

Mehr Informationssicherheit für KMU

Das 10-Punkte-Programm für einen wirkungsvollen IT-Grundschutz



Basis für die vorliegende Broschüre bilden die «Zehn goldenen Regeln der Informationssicherheit in KMU» der Fachgruppe KMU der Stiftung InfoSurance. www.infosurance.ch/de/kmu.html

Konzept und Text:

Dr. Calista Fischer, Stiftung InfoSurance, Zürich

Druck und Gestaltung:

Fotorotar AG, Egg bei Zürich

Auflage: 60 000

Copyright:

Stiftung InfoSurance, Badenerstrasse 551, 8048 Zürich, Tel. +41 43 311 19 19, www.infosurance.ch
Die kostenlose Weiterverbreitung des Inhaltes dieser Broschüre ist unter Quellenangabe gestattet und im Sinn der Stiftung.

Die Stiftung InfoSurance übernimmt keinerlei Haftung für allfällige Schäden, die aus der Anwendung des 10-Punkte-Programms entstehen.

Liebe KMU-Geschäftsleiterin
Lieber KMU-Geschäftsleiter

Steht Ihr Ruf auf dem Spiel, verlieren Sie Kunden, oder müssen Sie gar Konventionalstrafe bezahlen, wenn Sie bei einem Auftrag nicht termingerecht liefern können? Haben Sie sich in diesem Zusammenhang schon einmal überlegt, ob in Ihrem Betrieb die Kernleistungen erbracht werden können, wenn das Computernetzwerk plötzlich nicht funktioniert? Unabhängig davon, ob in Ihrem Betrieb hundert oder bloss drei Computer im Einsatz stehen, als Mitglied der Geschäftsleitung sollten Sie sich periodisch mit Fragen dieser Art auseinander setzen.

Auch ein Betrieb, der seinen einzigen Computer nur dazu benutzt, um Rechnungen zu schreiben und gelegentlich ein E-Mail zu versenden, hat die gesetzliche Aufbewahrungspflicht von Geschäftsdaten zu erfüllen und den Datenschutz einzuhalten. Für einen unbeabsichtigten Verstoss gegen die gesetzlichen Auflagen reicht oft ein eingeschleppter Virus oder eine schlecht gewartete Firewall. Schlimmer noch, schädliche Computerprogramme können zum unwiederbringlichen Verlust von wichtigen Geschäftsdaten führen und so Ihr Unternehmen in seiner wirtschaftlichen Existenz gefährden.

Datenverluste und Computersysteme, die in kritischen Produktionsphasen durch bösartige Attacken aus dem Internet zusammenbrechen, können für die verantwortliche Geschäftsleitung teuer werden! Besonders da die Zahl der Angriffe auf Firmennetzwerke in den vergangenen Jahren dramatisch zugenommen hat und Schutzmassnahmen heute zu einem absoluten Muss geworden sind. Wer nicht dafür besorgt ist, dass in seinem Betrieb ausreichende Schutzvorkehrungen umgesetzt werden, lebt riskant. Auch ein Blick in die Zukunft bestätigt es: Das Thema Informationssicherung wird für alle Unternehmen immer bedeutender. Bereits heute verlangen Anbieter von Geschäftsversicherungen von ihren Kunden im Sicherheitsbereich immer mehr proaktives Handeln bis hin zum Nachweis von Sicherheitsvorkehrungen zur Informationssicherung. Es zahlt sich also aus, wenn Sie das Thema Informationssicherheit regelmässig in den Geschäftsleitungssitzungen thematisieren und diskutieren.

Wie Sie die Sicherheit und den Bestand Ihres Unternehmens, die Verfügbarkeit Ihrer Daten und Informationen nachhaltig verbessern und sich vor bösartigen Angriffen von innen und aussen schützen können, erfahren Sie auf den folgenden Seiten. Ziel unseres 10-Punkte-Programms ist es, Sie bei der Einführung eines wirkungsvollen Grundschutzes zu unterstützen, damit in Zukunft der Verlust von vitalen Geschäftsdaten verhindert werden kann und bei einem Systemausfall der finanzielle Schaden möglichst gering bleibt. Eine Checkliste und eine Linksammlung unterstützen Sie zusätzlich bei der Umsetzung des Programms und erlauben Ihnen die Kontrolle der umgesetzten Sicherheitsschritte.

Ich wünsche Ihnen und Ihrem Unternehmen viel Erfolg und eine nachhaltig verbesserte Informationssicherheit.



Dr. André Schmid,
Geschäftsleiter InfoSurance

«Zu je dreissig Prozent beruht Sicherheit auf technischen, organisatorischen und menschlichen Faktoren», so die Meinung von führenden Sicherheitsexperten zur Frage, wie Informations- und Kommunikationssysteme in Unternehmen sicher gemacht werden können. Die besten Sicherheitslösungen, die motiviertesten Mitarbeiter können nur dann zu einem wirkungsvollen Grundschutz beitragen, wenn auch die Geschäftsleitung ihren Beitrag zu mehr Sicherheit leistet.

