BPX.

43


# Cyber-Sicherheit im 21. Jahrhundert

## Sicherheitskonzepte und praktische Umsetzung für KMU

**Andreas Wisler**

goSecurity
EXPERTEN FÜR IHRE IT-SICHERHEIT

www.bpx.ch

BPX.


**Andreas Wisler**

# Cyber-Sicherheit im 21. Jahrhundert

## Sicherheitskonzepte und praktische Umsetzung für KMU

BPX-Edition
Rheinfelden/Schweiz

BPX

BPX Best Practice Xperts
E-Mail edition@bpx.ch
Internet www.bpx.ch

Andreas Wisler

# Cyber-Security im 21. Jahrhundert

## Sicherheitskonzepte und praktische Umsetzung für KMU

Rheinfelden/Schweiz
BPX-Edition 2018
ISBN 978-3-905413-58-8



Herstellung: BPX-Edition, Rheinfelden/Schweiz

Druck und Verarbeitung: Galledia AG, Flawil

## Inhalt

# 1 Management Summary

Praktisch jeden Tag kann von Cyber-Angriffen gelesen werden: «Tausende Zugangsdaten gestohlen und im Internet verfügbar.» Auch die gefundenen Schwachstellen in diversen Programmen haben einen neuen Höchstwert erreicht.

Der Hauptzweck für ein Unternehmen ist, dass die Informationen zur richtigen Zeit, in der richtigen Qualität, am richtigen Ort und der richtigen Person zur Verfügung stehen.

Daher ist es wichtig, dass die Informationssicherheit heute zuoberst auf der Prioritätenliste weitsichtiger KMU-Führungskräfte steht. In allen Betrieben spielt Information eine entscheidende Rolle, und diese gilt es zu schützen.

Die Angriffsszenarien auf der anderen Seite werden immer ausgefeilter. Viele davon zielen auf den Faktor Mensch ab. Nur gut ausgebildetes und sensibilisiertes Personal kann die wichtigen Informationen sicher handhaben. Von nicht ausgebildetem Personal richtige Entscheidungen zu erwarten, ist sinnlos. Vier wichtige Punkte sollen besonders hervorgehoben werden:

- Informationssicherheit (IS) ist eine Managementaufgabe.
- Ein Vorsorgeplan (BCM) hilft im Worst Case zu überleben.
- Für IS und deren Unterhalt muss Budget bereitgestellt werden.
- Zuverlässiges Personal gibt es nur mit Ausbildung.

Kleinere KMU haben meist die personellen Ressourcen nicht, um einen eigenen Chief Information Security Officer (CISO) einzustellen. In diesen Fällen ist es sinnvoll, die Aufgaben an ein spezialisiertes Unternehmen auszulagern. Doch auch beim Outsourcing von IS bleibt die Verantwortung bei der Unternehmensführung.

Gelebte IS bringt auch eine Reihe von Vorteilen, z.B.:

## BPX. Management Summary

- Das Vertrauen der Kunden steigt.
- Die Angriffsfläche für Hacker wird kleiner.
- Mit Vorausdenken lässt sich viel Geld sparen.
- Gut ausgebildetes Personal unterstützt Sie.
- Ihr Unternehmen ist für den Notfall vorbereitet und kann überleben.

In diesem Booklet erfahren Sie,

- worauf bei der Entwicklung von Informationssicherheit zu achten ist,
- wie die Gesetzeslage aussieht,
- welche Standards Ihnen helfen,
- wo die heutigen Gefahren liegen,
- wie Sie Risiken in den Griff bekommen können und
- welche Technologien Ihnen zur Verfügung stehen.

Die Anforderungen an und die Abhängigkeit von der IT nehmen immer mehr zu. Auch die Komplexität hat stark zugenommen, viele Projekte stehen zudem unter grossem Zeitdruck. Auf der anderen Seite nehmen die Gefahren und Risiken ebenfalls rapid zu. Das organisierte Verbrechen hat längstens den Weg ins Internet gefunden und verdient viel Geld mit Angriffen, Erpressungen, Spam und Malware. Daher ist es essenziell wichtig, sich mit den Bedrohungen auseinanderzusetzen und entsprechende Massnahmen proaktiv zu ergreifen. Dieses Booklet soll Ihnen einen Überblick und Ideen dazu bieten.

*Andreas Wisler*

# 2 Managementverantwortung

Die Geschäftsleitung hat die Verpflichtung, Massnahmen zur Gewährleistung von Informationssicherheit im Unternehmen umzusetzen. Folgende gesetzliche Bestimmungen enthalten Forderungen dazu:

- Buchführungsvorschriften: Buchführungsrecht, Obligationenrecht mit Kontrolle des internen Kontrollsystems inklusive Risikobeurteilung
- Aufbewahrungspflicht: Normalerweise 10 Jahre. Diese Zeitspanne kann je nach Branche und zwecks Beweispflicht auch länger sein.
- Öffentlich-rechtliche Vorschriften, z.B. bezüglich Auskunftspflicht, Berufsgeheimnissen usw.
- Strafrecht, z.B. unbefugtes Eindringen in ein Datenverarbeitungssystem oder Datenbeschädigung kann nur geahndet werden bei Nachweis von speziellen Schutzmassnahmen.
- Aktienrecht: Es definiert die Organhaftung von Verwaltungsrat und Geschäftsleitung. Sie kann bis zur Haftung mit dem persönlichen Eigentum gehen.
- Vertragsrecht: Gewährleistung der angebotenen Leistungen, Schadenersatz
- Branchenspezifische Rechtsvorschriften: beispielsweise in der Pharmabranche, bei Banken, Versicherungen, im Gesundheitswesen oder in der Nahrungsmittelverarbeitung
- Datenschutzgesetz: Gesetz über den Schutz von Personendaten; inklusive Datenaustausch mit Drittstaaten
- Persönlichkeitsrecht: Überwachung, Genugtuung, Schadenersatz

Die Durchsetzung von Compliance mit bestehenden Gesetzen liegt in der Verantwortung des Verwaltungsrats und der Geschäftsleitung. Der Einsatz heutiger Informationssicherheits-Management-Systeme erleichtert und unterstützt diese Aufgabe wesentlich.

