

Schutz & Sicherheit

Internet-ABC für KMU

Überblick

Zusammenfassung

Die Öffnung der internen Netze durch das Internet weckt bei den meisten KMU Sicherheitsbedenken. Mehr als die Hälfte der KMU nennen ungenügenden Datenschutz und unsichere Zahlungsabwicklung als Hindernisse für den Onlineverkauf. Die Schweizer Unternehmen setzen verschiedene Vorsorgemassnahmen ein. Über 80% haben Antivirenprogramme installiert und sichern ihre Daten periodisch. Das Sicherheitsmanagement ist jedoch ein ganzheitlicher Prozess, der ein Unternehmen vor einem Verlust der Integrität, Vertraulichkeit und Verfügbarkeit von sensiblen Daten schützen kann.

Inhalt

Verbreitung und Bedeutung

- Sicherheitsbedenken
- Vorsorgemassnahmen

Sicherheitsmanagement

- Risiken
- Sicherheitsmanagement
- IT-Strukturanalyse

Wichtige Massnahmen

- Technische Massnahmen
- Organisatorische und personelle Massnahmen

Fallbeispiele

- Netzwerkplan eines Dienstleistungsunternehmens
- Auszug aus einem Nutzungsreglement

Checkliste

Impressum

Schutz & Sicherheit

Internet-ABC für KMU

Verbreitung und Bedeutung

Durch die zunehmende Vernetzung entstehen Risiken für die Datensicherheit und den Datenschutz in einem Unternehmen. Die Offenheit des Internets bietet auch aussenstehenden Dritten die Möglichkeit, das interne Netzwerk anzugreifen oder auf die internen Daten zuzugreifen. Die folgenden Ausführungen zeigen, wie man sich vor solchen Angriffen schützen kann.

Datensicherheit ist das Ergebnis von Datensicherung. Datensicherung umfasst alle Massnahmen zum Schutz der Daten vor Verlust von Vertraulichkeit, Integrität und Verfügbarkeit. Dagegen wird unter Datenschutz der Schutz von personenbezogenen Daten vor unerlaubter Bearbeitung verstanden. Das Bundesgesetz über den Datenschutz konkretisiert die Anforderungen des Datenschutzes:

- Personendaten dürfen nur rechtmässig beschafft werden
- Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein
- Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist

Definition: Datensicherheit und Datenschutz.

Sicherheitsbedenken

Mehr als die Hälfte der KMU nennen Probleme im Datenschutz und der Zahlungsabwicklung als Barrieren für den Onlineverkauf (vgl. Abbildung 1).

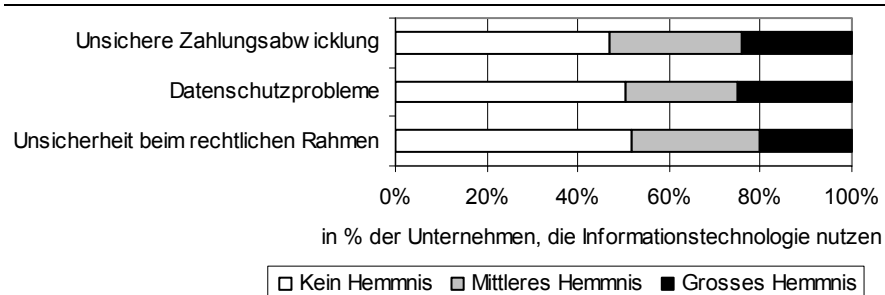


Abbildung 1: Sicherheitsbedenken in Schweizer Unternehmen.¹

¹ KOF (2002).

Schutz & Sicherheit

Internet-ABC für KMU

Vorsorgemassnahmen

Das Bewusstsein über sicherheitsrelevante Probleme zeigt sich auch in den Vorsorgemassnahmen, die von Unternehmen getroffen werden. Die Universität Fribourg untersuchte den Einsatz von technischen und organisatorischen Massnahmen bei Unternehmen zur Sicherstellung der Datensicherheit und des Datenschutzes im Jahr 2002. Knapp 85% der Befragten schützen ihre Daten mit Antivirenprogrammen. Fast gleich viele sichern ihre Daten periodisch. Zwei Drittel der Unternehmen setzen Firewalls ein.