- Bestimmen Sie in Ihrem Unternehmen, auch wenn Sie nur zwei Personen beschäftigen, einen EDV- bzw. IT-Verantwortlichen sowie einen Stellvertreter. Ist das nötige Wissen für diese Aufgabe nicht vorhanden, schicken Sie Ihre Mitarbeiterin oder Ihren Mitarbeiter in einen entsprechenden Kurs oder arbeiten Sie mit einem externen IT-Sicherheitsexperten zusammen. Ein dreitägiger Lehrgang oder eine externe Fachperson kommt Ihr Unternehmen wesentlich günstiger zu stehen als die Folgen eines Datenverlustes oder ein Verstoß gegen das Datenschutzgesetz.
- Alle Sicherheitsaufgaben, die an den internen IT-Verantwortlichen und an externe Personen delegiert werden, wie z.B. das Erstellen von Backups, sind schriftlich zu erteilen und in einem «Pflichtenheft» festzuhalten (eine Aufstellung mit den wichtigsten Aufgaben des IT-Verantwortlichen finden Sie unten).
- Kontrollieren Sie regelmässig, ob der IT-Verantwortliche die ihm übertragenen Aufgaben korrekt ausführt.
- Sämtliche Mitarbeiterinnen und Mitarbeiter, die an einem Computer tätig sind, erhalten ein Benutzungsreglement, das beschreibt, welche Aktionen auf dem Computer durchgeführt werden dürfen und welche untersagt sind (einen Vorschlag für ein Mitarbeiterreglement finden Sie auf Seite 9, Schritt 8).

Zu den Aufgaben eines internen oder externen IT-Verantwortlichen gehören u.a.:

- Regelmässige Datensicherung bei Servern, Clients (Arbeitsstationen), Notebooks (Laptops) und anderen mobilen Geräten (siehe Schritt 2).
- Aktuellhalten von Antivirus-Programm, Firewall, Betriebssystemen und sonstiger Software (siehe Schritte 3, 4 und 5).
- Führen einer Liste mit allen im Unternehmen vorhandenen Computern, den darauf installierten Programmen sowie den ausgeführten Software-Aktualisierungen (siehe Schritt 5).
- Verwalten der Zugriffsrechte – welche Programme darf der einzelne Mitarbeitende ausführen? Auf welche Daten, Informationen, Files hat er Zugriff?
- Führen und Aktuellhalten einer Liste mit allen Personen, die Remote Access auf das Firmennetzwerk haben, also von aussen auf das Firmennetzwerk zugreifen können – u.a. genaue Dauer der Berechtigung festlegen und diese nach Ablauf entziehen. Sorgen Sie dafür, dass deren Schutzprogramme aktuell gehalten werden.
- Sicherstellen, dass es von IT-Seite zu keinen Verletzungen des Datenschutzgesetzes kommt – u.a. durch das Aktuellhalten der diversen Schutzprogramme (Firewall, Antivirus-Programm) und das Verwenden von starken Passwörtern (siehe Schritte 3, 4, 7).
- Kontrollieren, dass die Mitarbeiterinnen und Mitarbeiter die IT-Richtlinien einhalten (siehe Schritt 8).
- Ansprechpartner für Sicherheitsfragen, Meldestelle bei sicherheitsrelevanten Vorkommnissen – z.B. bei Verlust von Notebooks, bei festgestellten Viren usw.

Nicht nur Hacker und Viren bedrohen Ihre Geschäftsdaten. Auch Gefahren wie Feuer, Wasser, Kurzschlüsse können im Schadensfall zum Totalverlust von wichtigen Informationen führen. Eine doppelt unangenehme Situation, denn auch der Gesetzgeber verlangt, dass Geschäftsdaten aufbewahrt und archiviert werden. Der Verlust von Betriebsdaten ist in jedem Fall unbedingt zu verhindern. Daten werden deshalb regelmässig gespeichert, sicher archiviert und die Backups periodisch getestet.

- Sorgen Sie dafür, dass elektronische Daten regelmässig auf einem beweglichen Speichermedium, wie Band, CD, DVD oder Diskette, gespeichert werden. Die Häufigkeit der Datensicherung richtet sich nach Tätigkeit und Grösse Ihres Unternehmens. Die komplette Sicherung aller Daten muss im Minimum einmal pro Woche, bei grösseren Betrieben täglich durchgeführt werden.
- Regeln Sie schriftlich, wer die Datensicherung ausführt und wie häufig dies zu geschehen hat. Führen Sie eine Kontrollliste, in der die erfolgte Datensicherung eingetragen werden muss (siehe Pflichtenheft IT-Verantwortlicher, Schritt 1).
- Gesichert werden alle im Unternehmen bearbeiteten Daten – sämtliche Files (Dateien), Briefe, Tabellen und E-Mails mit geschäftsrelevantem Inhalt.
- Idealerweise wird auch von der Softwarekonfiguration ein Backup gemacht. So wird bei einem Totalausfall der Computersysteme wertvolle Zeit gespart, weil die Software schneller wieder installiert werden kann.

■ **Wichtig:** Wochen-, Monats- und Jahres-Backups dürfen nicht im Betrieb aufbewahrt werden, da sie bei Feuer oder Wassereintrüben ebenfalls zerstört werden! Auch Daten, wie z.B. wichtige Verträge und Urkunden, die nur in Papierform vorliegen, sollten unbedingt kopiert und ausser Haus gebracht werden. Empfohlener Aufbewahrungsort für Sicherungskopien und wichtige Geschäftspapiere: Banksafe oder bei Ihnen zu Hause.

- Prüfen Sie regelmässig, ob sich Ihre Sicherungskopien noch lesen lassen!