Gesetze sind aber nicht der Hauptgrund zum Einsatz von Sicherheitsmassnahmen. Diese verlangen mehrheitlich Elemente, die sowieso für jedes Unter-

nehmen wichtig sind – oder zur Vermeidung von grösserem Schaden führen.

## 2.1 Managed Security Services

Vergibt ein Unternehmen Teile seiner Informationsverarbeitung an ein externes Unternehmen, dann müssen zusätzliche Kriterien beachtet werden. Wichtige Punkte dabei sind:

- Die Verantwortung bleibt beim Auftraggeber.
- Überprüfbare Service Level Agreements (SLA)
- Gemeinsames Sicherheitskonzept
- Einhaltung der Lizenzbedingungen
- Umsetzung branchenspezifischer Vorschriften
- Datenschutzgesetze, v.a. bei grenzüberschreitenden Transaktionen

Um die wichtigste Ressource in heutigen Unternehmen zu sichern, ist es unabdingbar, dass das oberste Management sich diese Aufgabe weit oben auf die Prioritätenliste setzt. Mitarbeitende richten sich automatisch auf die Vorgaben der Geschäftsleitung aus. Fehlen diese Vorgaben oder haben sie eine niedrige Priorität, dann kann nicht von IS gesprochen werden.

Beispiel: Bekommt ein Mitarbeiter den Auftrag, mit dem Passwort des Chefs die Verträge kurz auszudrucken, zu denen er mit seinem Passwort keinen Zugriff hat, dann zeugt das zwar von grossem Vertrauen seitens des Chefs, vermutlich werden auch die weiteren Sicherheitsvorschriften nur als lästiges Übel empfunden. Anstatt die Verträge der Geschäftspartnerin verschlüsselt zuzustellen, werden diese unverschlüsselt übertragen. Erfahrungsgemäss wird dies von anderen Mitarbeitenden in Kürze nachgeahmt werden. Damit verlieren Aufwendungen für die Informationssicherheit an Wert.

Oft ist es noch schlimmer, da man sich der Gewissheit hingibt, «wir tun ja etwas für die Informationssicherheit», z.B. durch regelmässige Back-ups. Da diese aber nie auf korrekte Funktionsweise überprüft wurden und oft auch nicht in feuersicheren Behältern ausserhalb des Betriebes lagern, kann ein vollständi-

ger Restore (Wiederherstellung) nicht garantiert werden.

Dazu kommt, dass gerade grössere Schäden dort vorkommen, wo das Personal denkt: «Das kann bei uns nie passieren.»

> Locker gehandhabte Informationssicherheit aufgrund fehlenden Managementsupports ist schlimmer als keine!

## 2.2 Begrifflichkeiten

Die **IT-Sicherheit** bezeichnet die technischen Elemente. Damit sind klassisch Antivirenlösungen, Firewalls, Back-up etc. gemeint. In Medien wird dieser Begriff bevorzugt verwendet, da er sehr kurz ist und alle sich etwas darunter vorstellen können.

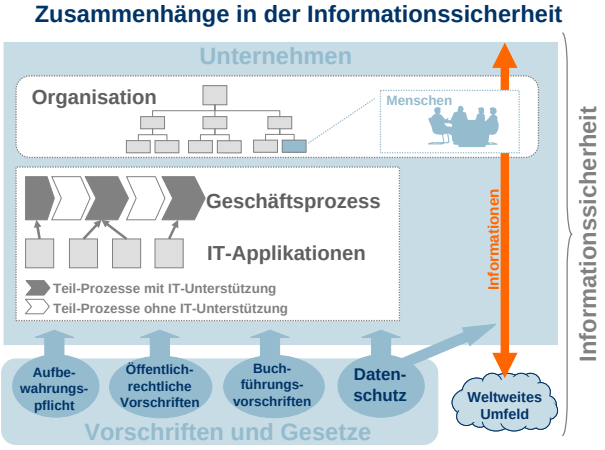


Abbildung 1: Zusammenhänge in der Informationssicherheit

**Informationssicherheit** bezeichnet den Schutz von Informationen, dies in jeglicher Form, egal ob auf Papier oder in Systemen gespeichert. Die drei klassischen Schutzziele **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** werden dazu gezählt. Weiter gehört die immer wichtiger werdende Nichtabstreitbarkeit in diese Kategorie. Mit der Informationssicherheit sollen Risiken minimiert und dadurch der Schutz vor Gefahren oder Bedrohungen erhöht werden.


Abbildung 2: Grundbausteine der Informationssicherheit

Mit **Cyber-Sicherheit** soll gezeigt werden, dass es sich nicht nur um meine eigene Firma oder Umgebung handelt, sondern die Gesamtheit damit gemeint ist. Alles ist heute miteinander verbunden, Anwendungen und Prozesse sind abhängig von anderen. Die Sicherheit kann nicht mehr isoliert betrachtet werden, sondern weitet sich auch auf Infrastrukturen wie Stromversorgung und Telekommunikation aus.

Die Abhängigkeit von ICT steigt an. Informationen werden zunehmend businesskritischer. Diese Abhängigkeiten können Sie mit geeigneten Massnahmen reduzieren.

## 2.3 Rechtliche Aspekte

### 2.3.1 Strafgesetz

Straftaten erfolgen immer mehr auch im elektronischen Bereich. Im Schweizerischen Strafgesetzbuch (StGB) sind einige Artikel vorhanden, die gegen Computerkriminalität zielen:

- Unbefugte Datenbeschaffung (StGB Art. 143)
- Unbefugtes Eindringen in ein Datenverarbeitungssystem (StGB Art. 143bis)
- Datenbeschädigung (StGB Art. 144bis)
- Betrügerischer Missbrauch einer Datenverarbeitungsanlage (StGB Art. 147)
- Herstellen und Inverkehrbringen von Materialien zur unbefugten Entschlüsselung codierter Angebote (StGB Art. 150bis)

### 2.3.2 Datenschutzgesetz

Das Datenschutzgesetz – kurz DSG – bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden. Es gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch Private und Bundesorgane.