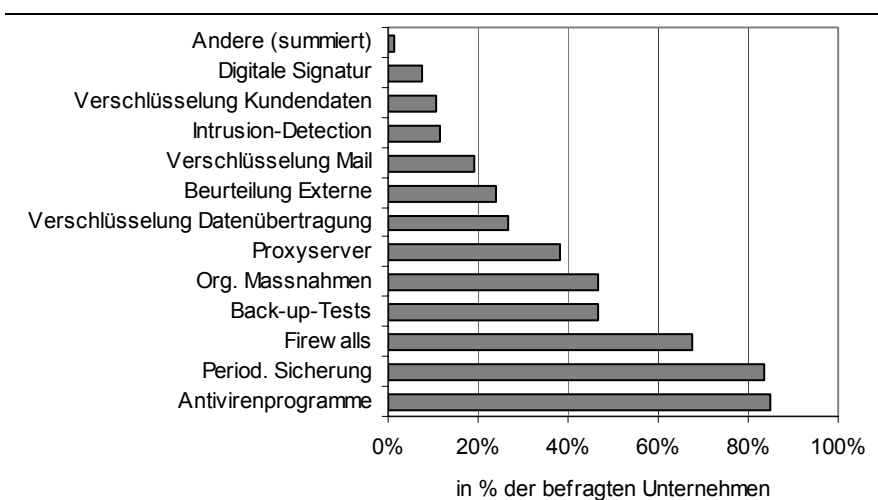


Abbildung 2: Sicherheitsvorkehrungen in Schweizer Unternehmen.²

Eine Untersuchung an der Fachhochschule Winterthur zum Thema Sicherheit in KMU zeigte, welche Daten für die KMU schützenswert sind:³ Kundendaten, Personaldaten, dem Datenschutz unterstellte Daten und Buchhaltungsdaten stufen die KMU als sensibel ein. Die am meisten verbreiteten Massnahmen zur Gewährleistung der Datensicherheit sind gemäss dieser Untersuchung Anleitungen zum Back-up (75%) und Richtlinien im Umgang mit E-Mail und Internet (43%). Die KMU testen jedoch das Back-up nur selten, um sicherzustellen, dass sie im Notfall auf die Daten zugreifen können. Über drei Viertel der Unternehmen glauben jedoch kaum an einen Angriff auf ihr System von aussen.

² Universität Fribourg: Internet & Customer Relationship Management, Marktstudie 2002 in Schweizer Unternehmen und Organisationen, Universität Fribourg in Zusammenarbeit mit dem Bundesamt für Statistik in Neuchâtel und KPMG Consulting AG in Zürich, Fribourg 2002.

³ Reisacher, D.: Marktanalyse, Wie sicher ist die IT von KMU? in: KMU Nr. 10, Oktober 2002.

Schutz & Sicherheit

Internet-ABC für KMU

Sicherheitsmanagement

Risiken

Die verstärkte Öffnung durch das Internet bietet aussenstehenden Dritten die Möglichkeit, das interne Netzwerk anzugreifen oder auf die internen Daten zuzugreifen. Die Angriffe auf gespeicherte oder Daten erfolgen während der Übertragung. Es gibt drei Folgen von Angriffen auf gespeicherte Daten:

- Verlust oder Verfälschung von Daten
- Ausspähen von Daten
- Eindringen in Systeme

Diese Gefahren werden durch Viren oder Hackerangriffe ausgelöst.

Bei den Angriffen auf Daten im Übertragungsprozess unterscheidet man passive und aktive Angriffe. Passive Angriffe beschränken sich auf die Überwachung der Kommunikation zwischen zwei Partnern. Aktive Angriffe richten sich gegen die Integrität und Verfügbarkeit. Sie sind verbunden mit der Veränderung der Daten oder der Erzeugung falscher Datenflüsse.