Beispiel für einen Betrieb mit täglichem Backup

- Tages-Backup: je ein Speichermedium (Band, CD, DVD oder Diskette) für die Tage Mo, Di, Mi und Do. Die Tageskopien werden jeweils am entsprechenden Wochentag in der folgenden Woche überschrieben. Tageskopien werden im Betrieb, aber ausserhalb des Serverraums, aufbewahrt.
- Wochen-Backup: jeden Freitag. Für jeden Freitag im Monat ist ein separates Speichermedium zu verwenden – ausserhalb des Betriebs aufbewahren!
- Monats-Backup: jeweils Ende Monat. Die Monats-Backups werden nicht mehr überschrieben – ausserhalb des Betriebs aufbewahren!
- Jahres-Backup: jeweils Ende Jahr. Das Jahres-Backup wird nicht mehr überschrieben – ausserhalb des Betriebs aufbewahren!

Internet und E-Mail sind Kommunikations- und Informationsmittel, die aus dem modernen Geschäftsalltag nicht mehr wegzudenken sind. Schädliche Programme, wie z.B. Viren, können diese Kommunikationsinfrastrukturen lahm legen und die wirtschaftliche Existenz eines Unternehmens gefährden. Neben dem direkten Schaden werden unzureichend geschützte Computersysteme häufig zur Verbreitung von Viren und für gezielte Attacken gegen ein drittes Unternehmen missbraucht. Wer als Geschäftsleiter ungenügende Vorkehrungen zum Schutz seiner Computersysteme trifft, handelt fahrlässig und muss allenfalls sogar mit Strafverfolgung rechnen.

- Computerviren können Daten und Programme verändern, manipulieren oder sogar vollständig zerstören. Bösertige Computerprogramme werden via E-Mail-Anhänge (Attachments) und Speichermedien wie Disketten usw. übertragen. Im Internet sind Viren oft als nützliche oder unterhaltende Gratisprogramme getarnt, die durch einen simplen Mausklick aktiviert werden.
- Den einzigen Schutz vor bekannten Viren bietet ein Antivirus-Programm, das gefährliche Eindringlinge, wie Viren und Würmer, identifiziert und unschädlich macht. Die entsprechenden Programme können in Computerläden gekauft oder kostenlos aus dem Internet heruntergeladen werden.
- Da Hacker dauernd neue Viren programmieren, muss das Antivirus-Programm laufend aktualisiert werden. Je nach Produkt, das Sie verwenden, sucht sich das Programm auf der Homepage des Herstellers selbständig die verfügbaren Aktualisierungen. Informieren Sie sich bei Ihrem Verkäufer, ob dies bei Ihrem Programm der Fall ist. Falls dies nicht so ist, sollte die Aktualisierung jede Woche, besser noch jeden Tag durchgeführt werden.
- Damit Ihr Netzwerk zuverlässig vor Viren und anderen schädlichen Programmen geschützt ist, muss das Antivirus-Programm auf sämtlichen Servern und Arbeitsstationen (Clients) installiert und regelmässig aktualisiert werden.
- «Virus-Scans» sind im Minimum einmal wöchentlich durchzuführen, damit unerkannt eingeschleppte Viren entdeckt und eliminiert werden können. Bei regem Datenaustausch und bei Verdacht auf einen Virus empfiehlt sich ein täglicher Virus-Scan.
- Bei grösseren Netzwerken werden das Antivirus-Programm und die Aktualisierungen am besten zentral und automatisch betrieben.
- **Nicht vergessen:** Werkseitige Passworteinstellungen bei Geräten, Betriebssystemen und Anwendungsprogrammen müssen vom IT-Verantwortlichen sofort geändert werden – Pflichtenheft IT-Verantwortlicher!

Tipps für Mitarbeiter IT-Richtlinien (siehe auch Schritt 8):

- Eingegangene Virus-Warnungen müssen unverzüglich dem IT-Verantwortlichen gemeldet werden.
- Das Ausschalten des Antivirus-Programms ist ausdrücklich untersagt.
- Tests, wie und ob das Antivirus-Programm im Ernstfall funktioniert, sind ausdrücklich nicht gestattet.

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 ist es die Firewall, die diese Sicherheitsaufgabe erfüllt. Ohne Firewall können Unbefugte auf Ihren Computersystemen Befehle ausführen, an Geschäftsgeheimnisse und Daten gelangen, die dem Datenschutzgesetz unterstehen oder auch Ihre Rechner zu illegalen Attacken auf Dritte missbrauchen.

- Installieren Sie eine Firewall. Sorgen Sie dafür, dass der Internetzugang ausschliesslich über die Firewall erfolgen kann (siehe unten). Für Firmennetzwerke ist eine Hardware-Firewall, für mobile Geräte (Notebooks) eine Software-Firewall zu empfehlen. Im Handel sind Produkte erhältlich, die gleichzeitig eine Firewall und einen Antivirenschutz bieten. Gerade für kleinere Betriebe sind kombinierte Produkte sehr zu empfehlen.
- Manche Betriebssysteme, wie z.B. Windows XP oder Mac OSX, haben eine Firewall eingebaut, die allerdings keinen vollständigen Schutz bietet. Nutzen Sie aber auf jeden Fall auch diese Möglichkeit und aktivieren Sie die Firewall.
- Die Firewall muss regelmässig mit den neuesten Bedrohungsmustern aktualisiert und auf ihre Funktionsfähigkeit geprüft werden (Update – siehe Schritt 5).
- Sämtliche Netzwerkübergänge müssen mit einer Firewall gesichert werden. Stellen Sie sicher, dass die Verbindungen zu Lieferanten, Kunden, Outsourcern und Mitarbeitenden, die Remote Access auf Ihr Netzwerk haben, mit einer Firewall gesichert sind und diese Firewalls aktuell gehalten werden.
- Wenn in Ihrem Betrieb Wireless-LAN-Computer eingesetzt werden, sorgen Sie dafür, dass dies richtig und sicher getan wird (siehe Schritt 6). Falsch genutzte Wireless-LAN-Geräte machen den ganzen Schutz zunichte, den Ihnen Ihre Firewall bietet.
- Falls der Zugang zur Konfiguration Ihrer Firewall mit einem Passwort geschützt werden kann, sollten Sie dies tun. Verwenden Sie dazu ein starkes Passwort (siehe Schritt 7). Es lohnt sich, die Konfiguration der Firewall zu speichern (siehe Schritt 2).