Gebote zur Einhaltung des Schutzes der Privatsphäre:

- Daten dürfen nur rechtmässig beschafft werden (Art. 4 Abs. 1 DSG), d.h. bei der Beschaffung dürfen die Personen, welche Informationen geben sollen, weder irregeführt noch unter Druck gesetzt werden.
- Die Bearbeitung muss sich, gemessen am Bearbeitungszweck, auf die Daten beschränken, die geeignet und erforderlich sind (Art. 4 Abs. 2 DSG), um einen bestimmten, legitimen Bearbeitungszweck zu erreichen. Dies ist das Prinzip der Verhältnismässigkeit.
- Daten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG).
- Wer Daten bearbeitet, hat dafür zu sorgen, dass die Informationen korrekt sind (Art. 5 DSG). Korrekt sind sie dann, wenn sie nicht nur inhaltlich richtig, sondern auch aktuell und entsprechend dem Bearbeitungszweck vollständig sind.
- Die Bekanntgabe von besonders schützenswerten Daten und Persönlichkeitsprofilen ist nur mit Einwilligung der betroffenen Person gestattet (Art. 12 Abs. 2 lit.a DSG).
- Daten dürfen nur in Länder transferiert werden, in denen ein gleichwertiger Datenschutz gewährleistet ist (Art. 6 Abs. 1 DSG).
- Daten müssen durch angemessene technische oder organisatorische Massnahmen gegen unbefugtes Bearbeiten gesichert werden (Art. 7 DSG).
- Den Betroffenen ist Einsicht in ihre Daten zu gewähren (Art. 8ff DSG).

Hinweis: Beim Zeitpunkt der Erstellung dieses Booklets war das DSG gerade in Überarbeitung. Das Ziel der Überarbeitung ist die Anpassung an die EU-Datenschutzgrundverordnung (DSGVO), die ein adäquates Schutzniveau zur Europäischen Union bietet

und den Datenaustausch unter den angeschlossenen Mitgliedern erleichtert.

### 2.3.3 Internes Kontrollsystem IKS

Das Obligationenrecht fordert mit dem Artikel 728a die Umsetzung eines internen Kontrollsystems.

Das IKS ist ein Managementinstrument zur zweckmässigen Sicherstellung von Unternehmenszielen in den Bereichen «Prozesse», «Informationen», «Vermögensschutz» und «Compliance». Das IKS umfasst alle dafür von der Geschäftsleitung planmässig angeordneten organisatorischen Methoden und Massnahmen.

## 2.4 Organisatorische IS-Massnahmen

Folgende organisatorische Punkte sollten in jedem KMU realisiert sein:

- Aktuelle und regelmässig überprüfte Sicherheitsprozesse sind eingeführt.
- Für die wichtigen Informationsbereiche sind Richtlinien erstellt.
- Es existiert ein rollen- oder gruppenbasiertes Zugriffskonzept.
- Die Benutzerkonten werden bei personellen Veränderungen nachgeführt / gelöscht.
- Die Mitarbeiter sind auf IS geschult (Awareness).
- Eine Risikoanalyse wird regelmässig durchgeführt und beurteilt (evtl. ergänzt mit einer Business Impact Analyse BIA).
- Angepasste Sicherheitsmassnahmen sind umgesetzt.
- Für die geschäftskritischen Prozesse existiert ein Betriebshandbuch.
- Es wurde ein Notfall- oder Katastrophen-Vorsorgeplan erstellt, der regelmässig getestet wird.
- Neue Software und Patches werden zeitnah installiert.
- Gesetzliche Auflagen werden periodisch auf Einhaltung überprüft (Beachtung auch von ausländischen Gesetzen).

# 3 Grundschutz für KMU

In der Praxis hat es sich bewährt, auf einen guten Grundschutz zu achten, d.h. alle Geschäftsprozesse werden unabhängig von ihrer Risikoeinstufung möglichst gut gesichert. Ist das Unternehmen speziellen Risiken ausgesetzt, dann sind eine spezifische Risiko-Analyse und darauf basierend erhöhte Sicherheitsmassnahmen unumgänglich.

Um die Entwicklung von Sicherheitskonzepten zu vereinfachen, wurden Standards (Normen) geschaffen. Nachfolgend eine Übersicht über die meist angewandten:

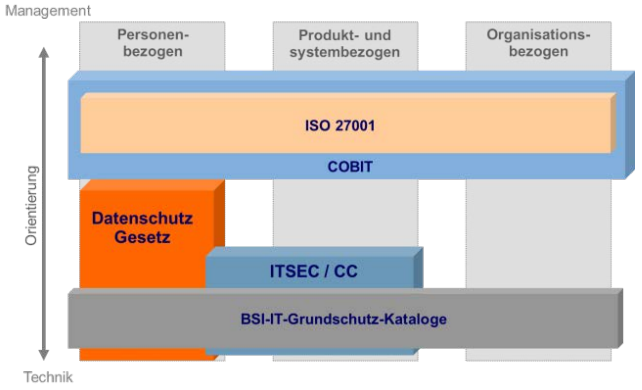


Abbildung 3: Übersicht über die Rahmenwerke in IS: OP, Cobit, BSI Grundschutz-Kataloge, ITSEC / CC, DSG

In Europa ist ISO 27001 am bekanntesten. Zur Abdeckung des Grundschutzes in der IT wird auf die BSI-Grundschutz-Kataloge (neu: Kompendium) abgestützt. Bei Hard- und Software wird oft ein Nachweis nach Common Criteria gefordert. Jede Firma in der Schweiz untersteht dem Datenschutzgesetz. Meldepflichtig sind Datenbanken mit sensiblen Personendaten (wie Geburtsdatum, Religion oder Gesundheitsdaten).[1]

[1] Verschiedene Ausbildungsprogramme und Checklisten finden Sie unter www.datenschutz.ch, www.edoeb.admin.ch oder www.bsi-fuer-buerger.de.

## 3.1 Grundschutz nach BSI

Das Deutsche Bundesamt für Sicherheit in der Informationstechnik stellt umfangreiche Informationen kostenlos zur Verfügung. Diese sind als IT-Grundschutz-Kataloge unter www.bsi.de/gshb abrufbar. Sie dienen dazu, einen Grundschutz in der IT zu erstellen. Seit Anfang 2018 werden die Kataloge nach und nach in das Grundschutz-Kompendium überführt.

Es gibt zusätzlich die BSI-Standards zur IT-Sicherheit. Diese Teile decken den Management-Teil (BSI 200-1, Managementsysteme für Informationssicherheit), die Vorgehensweise (BSI 200-2, IT-Grundschutz-Methodik), das Erstellen von Risikoanalysen (BSI 200-3) und das Notfallmanagement (BSI 100-4) ab.