Angriffe durch Viren oder durch Hacker können die Datensicherheit und den Datenschutz beeinträchtigen. Dabei werden die Daten folgenden Risiken ausgesetzt:

- Unbefugte oder zufällige Vernichtung
- Technischer Fehler
- Fälschung, Diebstahl oder widerrechtliche Verwendung
- Unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen

Sicherheitsmanagement

Zur Gewährleistung der Datensicherheit und des Datenschutzes gelten folgende Anforderungen an das Sicherheitsmanagement:

- Integrität: Die Daten sind konsistent und korrekt.
- Vertraulichkeit: Vertraulichkeit ist gegeben, wenn die Daten nur durch autorisierte Personen eingesehen werden können.
- Verfügbarkeit: Die Verfügbarkeit ist gewährleistet, wenn die Funktionalität der Anwendungen nicht beeinträchtigt wurde.

Eine solide Ausgangslage für die Sicherstellung der drei Anforderungen bietet der IT-Sicherheitsprozess (vgl. Abbildung 3). Dieser beginnt mit der Analyse der IT-Architektur in einem Unternehmen. Die technischen und organisatorischen Massnahmen, die in einem Sicherheitskonzept festgehalten werden, bauen auf den Ergebnissen der Analyse auf. Je nach Resultat sind unterschiedliche Massnahmen geeignet, um den Datenschutz und die Datensicherheit zu gewährleisten. Die Umsetzung der Massnahmen und die laufende Kontrolle halten die Sicherheit aufrecht.

Schutz & Sicherheit

Internet-ABC für KMU

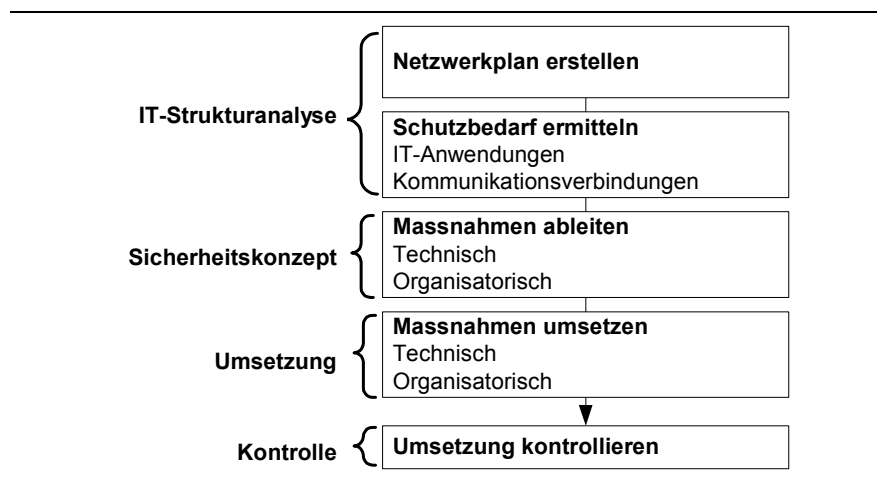


Abbildung 3: IT-Sicherheitsprozess.⁴

IT-Strukturanalyse

1. Erstellen eines Netzwerkplans

Voraussetzung des Sicherheitskonzepts ist eine Situationsaufnahme der aktuell eingesetzten Informationstechnik im Unternehmen. In einem Netzwerkplan werden die IT-Systeme, die Anwendungen, die Netzverbindungen zwischen ihnen sowie die Verbindungen nach aussen aufgezeichnet. Eine Liste detailliert den Netzwerkplan mit Angaben zu den einzelnen Komponenten wie Status des Systems, Betriebssystem, Hardware-Architektur, Typ und Funktion.

2. Ermitteln des Schutzbedarfs

Zunächst wird der Schutzbedarf für die IT-Anwendungen ermittelt. Daraus abgeleitet wird der Schutzbedarf für die Kommunikationsverbindungen.

Für jede Anwendung wird das Sicherheitsniveau in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit festgelegt. Dieser Schutzbedarf orientiert sich an potenziellen Schäden, die mit einer Beeinträchtigung des betroffenen Systems verbunden sind. Die Schutzkategorien können individuell festgelegt werden: Ein niedriger bis mittlerer Schutzbedarf ist angebracht bei Schadensauswirkungen in begrenztem Ausmass. Hoher Schutzbedarf besteht für Daten, bei denen eine Schadensauswirkung beträchtlich ist. Ein sehr hoher Schutzbedarf besteht für Daten, deren Schädigung das weitere Überleben des Unternehmens bedrohen.

