werden und verlangt zur Aktivierung eine Handlung des Benutzers. Als Schutz sollte ein *Virens Scanner* eingesetzt und regelmässig aktualisiert und aktiviert werden.

Virens Scanner Programm zum Auffinden und Entfernen von Computerviren und anderen Computerschädlingen. Siehe auch *Anti-Virus Software* und *Malware*.

VPN (Virtual Private Network) Technologie, die durch den Einsatz von Verschlüsselung und Zugangskontrollen (*Login*) die sichere Nutzung von öffentlichen Netzwerken (z.B. Internet) für private Zwecke ermöglicht.

Wurm Schädliches Programm (*Malware*), das sich ohne Zutun von Dritten und unter Ausnutzung von Schwachstellen oder fehlerhaften Programmen über Netzwerke ausbreitet und diese und die daran angeschlossenen Rechner vorübergehend blockiert. Oft enthalten Würmer auch Befehle, welche Daten zerstören. Als Mindestschutz sollte ein *Virens Scanner* eingesetzt werden.

Zombie Unter der Kontrolle eines Dritten (z.B. *Cracker*) stehender Computer, der ein *Trojanisches Pferd* beherbergt und in der Regel für Angriffe auf andere Computer innerhalb des Internet verwendet wird.