Ein Schweizer Standardwerk zur Informationssicherheit ist das «Sicherheitshandbuch für die Praxis».[2]


Abbildung 4: BSI-Zertifikate sind kompatibel mit ISO 27001.

[2] www.sihb.ch. Dieses Standardwerk wurde explizit für KMU aufgebaut und ist mit Vorlagen, Checklisten und weiteren Tipps ein unerlässliches Hilfsmittel für Sicherheitsverantwortliche.

## 3.2 ISO 27000

Aufgrund der Komplexität der Informationstechnik und der Nachfrage nach Zertifizierungen ist eine Vielzahl von Anleitungen, Standards und nationalen Normen entstanden. Die Norm ISO/IEC 27001 spezifiziert Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Management-Systems (ISMS) unter Berücksichtigung der Risiken. Unternehmen können sich nach diesem Standard zertifizieren lassen.

ISO 27002 definiert ein Rahmenwerk für das IT-Sicherheitsmanagement. Es befasst sich mit den erforderlichen Schritten, um ein funktionierendes IT-Sicherheitsmanagementsystem aufzubauen und gliedert sich in 14 Managementgebiete mit 35 Massnahmenzielen. Darin sind 114 übergeordnete Sicherheitsanforderungen enthalten (baseline controls).

Für KMU weiter von Interesse ist der Standard ISO/IEC 27005, welcher Richtlinien, Tabellen und Beispiele zum IT-Risikomanagement bietet. Es behandelt die Einschätzung, Behandlung, Akzeptanz, Kommunikation und Überwachung / Kontrolle von Risiken.

Auch wenn Sie keine Zertifizierung anstreben, geben Ihnen die einzelnen Kapitel gute Hinweise, woran Sie denken müssen, wenn Sie wirksame Sicherheit für die Informationen umsetzen wollen.

Verfolgen Sie dazu meinen ISO-Blog unter https://andreaswisler.com/blog.

# 4 Praxis der Informationssicherheit

Die Erfahrungen zeigen, dass das Geheimnis hinter effektiver Informationssicherheit darin liegt, dass sich das Management dieser Aufgabe bewusst ist und dass Sicherheitsprozesse eingeführt und gelebt werden. Die Schäden von negativen Ereignissen sind dann am grössten, wenn Unternehmen darauf nicht vorbereitet sind.

## 4.1 Bedrohungsszenarien

Die Bedrohungen, die sich auf ein KMU auswirken können, sind mannigfaltig. Dieses Kapitel gibt eine kurze Übersicht dazu.

**Physische Bedrohungen**

Darunter fallen z.B. Wassereinbrüche, Feuer, Blitzschlag, Sturm, Erdbeben usw. Auch in unserer modernen Welt können solche Ereignisse relativ häufig auftreten.

**Checkliste physische Bedrohungen:**

Wurden folgende Bedrohungen überprüft und die Resultate in die Risikoanalyse integriert? [3]

- Sturm (Dach abdecken)
- Blitzschlag
- Brand
- Unzulässige Temperatur und Luftfeuchtigkeit
- Wasserleitungsbrüche / Hochwasser
- Erdrutsch
- Erdbeben
- Schneelast
- Bäume
- Staub, Verschmutzung
- Stromzuführungen und Kurzschlüsse
- Gasleitungen

[3] Detaillierte Auflistung siehe auch G1 Gefährdungskatalog Höhere Gewalt des BSI: www.bsi.de/gshb/deutsch/g/g01.htm

- Lager von Explosivstoffen
- Anflugschneise Flughafen
- Verfügbarkeit von Transportmitteln
- Ungesicherter Zugang

**Bedrohungen im IT-Bereich**

Entsprechend den geschäftskritischen Prozessen mit IT-Unterstützung müssen hier die Bedrohungen gegen Hardware, Programme und Datenbestände beachtet werden.[4]

- Ausfall von Netzteilen
- Recovery von Back-ups funktioniert nicht
- Keine Patches oder Upgrades installiert
- Nach Upgrades laufen nicht mehr alle Programme.
- Nach Neuinstallation von Betriebssystemen sind bisherige Daten und Einstellungen verschwunden.
- Netzwerkausfälle wegen schlechter Verkabelung
- Passworte sind mehreren Personen bekannt.
- Teile von Datenbeständen werden auf persönliche Computer geladen.
- Installationen und Konfigurationen sind nicht dokumentiert.
- Entwickler installieren und betreiben Applikationen.

**Bedrohungen im Telekommunikationsbereich**

Die Grundlage für das Verständnis der heutigen Bedrohungen im Telekommunikationsbereich beruht auf dem Verständnis der unterschiedlichen Technologien und Geschäftsprozesse.

Malware hat immer noch Hochkonjunktur. Zugenommen haben vor allem Ransomware (Verschlüsseln der Daten und nur gegen Bezahlung eines «Lösegelds» wird der Schlüssel zum Entschlüsseln der Daten herausgegeben), Phishing sowie Botnetze mit dem Ziel von Betriebsspionage, Auslesen von Passwörtern und Kreditkartennummern sowie Identitätsdiebstahl. Die Online-Attacken verlagern sich

[4] Weitere Bedrohungen im IT-Bereich siehe Risikoanalyse vom BSI, Technisches Versagen: www.bsi.de/gshb/deutsch/g/g04.htm

immer mehr vom Stören und Zerstören mit Malware hin zu schädlichem Code in Browserinhalten (via infizierter Webseiten, sogenannter Drive-by). Oft kommt dabei nicht nur ein Mittel zum Einsatz, sondern eine Kombination davon.

Eine immer ernster zu nehmende Gefahr sind zudem ausgehende E-Mails via externe Webmail-Accounts. Da diese E-Mails über den Browser laufen, werden sie von vielen Firewalls nicht erkannt. Dadurch können wichtige Geschäftsgeheimnisse ohne Risiko aus dem Unternehmen herausgebracht werden. Da diese E-Mails auch auf vielfach ungenügend geschützten Servern (im Ausland) lagern, können peinliche Pannen passieren, was auch zu einer Gefährdung des Ansehens führen kann (Verschiedene Geheimdienste beispielsweise filtern schon seit längerer Zeit den gesamten Internetverkehr und verkaufen die Informationen an zahlungskräftige Kunden!). KMU mit sensiblen Daten sollten ihr Personal entsprechend informieren und die Richtlinien anpassen.