Die Schadensfolgen lassen sich in folgende Kategorien einteilen:

- Verstoss gegen Gesetze/Vorschriften/Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Finanzielle Auswirkungen

⁴ In Anlehnung an: Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch, Bonn 2002.

Schutz & Sicherheit

Internet-ABC für KMU

Mit der Fragestellung „Was wäre, wenn...?“ lassen sich die maximalen Schäden ermitteln. Die Ergebnisse werden in einer Tabelle dokumentiert (vgl. Tabelle 1).

IT-System	Anforderung	Schutzbedarf	Begründung
Datenbank mit Personaldaten	Vertraulichkeit	Sehr hoch	Bei Veröffentlichung der Personaldaten wird das Datenschutzgesetz verletzt.
	Integrität	Mittel	Unkorrekte Datensätze können rasch rekonstruiert werden.
	Verfügbarkeit	Mittel	Ein Ausfall hat keine geschäftskritischen Folgen.

Tabelle 1: Beispiel für den Schutzbedarf von Personaldaten.

Zur Ermittlung des Schutzbedarfs von Kommunikationsverbindungen werden folgende Kriterien beurteilt.

- Handelt es sich um eine Aussenverbindung?
- Werden über die Verbindung hochschützenswerte Daten übermittelt?
- Führen die Verbindungen von und zu kritischen Anwendungen?

Alle Kommunikationsverbindungen, für die mindestens eine der drei Fragen mit Ja beantwortet wird, sind als kritische Verbindung identifiziert. Im Netzplan werden die schützenswerten Anwendungen und Kommunikationsverbindungen gekennzeichnet. Je nach ermitteltem Schutzbedarf können die im folgenden Abschnitt vorgestellten technischen und organisatorischen Massnahmen eingesetzt werden, um das Risiko eines Verlustes der Vertraulichkeit, Integrität und Verfügbarkeit zu reduzieren.

Schutz & Sicherheit

Internet-ABC für KMU

Wichtige Massnahmen

Die folgenden technischen und organisatorischen Massnahmen reduzieren die grössten Risiken.

Technische Massnahmen

Installation eines Virenschutzes

Ein Virus ist ein kleines Programm oder ein Skript, welches beim Öffnen bestimmte Funktionen auf einem fremden Rechner ausführen kann. Ausgelöst wird eine Aktion durch die Personen auf deren System sich das Virus installiert hat. Zu unterscheiden sind Würmer, welche nur die Aufgabe der Vermehrung haben. Aber auch diese können zu massiven Schäden an den IT-Systemen führen oder einzelne Services zeitweise lahm legen. Eine gefährliche Art sind die Trojanischen Pferde: Ein unbefugter Dritter sendet ein Programm auf einen Rechner. Dieses Programm ermöglicht der Drittperson, ohne das Wissen des Eigentümers in dessen System einzudringen. Solche Fälle können sowohl die Vertraulichkeit als auch die Integrität und die Verfügbarkeit von Informationen massiv verletzen.

Mit einfachsten Methoden kann einem grossen Teil der Viren bereits entgegengewirkt werden:

- Installation: Installation einer Antivirensoftware eines namhaften Herstellers
- Aktualisierung: Regelmässige Installation der neusten Updates der Antivirensoftware und der Anwendungssoftware
- Filter: Typische Dateien automatisch herausfiltern (z.B. .pif-Dateien). Im Zweifelsfall das Attachment nicht öffnen und sich beim Absender erkundigen, was das Attachment enthält.
- E-Mail-Programm: Das automatische Anzeigen der Nachrichten und Öffnen von Programmen in Anhängen deaktivieren

Einrichten einer Firewall

Im Gegensatz zum Virus bedingt ein Hackerangriff auf ein fremdes System eine aktive Handlung der unberechtigten Drittperson. Auch solche Risiken gefährden die Vertraulichkeit, Integrität und Verfügbarkeit von Daten.