Tipps für Mitarbeiter IT-Richtlinien:

Der gesamte Internetverkehr wird über die Firewall abgewickelt. Aus Sicherheitsgründen ist es untersagt:

- auf anderen Wegen, z.B. via Modem, auf das Internet zuzugreifen,
- private Laptops und
- Wireless-LAN-Geräte im Unternehmen ohne schriftliche Einwilligung des IT-Verantwortlichen einzusetzen.

Kontrollieren Sie bei Ihrem Auto auch regelmässig Ölstand und Reifendruck? Und sorgen Sie bei abgenutzten Bremsbelägen dafür, dass diese rechtzeitig ersetzt werden? Genau so, wie Sie Ihren Wagen aus Sicherheitsgründen regelmässig warten, müssen auch die Computerprogramme in einem Unternehmen periodisch gepflegt und auf den neuesten Stand gebracht werden.

Menschen machen Fehler – da Computerprogramme von Menschen geschrieben werden, gibt es auch keine fehlerfreien Computerprogramme. Aus diesem Grund bieten die Hersteller regelmässig Software-Aktualisierungen an, so genannte «Updates» («Aktualisierung») oder «Patches» («Pflaster», «Korrektur»).

- Sorgen Sie dafür, dass die neuesten «Patches» für Betriebssysteme und Applikationen (Anwendungsprogramme) bei Ihnen installiert werden.
- Installieren Sie nur Aktualisierungen für die von Ihnen tatsächlich verwendete Version des Betriebssystems (z.B. Windows XP) und die von Ihnen eingesetzten Anwendungsversionen (z.B. Explorer 6).
- Verfügbare «Sicherheits-Updates» sollten immer sofort installiert werden.
- Bei den übrigen, nicht sicherheitsrelevanten «Updates» empfiehlt es sich abzuklären, besonders, wenn Sie Programme von verschiedenen Herstellern verwenden (z.B. Windows und SAP-Applikation), ob der neue «Patch» Störungen verursachen kann.
- Sämtliche am Netzwerk angeschlossenen Computer müssen «gepatcht» werden. Dies gilt auch für Notebooks und Geräte von externen Mitarbeiterinnen und Mitarbeitern!
- Für jeden Computer ist eine Liste zu führen, welche «Updates» installiert sind.

Hier finden Sie die neuesten «Updates» für die gängigsten Produkte:
Für Windows-Anwender: www.windowsupdate.com
Für Office-Anwender: www.officeupdate.com

«Mobile Computing» – von der mobilen Unsicherheit zu mehr mobiler Sicherheit

Zugegeben, ausgesprochen praktisch, vielseitig und schick sind sie ja, die Mobiltelefone, die kleinen Handheld-Computer und die Notebooks mit Wireless-LAN. Aus dem Geschäftsalltag sind sie auf jeden Fall nicht mehr wegzudenken. Doch falsch eingesetzt, bedeuten diese Geräte für jeden Betrieb ein immenses Sicherheitsrisiko. Besonders, wenn heikle Geschäftsdaten auf ihnen gespeichert sind. Wer aus geschäftlichen Gründen gezwungen ist, sensible Daten auf mobilen Geräten zu speichern, muss spezielle Sicherheitsvorkehrungen treffen.

- Sorgen Sie dafür, dass auf mobilen Geräten nur diejenigen Daten enthalten sind, die tatsächlich benötigt werden.
- Sämtliche mobilen Geräte müssen mit einem starken Passwort geschützt werden (siehe Schritt 7). Beim Verlust des Geräts oder im Fall eines Diebstahls haben Unbefugte sonst ein leichtes Spiel, an Ihre vertraulichen Geschäftsdaten zu gelangen.
- Heikle Firmendaten 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 heruntergeladen werden (z.B. PGP – Pretty Good Privacy – www.pgp.com).
- Über falsch eingesetzte Wireless-LAN-Geräte können Hacker aus Distanzen bis zu 500 Meter mit einfach zu bedienenden Programmen innerhalb von Minuten in Ihr Firmennetzwerk einbrechen! Besondere Vorsicht ist auch geboten, wenn Sie oder Ihre Mitarbeiter von einem externen Access Point (Hot Spot) auf das Firmennetz zugreifen.
- Aktivieren Sie bei Geräten mit Bluetooth (Handy, mobile Agenda, Handheld-Computer) diese Funktion nur bei Bedarf. In der übrigen Zeit ist die Bluetooth-Funktion zu deaktivieren. Sonst laufen Sie Gefahr, dass Ihr Gerät im Umkreis von bis zu 100 Meter ohne Ihr Wissen auf die Anfragen von anderen Bluetooth-Geräten antwortet.
- Tauschen Sie über Bluetooth nur Daten mit Personen aus, denen Sie vertrauen.