Zu immer grösserer Vorsicht ist auch beim Einsatz von Voice-over-IP (VoIP) geraten. Unverschlüsselte Übertragung von Sprachdiensten übers Internet ist für Fachleute einfach abzuhören.

**Bedrohungen bei mobilen Endgeräten**

Grundsätzlich gelten hier auch fast alle Bedrohungen aus dem Bereich der Telekommunikation. Erschwerend kommt dazu, dass sich die Benutzer der Bedrohungen und Schwachstellen ihrer Geräte nicht bewusst sind und oft grosse, sensible Datenbestände mit sich führen.

Die vorhandenen Risiken können durch entsprechende Vorschriften (nur absolut notwendige Daten auf den mobilen Geräten), restriktive Zugriffseinschränkungen, starke Authentifizierung und effektive Verschlüsselung reduziert werden.

Laptops und Mobiltelefone nie sichtbar im Auto zurücklassen! Auf Laptops für Unternehmensarbeiten sollten keine anderen Aktivitäten ausgeführt werden (Gaming, Chatten, Teilnahme an Tauschbörsen usw.).

**Bedrohungen im Identitätsbereich**

Der technische Teil hierzu wurde bereits im Kapitel Bedrohungen im Bereich Telekommunikation beschrieben. Moderne Technologien machen es möglich, die Identität einer Person unbemerkt zu stehlen. Danach sind Tür und Tor offen für Missbräuche. Einkaufen auf Rechnung eines anderen wird noch eine harmlose Nutzung von Identitätsdiebstahl sein. Spionage von Geschäftsgeheimnissen und Patentmissbrauch werden schon gröbere Varianten davon sein.

## 4.2 Risk Assessment / Risk Management

Eine Risiko-Analyse ist für jedes Unternehmen sinnvoll. Dabei gilt es, die möglichen Bedrohungen zu identifizieren und geeignete Massnahmen zu planen. Die folgende Grafik gibt dazu eine Übersicht:

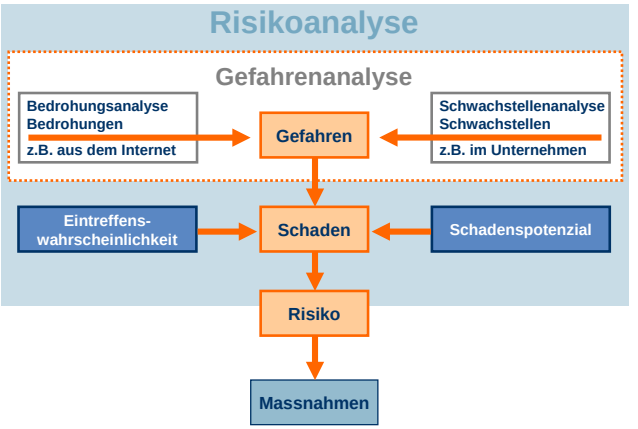


Abbildung 5: Übersicht über Risikoanalysen

Zuerst werden die vorhandenen Bedrohungen aufgelistet und eingestuft (z.B. tief, mittel, hoch), danach die vorhandenen Schwachstellen. Trifft eine Gefähr-

dung auf eine Schwachstelle, dann existiert eine Gefahr. Aus einer Gefahr kann ein Schaden mit einer gewissen Schadenshöhe und mit einer entsprechenden Eintretenswahrscheinlichkeit entstehen. Dies ergibt ein Risiko.

**Wichtige Begriffe:**

Ein **Risiko** ist definiert als eine auf ein spezifisches Objekt bezogene Gefahr, die hinsichtlich Eintretenswahrscheinlichkeit und Schadenausmass bewertet worden ist.

Unter **Gefahr** verstehen wir die mögliche Ursache für ein Schadenereignis; einen Zustand, Umstand oder Vorgang, aus dem ein Schaden für Mensch, Umwelt oder Sachgüter entstehen kann.

Eine **Gefährdung** ist eine auf ein bestimmtes Objekt bezogene Gefahr.

Eine **Bedrohung** ist eine Aktion oder ein Ereignis, das die «Auftragserfüllung» eines Systems verunmöglicht oder behindert.

Eine **Verwundbarkeit** ist eine Schwäche resp. Schwachstelle in Design, Implementation oder Betrieb von Systemen, Sicherheitsverfahren oder (generell) internen Kontrollen, welche für den unberechtigten Zugang zu Informationen, die Störung von kritischen Prozessen oder andere Bedrohungen ausgenützt werden könnte.

Das Erstellen von effektiven Risikoanalysen bedingt viel Wissen und Erfahrung. Dazu bestehen auch verschiedenste Tools. Deren Wert ist aber immer nur so gut, wie die eingegebenen Werte der Realität entsprechen. Schadenshöhe und Eintretenswahrscheinlichkeit sind immer Schätzungen und können im Extremfall weit danebenliegen. Sinnvollerweise wird jeweils eine Tabelle der verschiedenen Risiken erstellt mit den dazugehörigen möglichen Schadenshöhen und den Eintrittswahrscheinlichkeiten.

| Schaden | | [W] Wahrscheinlichkeit ( 0 – 4 ) | [S] Schadenhöhe (0 – 4) | [R] Risiko (W*S) |
|---|---|---|---|---|
| a) Datenverlust | Privatdaten (E-Mails, Fotos, Buchhaltung, ...) | 4 | 2 | 8 |
| | Geschäftsdaten (Adressen, Office-Dateien, Buchhaltung...) | 4 | 3 | 12 |
| b) Fehlende Datenintegrität (Vollständigkeit) | Privatdaten (E-Mails, Fotos, Buchhaltung, ...) | 1 | 1 | 1 |
| | Geschäftsdaten (Adressen, Office-Dateien, Buchhaltung...) | 2 | 3 | 6 |
| c) Einsicht/Preisgabe sensibler Daten (Confidentiality) | Privatdaten (E-Mails, Fotos, Buchhaltung, ...) | 1 | 1 | 1 |
| | Geschäftsdaten (Adressen, Office-Dateien, Buchhaltung...) Geschäftsschädigung | 4 | 4 | 16 |

Abbildung 6: Risikoanalyse

Um die Relationen unter den einzelnen Risiken besser zu sehen und zwecks deren Reduktion Schwerpunkte bei den Massnahmen zu setzen, werden die Risiken anschliessend am besten in eine Grafik eingetragen.