Bei Firewalls handelt es sich um Systeme, die bekannte Netzwerke gegenüber unbekanntem Netzwerken schützen. Sie verhindern damit den externen Zugriff durch nichtberechtigte Benutzer auf die internen Systeme und Daten. Ist ein Betrieb über eine ADSL-Leitung an das Internet angeschlossen, so verfügt er über eine fix zugeteilte Rechneradresse (IP) und ist damit für alle anderen Internetbenutzer eindeutig identifizierbar. Dieser Umstand verlangt bereits einen einfachen Schutz durch eine Firewall. Sobald jedoch aus mehreren Filialen auf die zentrale Kundendatenbank zugegriffen wird, genügt eine einfache Firewall nicht mehr. Hier muss das Netzwerk in verschiedene Sicherheitszonen (sog. Demilitarisierte Zonen, DMZ) unterteilt und mit mehreren Firewalls gesichert werden.

Schutz & Sicherheit

Internet-ABC für KMU

Installation einer Back-up-Lösung

Damit die auf dem Rechner gespeicherten Daten nach einem Verlust oder einer absichtlichen Zerstörung wieder hergestellt werden können (Restore), müssen sie vorgängig gesichert worden sein (Back-up). Diesen Prozess unterstützt eine Back-up-Lösung. In den meisten Fällen wird ein spezielles Tapelaufwerk mit Sicherungsbändern eingesetzt. Ist keine solche Lösung vorhanden, so ist die Verfügbarkeit nach einem Verlust akut gefährdet. Mit folgenden Schritten kann eine einfachere Back-up-Lösung aufgesetzt werden:

- Installieren: Das Laufwerk am Computer oder Netz anschliessen
- Testen: Einen Sicherungslauf durchspielen und Daten wieder herstellen
- Häufigkeit: Tägliche Sicherung mit je einem unterschiedlichen Tape pro Tag
- Ablageort: Die Tapes auf keinen Fall im selben Raum/Gebäude aufbewahren

Organisatorische und personelle Massnahmen

Unternehmenskultur

Die raffiniertesten technischen Lösungen und Richtlinien nützen nur wenig, wenn die Mitarbeiter/-innen die technischen Hilfsmittel nicht mit der nötigen Zuverlässigkeit und Sorgfalt einsetzen. Dabei ist wichtig, dass die Vorgesetzten das Geforderte auch entsprechend vorleben. Der Direktor muss ebenso über die Verhaltensregeln informiert sein wie sein Assistent. Damit steigen das Sicherheitsbewusstsein und die Akzeptanz von technischen und organisatorischen Massnahmen.

Schulung

Zur Sensibilisierung der Mitarbeiter/-innen und zur Förderung der Sicherheitskultur dienen Schulungen: Der Umgang mit ICT im Unternehmen muss bei Stellenantritt instruiert werden. Dies kann in Einzel- oder Gruppenschulungen erfolgen. Wichtig ist dabei, dass die Mitarbeiter/-innen den Sinn der Richtlinien und Gesetze verstehen und diese bei der täglichen Arbeit korrekt anwenden können.

Richtlinien

Die eindeutig formulierten Richtlinien zum Umgang mit ICT stellen ein wichtiges Instrument der internen Sicherheitsstrategie dar. Die Mitarbeiter/-innen erhalten dadurch einen Leitfaden für den täglichen Gebrauch der ICT, und dem Management ermöglichen sie die wirksame Überprüfung des Gebrauchs. Die Richtlinien werden von den Mitarbeiter/-innen bei Stellenantritt unterzeichnet. Sie decken mindestens folgende Punkte ab:

- Bestimmung der Aufbauorganisation und Verantwortlichkeiten
- Regelung der Einarbeitung/Schulung neuer Mitarbeiter/-innen
- Vereinbarung über Einhaltung der Richtlinien sowie der allgemein gültigen Gesetze und Verordnungen
- Rechte und Pflichten der Mitarbeiter/-innen beim Einsatz von ICT (z.B. Umgang mit Passwörtern)
- Sanktionen bei Zuwiderhandlungen
- Rechte und Pflichten der Unternehmung / der Vorgesetzten
- Regelung beim Ausscheiden von Mitarbeiter/-innen