6 Schritte zu einem sicheren Umgang mit Wireless-LAN in und ausserhalb des Unternehmens:

- Ändern Sie den vom Hersteller vorgegebenen Namen für Ihr kabelloses Netzwerk (Service Set ID – SSID). Verwenden Sie als neue Identifikation keinesfalls Ihren Firmennamen oder einen Begriff, der Rückschlüsse auf Ihre Tätigkeit erlaubt.
- Ändern Sie das Standard-Passwort Ihres Access Points. Verwenden Sie ein starkes Passwort (siehe Schritt 7).
- Aktivieren Sie die Verschlüsselung der kabellosen Datenübermittlung WEP (Wired Equivalent Privacy). Wählen Sie wenn möglich eine 128-bit-Verschlüsselung. Ändern Sie den vom Hersteller standardmäßig eingestellten WEP-Schlüssel. Vorsicht: Der WEP-Schlüssel kann von speziellen Hackerprogrammen innerhalb von ein bis zwei Stunden geknackt werden. Der WEP-Schlüssel sollte deshalb regelmäßig gewechselt werden.
- Verwenden Sie einen MAC-Adressen-Filter, falls Ihr Produkt diese Option bietet.
- Deaktivieren Sie die ungerichtete SSID-Ausstrahlung.
- Wireless-LAN-Geräte sollten ausschliesslich in einem Virtual Private Network (VPN) betrieben werden. Wird eine Verbindung ins Firmennetz über einen öffentlichen Access Point hergestellt, darf dies nur über VPN erfolgen. Viele Betriebssysteme beinhalten bereits ein VPN-System. Nutzen Sie es!



Wer Ihr Computerpasswort oder das Ihrer Mitarbeiter kennt und sich damit einloggt, besitzt Ihre Identität und verfügt über Ihre Berechtigungen. Durch Passwortdiebstahl können Unbefugte einfach an wichtigste Geschäftsformationen gelangen. Verhindern Sie also, dass in Ihrem Betrieb der Identitätsdiebstahl möglich ist. Halten Sie Ihre Mitarbeiter 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 acht Zeichen lang, enthalten Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen.
- Unbedingt Passwortmerkmale einsetzen! Anstelle des Passwortes merkt man sich einen geheimen Satz, was viel einfacher ist. Dem starken Passwort V2Jfd€u6% liegt der Satz «Vor 2 Jahren fiel der Euro um 6 Prozent» zugrunde. Um dieses Passwort zu erkennen, benötigt ein Hacker-Programm rund sechzig Jahre. Weitere Beispiele: Der Fragesatz «Fahren wir in 2 x 7 Tagen zu dritt nach Paris?» ergibt das starke Passwort «Fwi2x7TzdnP?».
- Wenn Sie unsicher sind, ob Ihr Passwort stark ist, können Sie mit einem ähnlichen Passwort einen Test durchführen. Tipp: Ein Passwort-Check macht Spass und ist ein gutes Mittel zur Mitarbeitersensibilisierung. Passwort-Check: www.datenschutz.ch
- **Nicht vergessen:** Werkseitige Passworteinstellungen bei Geräten, Betriebssystemen und Anwendungsprogrammen müssen vom IT-Verantwortlichen sofort geändert werden – Pflichtenheft IT-Verantwortlicher!



Verbotene Passwörter sind:

- Weniger als acht Zeichen lang
- Wörter und Namen, die in Wörterbüchern oder Dictionnaires zu finden sind – sie werden von einem Hackerprogramm mit Leichtigkeit erkannt
- Namen und Geburtsdaten aus dem Familienumfeld – sie können von Kollegen oder Bekannten leicht erraten werden
- AHV- und Pass-Nummern
- Namen und Begriffe aus dem Hobbybereich
- Zahlen- und Buchstabenfolgen, wie z.B. 1234 oder abcde, asdf

Verbotene Handlungen mit Passwörtern sind:

- Aufschreiben von Passwörtern auf Zetteln oder im Computersystem
- Das gleiche Passwort über längere Zeiträume zu verwenden – Passwortwechsel mindestens alle ein bis zwei Monate (evtl. Passwort-Wechsel forcieren durch IT-Verantwortlichen)
- Weitergeben des Passwortes an Dritte. Falls dies trotzdem einmal geschehen musste, ist das Passwort umgehend zu wechseln.

IT-Richtlinien und Sicherheitskampagnen schaffen Klarheit und Sicherheit bei Ihren Mitarbeitern

Ist bei Ihnen im Betrieb «erlaubt, was nicht stört»? Ohne verbindliche und verständliche Sicherheitsrichtlinien können Ihre Mitarbeiter nicht wissen, welche Handlungen erlaubt und welche nicht gestattet sind. Überlassen Sie die Sicherheit Ihrer Daten nicht dem Gutdünken Ihrer Mitarbeiter. Doch aufgepasst, Sicherheitsvorkehrungen werden von vielen als störend empfunden. Sensibilisieren Sie deshalb Ihre Mitarbeitenden regelmässig für die Sicherheit in Ihrem Betrieb. Sicherheitsregeln werden nur ernst genommen, wenn auch die Chefin und der Chef sie einhalten. Handeln Sie in allen Sicherheitsaspekten immer als Vorbild.

- Schriftliche Sicherheits- und IT-Richtlinien erlassen und von den Mitarbeitern unterzeichnen lassen (siehe unten).
- Basisausbildung aller Mitarbeitenden, z.B. auf Grundlage dieser Broschüre. Wichtigste Lernziele:
 - Bestimmen starker Passwörter (siehe auch Schritt 7)
 - Sicherer Umgang mit Internet und E-Mail
 - Sicherer Umgang mit dem Virenschutzprogramm
 - Ablegen und sichern von Dokumenten
 - Verstehen der Sicherheits- und IT-Richtlinien
- Durchführen von ein- bis zweijährlichen Sicherheits- und Sensibilisierungskampagnen. Dies lässt sich mit einfachen Mitteln, wie z.B. E-Mails an alle Mitarbeiter, Rundschreiben in der internen Post und Plakaten im Eingangsbereich und in der Kantine, kostengünstig realisieren. Beiträge in der Firmenzeitung usw. leisten ebenfalls wertvolle Dienste.
- Sorgen Sie deshalb dafür, dass Sicherheit in Ihrem Unternehmen immer wieder und auf ganz unterschiedliche Weise zum Thema gemacht wird.