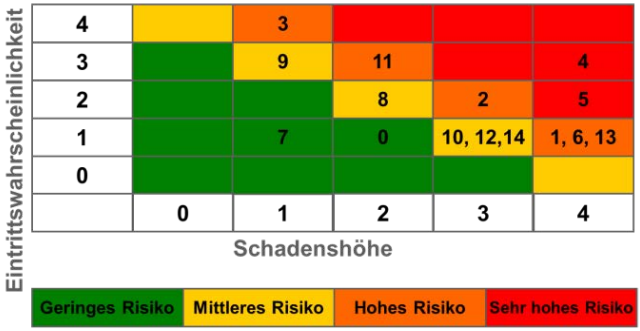


Abbildung 7: Risiko-Übersicht

In dieser Grafik sind die grössten Risiken nun einfach zu erkennen, die Risiken 4 und 5. Zu beachten ist jetzt bei den Entscheidungen für Massnahmen zur Reduktion von Risiken, dass nicht nur die Schadenshöhe reduziert wird, sondern auch die Schadenshäufigkeit.

Neben ISO 27005 gibt der Standard BSI 200-3 weitere Informationen und Überlegungen zum Risiko Management.

### Risiken reduzieren

Mit dem Erstellen einer Risikoanalyse ist ein wichtiger Schritt realisiert. Um nun auch den bestmöglichen Wert aus dieser Arbeit zu ziehen, muss überlegt werden, wie die einzelnen Risiken reduziert werden können. Die grundsätzlichen Möglichkeiten sind in der folgenden Grafik dargestellt.

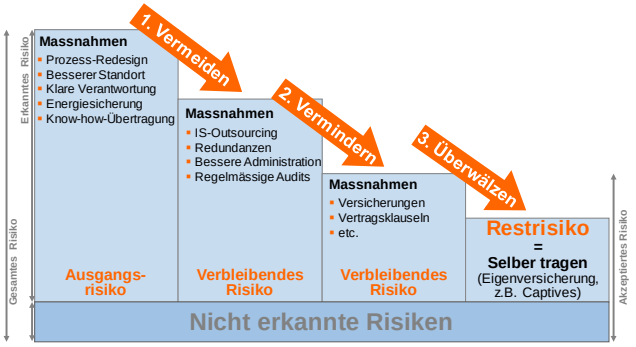


Abbildung 8: Risiko-Analyse

Am meisten Geld wird gespart, wenn sich Risiken vermeiden lassen. Oft ist dies aber mit einer Reduktion der möglichen Aktivitäten verbunden (z.B. bei Prozess-Redesign).

### Risiken managen

Um die Risiken wirklich im Griff zu haben, müssen diese im Wesentlichen auch kontrolliert und regelmässig neu eingeschätzt werden.

Beim Risiko-Management ist wichtig, dass jemand eindeutig der Prozessverantwortliche ist. Da Prozesse, deren Risiken und die angewandten Technologien sich öfters ändern, muss dieser Prozess auch periodisch (mindestens einmal pro Jahr) durchlaufen werden.

## 4.3 Risiko-Minimierung

Durch die nachfolgenden Punkte kann das Risiko bereits im Vorfeld auf ein Minimum reduziert werden.

- Erstellen Sie ein Pflichtenheft für IT-Verantwortliche.
- Sichern Sie Ihre Daten regelmässig mit Backups.
- Halten Sie Ihr Antivirus-Programm aktuell.
- Schützen Sie sich mit einer Firewall.
- Aktualisieren Sie Ihre Software regelmässig.
- Verwenden Sie starke Passwörter.
- Schützen Sie Ihre mobilen Geräte.
- Machen Sie Ihre IT-Benutzerrichtlinien bekannt.
- Schützen Sie die Umgebung Ihrer IT-Infrastruktur.

Je nach Gefährdungspotenzial können noch weitere Punkte dazukommen:

- Erstellen Sie ein Sicherheitskonzept.
- Etablieren Sie einen Risiko-Management-Prozess.
- Stufen Sie Ihre Daten nach Gefährdungspotenzial ein.
- Erstellen Sie ein Verschlüsselungskonzept.
- Sichern Sie die Übertragung Ihrer Daten.
- Bilden Sie die Mitarbeitenden in Informationssicherheit aus.
- Erstellen Sie einen Katastrophen-Vorsorgeplan.
- Schliessen Sie Supportverträge bei geschäftskritischen Prozessen.
- Bei sehr seltenen, aber grossen Risiken kann eine Risikoversicherung zweckmässig sein.

## 4.4 Business Continuity Management

Ein effektives Business Continuity Management (BCM) (zu Deutsch auch Katastrophen-Vorsorgeplan genannt) umfasst alle Planungsarbeiten, um einerseits Katastrophen wo immer möglich zu vermeiden und andererseits das Überleben des Unternehmens im Katastrophenfall zu sichern.

Ein bekannter und bewährter Standard für den Betrieb eines BCM ist die ISO Norm 22301. Unternehmen können sich nach diesem Standard zertifizieren lassen.

Ein BCM muss mindestens folgende Punkte umfassen:

- Erfassen der geschäftskritischen Prozesse
- Inventarisierung der Anlagen
- Identifikation von Schlüsselsystemen und -anwendungen
- Bestimmung der maximal zulässigen Ausfallzeiten
- Ersatzbeschaffungsplan/Ausweichmöglichkeiten
- Wiederanlaufplan und -management
- Eskalationsweg und Reporting
- Krisenorganisation mit Sammelstellen
- Bestimmung der Verantwortlichen mit Stellvertretern
- Datensicherung mit Auslagerung
- Recovery-Tests der Back-ups
- Ausbildungsplan
- Periodische Notfallübungen[5]

## 4.5 Die Bedeutung der Mitarbeiterschulung

Die Informationssicherheit steht und fällt in einem Unternehmen mit der Ausbildung und dem korrekten Verhalten der Mitarbeitenden. Ausbildungsmöglichkeiten existieren auf vielen Ebenen, von produktbezogenen, theoretischen, ausführungsbezogenen Kursen bis hin zu mehrsemestrigen Ausbildungen an diversen Fachhochschulen und Universitäten mit verschiedensten Zertifikaten.