Schutz & Sicherheit

Internet-ABC für KMU

Verhaltensregeln/Meldeprozess

- Stellt ein Mitarbeitender eine Unregelmässigkeit fest oder vermutet Lücken im Sicherheitskonzept, muss ihm bewusst sein, wie er sich zu verhalten hat. Folgende Schritte ermöglichen eine rasche Behebung des Problems:
- Klassifizieren der Situation
 - Verlust
 - Verfälschung
 - Unterbrechung
 - Ausspähen
 - Eindringen
- Sofort den Vorgesetzten informieren (auch bei Selbstverschulden)
- Keine weiteren Programme mehr ausführen
- Netzwerkanschluss unterbrechen

Überwachen der Mitarbeiter/-innen

Bei eindeutigen Verdachtsmomenten kann der Arbeitgeber das Verhalten der Mitarbeiter/-innen überwachen. Da dieser Prozess aber einen Eingriff in die Privatsphäre der überwachten Personen darstellt, müssen sie im Vorfeld über die Überwachung informiert werden. Der Ablaufprozess ist in Abbildung 4 beschrieben:

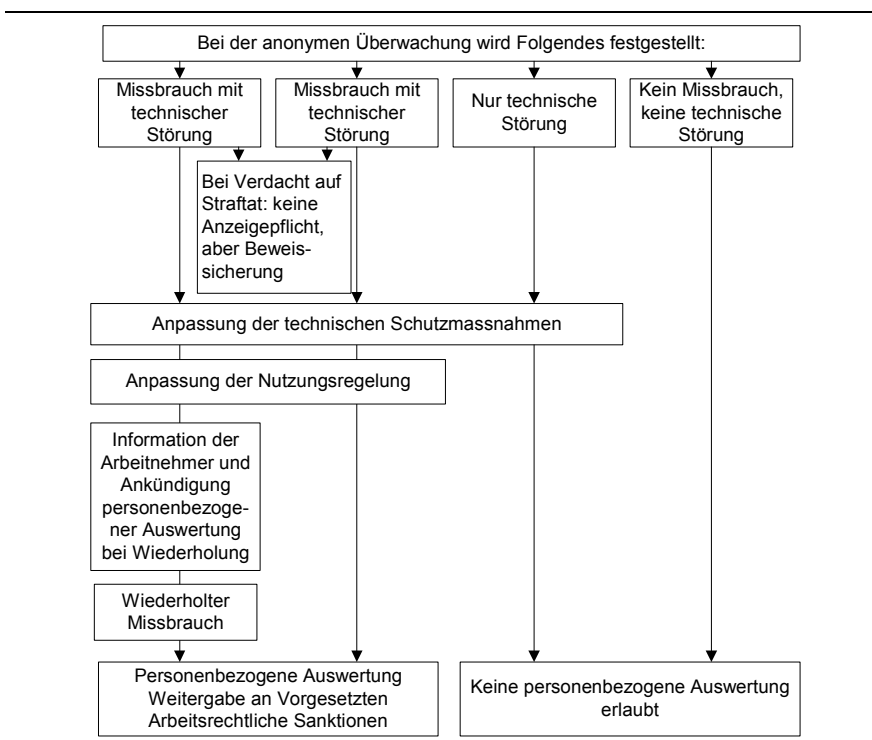


Abbildung 4: Ablauf der Internet- und E-Mail-Überwachung.⁵

⁵ In Anlehnung an: IT-Grundschutzhandbuch.

Schutz & Sicherheit

Internet-ABC für KMU

Fallbeispiele

Netzwerkplan eines Dienstleistungsunternehmens

Ausgangslage:

- 7 Mitarbeiter/-innen, alle haben einen Computer mit Zugang zum Internet
- Mailserver und Server der Website werden extern gehostet
- Datensicherung mit Back-up-Tapes
- 2 Datenserver
- Alle Bildschirmarbeitsplätze sind vernetzt
- Alle Daten sind auf einem Server abgelegt