Typische Punkte für Mitarbeiter-IT-Richtlinien:

- Umgang mit Passwörtern (siehe Schritt 7)
- Einsatz und Installation von nicht genehmigten Programmen untersagen (u.a. mobile Agenden, Spiele, animierte Bildschirmschoner usw.)
- Einsatz von nicht genehmigten Hardware-Komponenten untersagen (z.B. USB-Sticks, Modems, private Laptops, Wireless-LAN, Handheld-Computer usw.)
- Gebrauch des Internets festlegen – Informationen dürfen aus dem Internet heruntergeladen werden, nicht aber Programme, wie z.B. animierte Bildschirmschoner, Filme usw. Der Besuch von Chatrooms und Webseiten mit pornografischen, rassistischen und sexistischen Inhalten ist untersagt.
- Gebrauch von E-Mail festlegen
- Umgang mit Antivirus-Programm inkl. Aktualisierung festlegen, sofern dies nicht zentral vorgenommen wird
- Umgang mit Sicherheits-Patches regeln, sofern dies nicht zentral vorgenommen wird
- Datensicherung und Aufbewahrungspflicht festlegen
- Einhalten des vorgegebenen Ordnungssystems (siehe Schritt 10)
- Umgang mit Daten regeln, die dem Datenschutzgesetz unterstehen
- Umgang mit internen, vertraulichen und geheimen Informationen und Daten festlegen – z.B., welche Daten über E-Mail verbreitet werden dürfen
- Verhalten bei sicherheitsrelevanten Vorkommnissen, z.B. bei Viruswarnungen, Diebstählen und Verlusten von Laptops und Passwörtern – IT-Verantwortlicher muss sofort informiert werden
- Ankündigen von Disziplinar massnahmen und Sanktionen für den Fall, dass gegen die internen Sicherheitsrichtlinien verstossen wird.

Mitarbeiter-Richtlinien für den IT-Gebrauch

Wissen Sie, wer bei Ihnen über den Tag so alles ein und aus geht? Und können Sie für sämtliche Besucher die Hand ins Feuer legen? Einige wenige Vorkehrungen verhindern bereits, dass wichtige Geschäftsinformationen durch Unachtsamkeit an Unbefugte gelangen. Gelebte Sicherheit ist heute ein Qualitätskriterium und schafft Vertrauen bei Kunden und Lieferanten.

- Lassen Sie Besucher, Kunden und Bekannte nicht unbeaufsichtigt in Ihrem Betrieb umhergehen.
- Alle Drittpersonen werden am Empfang abgeholt und auch stets wieder zum Ausgang begleitet.
- Wer über kein Empfangsdesk verfügt, das den Eingangsbereich überblickt, oder wer den Empfang nicht dauernd besetzt halten kann, hält die Eingangstüre verschlossen und bringt ein Schild «Bitte läuten!» an.
- Sorgen Sie dafür, dass Schlüssel und Badges korrekt verwaltet und die entsprechenden Listen aktuell gehalten werden. Schlüssel mit Passepartout-Funktion sind nur restriktiv zu verteilen. Die entsprechenden Berechtigungen müssen periodisch auf ihre Notwendigkeit geprüft werden.
- Mitarbeiterinnen und Mitarbeiter, die aus dem Unternehmen austreten, müssen ihre Schlüssel, Badges und Zugangsberechtigungen beim Austritt abgeben.
- Stellen Sie sicher, dass sämtliche Eingangs- und Hintertüren sowie Parterrefenster über einen ausreichenden Einbruchschutz verfügen. Entsprechende Informationsblätter sind bei der örtlichen Polizei erhältlich.
- Server gehören in verschlossene Räume, zu denen nur der IT-Verantwortliche und sein Stellvertreter Zutritt haben. Wo dies nicht möglich ist, wird der Server wenigstens in einen abschliessbaren Computerschrank (Rack) eingebaut.
- Brennbares Material, wie Papier usw. nicht im Serverraum lagern.
- Sorgen Sie dafür, dass im Serverraum oder in unmittelbarer Nähe ein gut sichtbarer CO₂-Feuerlöscher platziert wird.
- Netzwerkdrucker gehören nicht in öffentlich zugängliche Räume, da Unbefugte Einblick in Dokumente erhalten können, die nicht für sie bestimmt sind (Datenschutzgesetz, Betriebsgeheimnisse usw.).
- Netzkabel, die durch öffentlich zugängliche Räume führen, sowie Modems, Hubs, Router und Switches in öffentlichen Räumen müssen speziell geschützt werden.

Hat Ordnung etwas mit Sicherheit zu tun? Mehr, als man auf den ersten Blick vielleicht meinen möchte. Ganz abgesehen von der Zeitersparnis, die ein aufgeräumter, ordentlicher Arbeitstisch bietet, gehen Informationen und Dokumente weniger verloren, als wenn die Arbeitsfläche mit Papieren, Handzetteln und Mäppchen übersät ist. Die Gefahr, dass sensible Dokumente im ungünstigsten Augenblick auftauchen oder von Unbefugten durch Zufall gelesen werden, wird so von Anfang an minimiert. Und denken Sie daran, Ordnung ist auch eine Frage des Images: Als Kunde oder Lieferant schliesst man vom ordentlichen Äussern bei einem Unternehmen gern auf die innere Haltung.