Ohne die Mithilfe und Kooperation der Mitarbeiter kann keine Sicherheit gewährleistet werden. Um die Aufmerksamkeit der Anwender zu erhöhen, eignet sich z.B. folgende 10-Punkte-Checkliste:

[5] Siehe auch E-Book: Der IT-Ernstfall, U. Moser, BPX-Edition ISBN 978-3-905413-23-6 www.bpx.ch

- Sichere Passwörter anwenden (Kombination von Zahlen, kleinen und grossen Buchstaben plus Sonderzeichen, Minimum 10, besser 12 Zeichen)
- Passwörter nicht aufschreiben (sich merken anhand eines Satzes)
- Ordnung halten auf dem Arbeitsplatz (keine sensiblen Dokumente liegen lassen, Stichwort: Clear Desk)
- Keine eigene Software installieren
- Vorsichtiger Umgang mit Attachments und Kurzlinks (E-Mails von Unbekannten löschen, keine Attachments anklicken und keine Links daraus anklicken)
- Antivirenprogramm nie ausschalten
- Phishing-Attacken erkennen
- Keine Auskünfte an unberechtigte Personen erteilen
- Bei seltsamen Vorfällen den Support anrufen

Diese Punkte können z.B. während eines Steh-Lunches anhand von Beispielen erklärt werden. Als Abschluss kann ein Flyer verteilt werden. Ein möglicher Flyer ist dabei www.geschichtenausdeminternet.ch.

Weitere Möglichkeiten sind:

- Schulungen
- Web-Based-Trainings
- Poster
- E-Mails
- Simulierte Phishing-Angriffe
- Videos
- Div. Give-aways
- U.v.m.

# 5 Gefahren

## 5.1 Spam

Mit dem Siegeszug der E-Mails kam auch der Spam. Der Begriff entstammt dem Sketch der englischen Comedyserie Monty Pythons Flying Circus: In einem Café besteht die Speisekarte ausschliesslich aus Gerichten mit SPAM, die «SPAM» teilweise mehrfach hintereinander im Namen enthalten. SPAM ist ein Markenname für Dosenfleisch, 1936 entstanden aus Spiced Ham.


Abbildung 9: SPiced hAM (Quelle: Wikipedia)

Mit Spam ist in der IT-Welt jegliche Art von unerwünschten E-Mails gemeint.

**Verbreitung von Spam**

Wie gelangen aber die Spammer an die eigene E-Mail-Adresse? Hier gibt es diverse Varianten. Eine Quelle sind E-Mail-Adressen auf der Webseite. Analog Google suchen Roboter nach E-Mail-Adressen auf der Webseite oder in Newsforen und Gästebüchern. Diese werden eingelesen und abgespeichert.

Weiter sind Viren und Würmer im Umlauf, die nichts anderes machen, als nach E-Mail-Adressen auf dem eigenen Rechner zu suchen, sei dies nun in einer Datei oder im E-Mail-Programm. So sind natürlich E-Mail-Weiterleitungen mit zum Teil x-Dutzenden Empfängern ein gefundenes Fressen für diese Malware.

Oft wird aber auch die Naivität der Internet-Surfer ausgenutzt. Ein Wettbewerb, eine Bestellung von Software oder sonst etwas Aufregendes wird dazu benutzt, um an die E-Mail-Adresse zu gelangen.

Daher lohnt es sich, das Kleingedruckte zu lesen und nicht blind private Angaben zu geben.

Die letzte Methode ist das automatisierte Durchprobieren von Adressen. So werden Tausende E-Mails verschickt, nur um zu testen, ob eine Fehlermeldung – sprich: E-Mail ist unzustellbar – zurückkommt oder ob die E-Mail zugestellt wird.

**Schutz vor Spam**

Die einfachste Regel ist, die E-Mail-Adresse gleich vertraulich zu behandeln wie die eigene Postadresse oder die Kreditkarten-Angaben. Die E-Mail sollte nur dann angegeben werden, wenn es nicht anders geht.

Analoges gilt auch für E-Mails, die verschickt werden. Es ist eine Unsitte, alle Empfänger ins An-Feld zu schreiben. Verwenden Sie immer das BCC-Feld für solche Weiterleitungen. So ist es für den Empfänger nicht ersichtlich, wer die E-Mail sonst noch erhalten hat. Sollte nur jemand einen Schädling auf seinem Rechner haben, ist nur der letzte Absender ersichtlich.

Schon aus gesetzlichen Gründen gehört eine E-Mail-Adresse im Impressum auf die eigene Webseite. Diese sollte jedoch nicht einfach als normaler Text oder Link platziert werden, sondern verschleiert abgelegt sein.

Eine Möglichkeit dazu ist die Verwendung von JavaScript. Folgendes Beispiel ergibt beim Anklicken die E-Mail empfaenger@domain.ch:

```
<script language="JavaScript">
  var user = "empfaenger"
  var site = "domain.ch"
  document.write('<a href=\"mailto:' + user + '@' +
site + '\">');
  document.write(user + '@' + site + '</a>');
</script>
```

Leider ist auf vielen Seiten die Angabe einer gültigen E-Mail-Adresse Pflicht. Zur Kontrolle wird der Code oder eine Download-Bestätigung an diese Adresse geschickt. Im Internet gibt es aus diesem Grund zahlreiche Einmal-Adress-Dienste. Eine frei definier-

bare E-Mail-Adresse wird gelöst, und sobald die erwartete Nachricht durch ist, wird sie automatisch wieder gelöscht.

Praktisch alle Provider haben inzwischen reagiert und bieten Spam-Filter an. Einfache Filter schauen dabei aber nur, woher die E-Mail kommt. Ist die Absender-Adresse (IP) auf einer schwarzen Liste, wird der Empfang verweigert (sogenannte RBL – Remote Black Lists). Bessere Filter analysieren zusätzlich den Inhalt und versuchen einen Wert zu bestimmen (z.B. Viagra = 10 Punkte). Sobald ein vorher definierter Schwellwert erreicht wird, wird die E-Mail als Spam gekennzeichnet. Diese Technik nennt man Bayes-Filter.