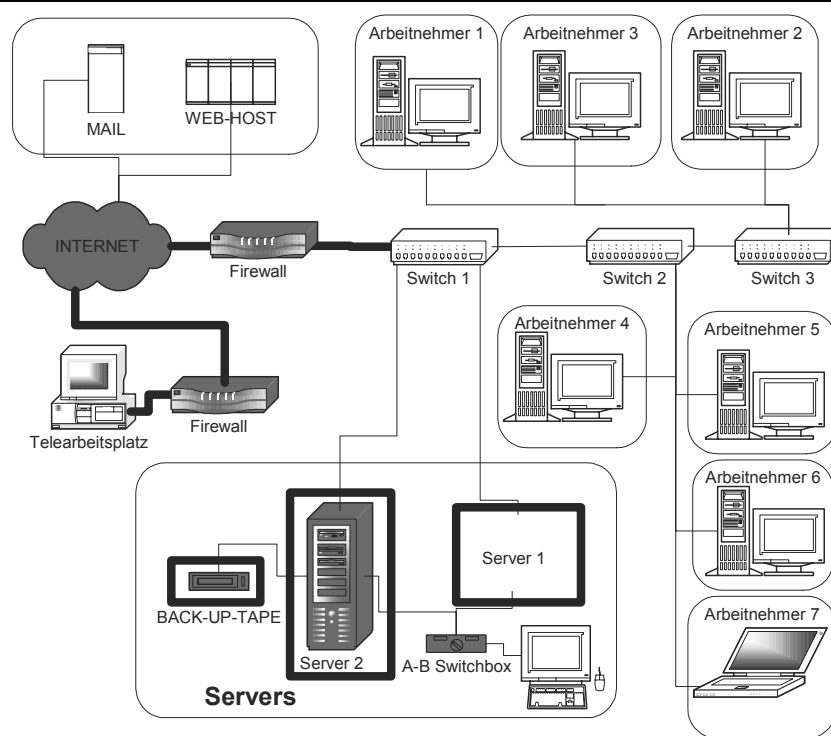


Abbildung 5: Beispiel eines Netzwerkplans.⁶

Ermittlung des Schutzbedarfs am Beispiel des Datenservers 1:

Vertraulichkeit:	Hoch	Die Personaldaten und Kundendaten auf dem Server sind sensible Daten.
Integrität:	Hoch	Die Kundendaten und Personaldaten können nicht wieder hergestellt werden.
Verfügbarkeit:	Hoch	Ohne die Daten steht der Betrieb im Unternehmen still.

⁶ Internet & Customer Relationship Management, Marktstudie 2002 in Schweizer Unternehmen und Organisationen, Universität Fribourg in Zusammenarbeit mit dem Bundesamt für Statistik in Neuchâtel und KPMG Consulting AG in Zürich.

Schutz & Sicherheit

Internet-ABC für KMU

Auszug aus einem Nutzungsreglement

Pflichten der Mitarbeiter/-innen:

- Die Nutzung der E-Mail ist auch für private Zwecke erlaubt.
- Die Nutzung weiterer Dienste im Internet wird einem Mitarbeitenden auch freigeschaltet. Das Downloaden von Dateien aus dem Internet ist grundsätzlich verboten.
- Es ist verboten, sich informativ oder kommunikativ mit Anbietern zu beschäftigen, die menschenverachtende, pädophile oder sexistische Themen anbieten.
- Die Weitergabe von eigenen Benutzererkennungen und sonstigen Authentifizierungsmitteln für eine Benutzung durch Dritte ist unzulässig.
- Das Installieren von privater Hard- und Software ist verboten.
- Sensible Daten dürfen nur verschlüsselt über das Internet übermittelt werden.
- Alle sicherheitsrelevanten Ereignisse sind sofort an die Informatikabteilung zu melden.

Aufzeichnung:

- Jeder Datenverkehr zwischen dem lokalen Netz und dem Internet wird aufgezeichnet. Die Protokolle werden mindestens ein Jahr aufbewahrt und bei Verdacht auf ein Sicherheitsproblem ausgewertet.
- Unsere Firma verzichtet auf den Einsatz von Programmen, die die systematische und dauerhafte Erfassung sämtlicher Aktivitäten am vernetzten Computer erfassen.

Sanktionen:

- Verstöße gegen diese Benutzerrichtlinien können dienst- und arbeitsrechtliche sowie strafrechtliche Konsequenzen haben. Sie können auch Grund für fristlose Kündigung sein.
- Bei Verletzung der Voraussetzungen und Regeln zur Überwachung der Internet- und E-Mail-Aktivitäten stehen dem betroffenen Arbeitnehmer die zivilrechtlichen Ansprüche wegen Persönlichkeitsverletzung zu.