- Für elektronische Daten und die Aufbewahrung von Papierdokumenten ist ein Ablagesystem einzuführen, das alle einhalten müssen – z.B. Ablage nach Kunden, Projekten.
- Nicht mehr benötigte Papierdokumente und Notizen mit sensiblen Daten müssen sicher vernichtet werden (Aktenvernichter oder Zerreißen). Sie gehören weder in den Abfall noch ins Altpapier.
- Das Ablagesystem muss logisch aufgebaut und so gestaltet sein, dass es von den Mitarbeiterinnen und Mitarbeitern verstanden und auch konsequent angewendet werden kann (siehe Schritt 8).
- Nicht mehr benötigte elektronische Daten auf Speichermedien wie Disketten, CDs und DVDs müssen sicher gelöscht und mehrfach überschrieben werden. Mit Microsoft-Windows ist dies nicht möglich. Der einfache Löschbefehl reicht also nicht aus! Nicht mehr benötigte Speichermedien mit sensiblen Daten werden deshalb physisch zerstört.
- Die saubere Arbeits- und Dokumentenübergabe bei Ferienabwesenheiten verhindert, dass Mitarbeiter in den Unterlagen oder Computern ihrer Kollegen stöbern und so durch Zufall auf Informationen stossen, die nicht für sie bestimmt sind.
- Werden Speichermedien ausser Haus gegeben, sind dafür neue, noch nie verwendete Datenträger einzusetzen. Konventionell gelöschte Informationen können leicht wieder hergestellt und von Unbefugten gelesen werden.
- Grundlagen für mehr Sicherheit, wie ausreichende Anzahl Schränke, Korpusse, Ordner usw. zur Verfügung stellen.
- Ordner mit Personaldaten, Verträgen und Offerten gehören unter Verschluss, damit es nicht zu Verstössen gegen das Datenschutzgesetz kommt.
- Während der Pausen und Abwesenheiten vom Arbeitsplatz sollte der Computer ausgeschaltet oder der Benutzer abgemeldet werden, damit Unbefugte keinen Einblick auf die bearbeiteten Dokumente haben. Wer mit sensiblen Daten arbeitet, schliesst sein Büro ab.
- Wer mit sensiblen Daten am Computer arbeitet, positioniert seinen Bildschirm so, dass Kollegen und Besucher die Informationen nicht ablesen können.

Glossar

Applikation Anwendungsprogramm, z.B. ein Textverarbeitungsprogramm oder ein E-Mail-Programm.

ADSL Sehr schneller Internetzugang. Bei ADSL ist der Computer bzw. der Server permanent mit dem Internet verbunden und Hackerangriffen somit dauernd ausgesetzt – *Firewall* einsetzen!

Attachment Anhang, an eine E-Mail angehängte Datei. Viele böartige Programme (*Malicious Code*) werden in solchen Anhängen verbreitet und durch das Öffnen des Attachments aktiviert. Attachments sollten deshalb nur von bekannten Absendern geöffnet werden.

Backup Wörtlich Rückendeckung, im IT-Zusammenhang Sicherungen von Daten, Programmen und Programmkonfigurationen.

Benutzername Bei der Anmeldung an ein Programm oder einen Dienst (z.B. Internet) werden in der Regel standardmässig ein frei wählbarer Benutzername und ein *Password* abgefragt. Dies dient zur Identifikation des berechtigten Benutzers.

Betriebssystem Systemsoftware oder Systemprogramme. Gruppe meist kleinerer Programme, die beim Start des Computers geladen werden und ihn betriebsbereit machen.

Browser Software, die es gestattet, von Servern im Internet Informationen abzurufen.

CD Speichermedium mit einer Speicherkapazität von bis zu 700 MB.

Client Arbeitsstation, d.h. der einzelne am Netzwerk angeschlossene Computer.

Diskette Speichermedium mit einer Speicherkapazität von 1.44 MB, für die langfristige Datenaufbewahrung nicht geeignet.

Download Wörtlich «herunterladen», gemeint ist das Herunterladen von Programmen und Updates aus dem Internet.

DVD Speichermedium mit 4.3 GB.

Firewall Wörtlich Brandschutzmauer, Gerät oder Sicherheitsprogramm, das die Verbindung ins Internet sichert und ein Netzwerk oder einen einzelnen Computer vor unbefugtem Zugriff von ausserhalb des Netzwerks schützt.

Hardware Physische Geräte, z.B. Computer, Drucker, Maus, Tastatur.

Hub Gerät, an welches mehrere Rechner eines Netzwerks angeschlossen werden, um eine sternförmige, strukturierte Topologie zu realisieren.

IP-Adresse Numerische Adresse, dient der Identifizierung der einzelnen Geräte in einem Netzwerk.

ISDN Digitales Fernmeldenetz zur Übertragung von Telefon, Fax und Daten mit Übertragungsraten von 64 bzw. 128 KB pro Sekunde. Im Vergleich mit der analogen Technik verbesserte Übertragungsqualität und -sicherheit.

Junk-Mail Wörtlich Abfall-Mail, unerwünschte E-Mails.

Login Anmelden an einen Dienst, erfolgt in der Regel mit *Benutzername* und *Password*.

Malicious Code Sammelbegriff für böartige Programme, wie z.B. *Viren*, *Würmer*, *Trojaner* usw.