Schutz & Sicherheit

Internet-ABC für KMU

Checkliste

IT-Strukturanalyse

- Erstellen Sie einen Netzwerkplan.
- Erstellen Sie eine detaillierte Liste aller eingesetzten IT-Systeme.
- Erstellen Sie eine detaillierte Liste aller eingesetzten Anwendungen.
- Ermitteln Sie den Schutzbedarf der IT-Systeme, Anwendungen und Verbindungen.

Technische Massnahmen

Datensicherung

- Arbeiten Sie ein Datensicherungskonzept aus.
- Legen Sie die Häufigkeit der Datensicherung fest.
- Trennen Sie den Datenträger mit den gesicherten Daten örtlich von Ihrem Büro.
- Testen Sie die Wiederherstellung der Daten.

Virenschutz

- Installieren Sie ein Virenschutzprogramm eines namhaften Herstellers.
- Führen Sie die Virenupdates jeweils bei Aufforderung durch die Software aus.

Organisatorische Massnahmen

Nutzungsreglement

- Formulieren Sie ein Nutzungsreglement.
- Legen Sie darin Regeln für die private Nutzung des Internets fest.
- Legen Sie darin die Sanktionsmöglichkeiten fest.
- Stellen Sie sicher, dass jeder neue Mitarbeitende das Nutzungsreglement erhält und unterschreibt.
- Stellen Sie in Schulungen sicher, dass das Nutzungsreglement verstanden wird.
- Halten Sie im Nutzungsreglement fest, wie Sie mit Personendaten der Mitarbeiter/-innen umgehen.
- Weisen Sie Ihre Mitarbeiter/-innen auf die Wirkung von unvorsichtigem Umgang mit dem Internet und mit der E-Mail hin.

Zugriffskontrolle

- Verwenden Sie pro Benutzer ein persönliches Passwort.
- Die Passwörter müssen in regelmässigen Abständen gewechselt werden.
- Die Passwörter dürfen nicht einfach zu erraten sein. Geburtsdatum, Name etc. sind nicht geeignet.
- Die Passwörter dürfen nicht abgespeichert oder auf einem Zettel am Arbeitsplatz aufgeschrieben werden.

Impressum

Internet-ABC für KMU



Alle Themen im Internet-ABC für KMU

- Schutz & Sicherheit
- E-Mail-Nutzung
- Informationsbeschaffung
- Internetanschluss
- Internetinfrastruktur
- Internetauftritt
- E-Collaboration
- Marketing & Verkauf
- Werbung im Internet
- Wirtschaftlichkeit
- Angebote der öffentlichen Hand
- Glossar

Herausgeber:

Staatssekretariat für Wirtschaft (seco), Task Force KMU,
Effingerstrasse 31, 3003 Bern.

Autoren:

Adrian Tschanz, Nicole Scheidegger, Peter Rügsegger, Pascal Sieber,
Dr. Pascal Sieber & Partners AG, Laupenstrasse 1, 3008 Bern.

Herkunft der verwendeten Daten:

Die Daten zur Beschreibung der Verbreitung der in diesem Dokument beschriebenen Phänomene wurden vom Bundesamt für Statistik (BfS) zur Verfügung gestellt:

„Die Verbreitung von Informations- und Kommunikationstechnologien sowie E-Commerce in der Schweizer Wirtschaft, 2002.“

Die Datenerhebung sowie die Datenauswertungen für diesen Bericht wurden von der Konjunkturforschungsstelle der ETH Zürich (KOF) durchgeführt.

Verkaufspreis:

kostenlos

Lieferung:

Im PDF-Format

Bezug:

Staatssekretariat für Wirtschaft (seco),
Effingerstrasse 31, 3003 Bern.
<http://www.kmuinfo.ch/>

Wiedergabe von Beiträgen und Abbildungen, auch auszugsweise oder in Ausschnitten, nur mit Erlaubnis des Herausgebers und mit Quellenverweis.

Bern, September 2003

www.kmuinfo.ch

Damit aus Ideen Unternehmen werden
Task Force KMU