Modem Elektronisches System, das zur Aufbereitung und/oder Umwandlung elektrischer Signale für Senden und Empfang in Kommunikations-Netzwerken verwendet wird und den Internetzugang über die Telefonleitung ermöglicht.

Password Geheimer Erkennungscode bzw. Schlüssel.

Patch Wörtlich Pflaster, Programmaktualisierung von Betriebssystem- und Anwendungsprogrammen (*Update*).

Port Wörtlich Pforte, numerische Angabe, die dazu dient, ein ankommendes Datenpaket an die richtige Pforte, d.h. an den richtigen Dienst, zu vermitteln. So wird ein ankommendes E-Mail als solches identifiziert und durch den E-Mail-Port hereingelassen.

Provider Anbieter eines Internetzugangs, z.B. Bluewin, Sunrise, Cablecom, Green.ch.

Remote Access Zugriff von ausserhalb auf das firmeneigene Netzwerk. Die Berechtigung für Remote Access ist zeitlich zu limitieren, die Aktivitäten von Personen mit Remote Access müssen überwacht werden.

Router Gerät, welches Netzwerke untereinander verbindet.

Server Computer, der seine Hardware- und Software-Ressourcen in einem Netzwerk anderen Rechnern (*Clients*) zugänglich macht, z.B. Applikations-, Daten-, Web-, Mail-Server.

Signatur, digitale Digitale Unterschrift mit verbindlichem Charakter.

Software Informationen und Programme, die von der *Hardware* bearbeitet oder ausgeführt werden können.

Spam Massen-E-Mail, analog zu den Kettenbriefen, die früher mit der Post verschickt wurden. Gegen Spam hilft ein *Spamfilter*.

Spamfilter Filtert ungewünschte *Spam*-E-Mails aus dem Posteingang. Internet-*Provider* bieten oftmals die Möglichkeit, Spam bereits auf der *Provider*-Ebene auszufiltern, so dass die unerwünschten E-Mails gar nicht in den regulären Posteingang gelangen. Für einen weitergehenden Spamschutz sind im Handel Programme erhältlich. Verschiedene Hersteller bieten Programmpakete an, die *Firewall*, *Virenschutz* und *Spamfilter* umfassen.

Switch Gerät, welches Computer untereinander verbindet.

Trojaner, trojanisches Pferd Schädlicher Programmteil (*Malicious Code*). Wird üblicherweise als Bestandteil einer E-Mail, beim Herunterladen einer Datei oder durch offene Ports unbemerkt auf dem Rechner abgespeichert. Unter vorgegebenen Bedingungen aktiviert es sich auf dem befallenen Computer und sammelt, manipuliert oder zerstört Daten. Moderne Form von Spionage und Sabotage.

Update Aktualisieren eines Programms (*Patch*).

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

USB-Stick Speichermedium, das in den USB-Port gesteckt wird. Dank seiner Kleinheit und der riesigen Speicherkapazität (bis zu 1 GB) ein Gerät, das gerne in der Wirtschaftsspionage eingesetzt wird.

Virus Verstecktes, schädliches Programm (*Malicious Code*), das Daten zerstört. Kann durch jede Form der Datenübernahme (*Internet*, *Disketten*, *CDs*, *Netzwerke* usw.) übertragen und verbreitet werden – *Anti-virus*-Programm einsetzen.

Virens scanner Programm zum Auffinden von Computerviren.

VPN Abkürzung für Virtual Private Network, Netzwerk aus virtuellen Verbindungen (z.B. via Internet), über die Daten sicher (verschlüsselt) übertragen werden. Dank VPN können die verschiedenen Zweigstellen eines Unternehmens kostengünstig und abhörsicher miteinander kommunizieren.

Wurm Von einer Datei unabhängiges, schädliches Programm (*Malicious Code*), das sich unter Ausnutzung von Schwachstellen durch Kopieren von einem Rechnersystem oder -netzwerk zum nächsten ausbreitet. Meistens enthält ein Wurm Befehle, die Daten direkt zerstören oder die Systemleistung beeinträchtigen.

Zombie Ferngesteuerter Computer, der typischerweise für konzentrierte Angriffe innerhalb des Internets verwendet wird.

Wir danken den unten aufgeführten Personen und Institutionen für ihr Engagement, das Einbringen ihres Know-hows und die in vielen Stunden gemeinnütziger Arbeit in der Fachgruppe KMU der Stiftung InfoSurance erstellten Primärunterlagen:

Carlos Rieder, Hochschule für Wirtschaft, Luzern (Leiter Fachgruppe KMU bei der Stiftung InfoSurance)

Jürg Altenburger, IBM, Zürich

Christoph Bangerter, E-Mediat AG, Schönbühl

Marcel Beil, Symantec Switzerland AG, Bassersdorf

Herbert Brun, UPAQ Ltd., Küsnacht

Roger Caspar, Bluewin, Zürich

Martin Denz, Verbindung Schweizer Ärztinnen und Ärzte FMH, Bern

Christof Egli, Ernst Basler + Partner AG, Zollikon

Roger Halbheer, Microsoft Schweiz GmbH, Wallisellen

Peter Kunz, Omnisec, Dällikon

Anton Lagger, Bundesamt für wirtschaftliche Landesversorgung, Bern

Peter Neuhaus, Stiftung KMU Schweiz, Bern

Peter Otth, Symantec Switzerland AG, Bassersdorf

Ivo Pfister, Stiftung InfoSurance, Zürich

Marc Vallotton, InfoGuard AG, Zug

Christian Weber, Staatssekretariat für Wirtschaft SECO, Bern