## 5.2 Malware

Malware ist die Abkürzung für Malicious Software. Ein solches Schadprogramm aufzulesen passiert schneller, als oft gedacht wird – sei es durch Würmer (Programme, die sich selber verbreiten und Lücken in Betriebssystemen oder verwendeten Applikationen ausnutzen), Viren (benötigen aktives Dazutun des Benutzers, z.B. Attachment anklicken) oder Trojanische Pferde (Vorgaukeln von falschen Tatsachen). Oft wird die Verteilung dieser Malware auf speziell präparierten Seiten vorgenommen.

Neuere Techniken versuchen, das Viren-Programm so zu verstecken, dass es durch Antivirenscanner und andere Schädlingssucher schon gar nicht erkannt wird. Die Programme werden so versteckt, dass diese für das Betriebssystem nicht sichtbar sind. Rootkit heisst diese Technik. Daher gilt auch weiterhin: Nur das anschauen oder öffnen, was man wirklich will.

Die Gefahr von Viren ist allgegenwärtig. Pro Tag werden ca. 200'000 neue Schädlinge entdeckt. Zudem werden die sich im Umlauf befindlichen Viren immer raffinierter. Daher ist auch in Zukunft ein zuverlässiger und umfassender Virenschutz notwendig. Vergessen Sie nicht, den Virenschutz regelmässig zu aktualisieren!

## 5.3 Botnetze

Eine grosse Gefahr geht heute von Bot-Netzwerken aus. Diese werden immer grösser und komplexer. Oft ist den Anwendern aber gar nicht bewusst, dass der eigene Computer (oder die smarte Lampe an der Decke) als sogenannter Zombie missbraucht wird.

Sobald dann der eigene Rechner unter der Kontrolle von Fremden ist, wird er dazu benutzt, Spam zu verschicken, Angriffe im Internet durchzuführen (sogenannte DDoS-Angriffe) oder als Tarnung für illegale Aktivitäten eingesetzt. Aktuelle Zahlen sprechen von Botnetzen, die mehrere Hunderttausend Rechner beinhalten. Halten Sie deshalb Ihre Rechner immer auf dem aktuellsten Stand!

## 5.4 Mobiler Zugriff

Der mobile Zugriff von unterwegs ist eine beliebte Möglichkeit, noch schnell seine Termine abzugleichen, die neuesten E-Mails zu beantworten oder an einem wichtigen Dokument weiterzuarbeiten. Es ist erstaunlich, wie unachtsam mit den mobilen Geräten umgegangen wird.

Daher ist es angebracht, die Daten auf diesen Maschinen zu schützen. Ein BIOS-Passwort (Passwort beim Starten des Rechners ) oder das Anmelde-Passwort von Windows sind dabei kein effektiver Schutz. Das BIOS-Passwort kann mit einem einfachen Stecker auf dem Motherboard gelöscht werden. Der Schutz von Windows kann mit einem USB-Stick und dem entsprechenden Programm innert Sekunden ausgehebelt werden.

Nur eine Harddisk- oder Datenverschlüsselung hilft, dass die Daten nicht in fremde Hände geraten.

Ein weiterer Punkt, der regelmässig vergessen geht, ist die Aktualität des mobilen Gerätes. Nur wenn Aktualisierungen für das Handy angeboten und rechtzeitig eingespielt werden, kann der Schutz hoch gehalten werden.

## 5.5 Phishing

Die Gefahr von Phishing-Attacken hat massiv zugenommen. Früher waren viele Phishing-Mails schon an der holprigen oder fremden Sprache zu erkennen, heute sind diese korrekt in Deutsch, ja sogar schon in Schweizerdeutsch formuliert. Wichtig ist, nicht willkürlich auf Links zu klicken, sondern sich zuerst klar zu sein, wohin dieser zeigt. Gesunder Menschenverstand und aktuelle Systeme bewahren vor Missbrauch und Manipulation.

## 5.6 Social Engineering

Bevor in ein Netzwerk eingedrungen wird, ist es von Vorteil, viele Informationen über das Unternehmen zu sammeln. Meist nähern sich die Angreifer beim Social Engineering zunächst einem Mitarbeiter in einer untergeordneten Position, etwa der Sekretärin oder der Putzfrau, um Gepflogenheiten und Umgangsformen in Erfahrung zu bringen. Die unter Social Media erwähnten Möglichkeiten bieten eine zusätzliche Informationsquelle. Bei der Annäherung an den eigentlichen Geheimnisträger verschaffen sie ihm dann den Eindruck, dass es sich angesichts der Detailkenntnis bei dem eigentlich Fremden ja keinesfalls um einen Aussenstehenden handeln kann. Und schon sind wichtige Informationen in die falschen Hände gelangt. Seien Sie sich immer sicher, mit wem Sie sprechen oder mit wem Sie gerade telefonieren, bevor Sie Informationen weitergeben. Achten Sie hier besonders auch auf Gespräche zwischen Ihnen und einer vertrauten Person, z.B. im Zug. Hier sind schon viele interessante Gespräche belauscht worden.

## 5.7 Social Media

Soziale Medien erfreuen sich grosser Beliebtheit, sei dies Facebook, Snapchat, Instagram im privaten oder Xing und Linkedin im geschäftlichen Umfeld. Getweeted, gepostet, geliked wird ständig und überall. Vielleicht ist diese Information für sich alleine kein Problem, werden aber die Daten aus verschiedenen Quellen und Diensten miteinander verknüpft, können

plötzlich unangenehme Zusammenhänge entstehen. Daher ist es wichtig darauf zu achten, was veröffentlicht wird. Die Empfehlung ist, die verfügbaren Sicherheitseinstellungen so gut wie möglich zu nutzen und mit Bedacht Neuigkeiten zu veröffentlichen.

## 5.8 Spuren im Netz

Heute hinterlässt jeder Spuren im Netz, ob bewusst oder unbewusst. Viele soziale Dienste, Werbenetzwerke und weitere versuchen die Vorlieben der Benutzenden zu kennen und entsprechende Werbung anzubieten. Es macht wenig Sinn, einem Hundebesitzer Werbung für Katzenfutter anzubieten, das lehnt er ab. Aber das beste Hundefutter, das es je gegeben hat, könnte zum Ziel führen. Im Durchschnitt lädt heute eine Webseite 10 bis 50 weitere Webseiten nach. Oft sind dies auch Google und Facebook. Da auch die Zeit, die ein Benutzer braucht, um eine Seite zu lesen (oder eben nicht zu lesen), gemessen wird, kann schön erkannt werden, was diese Person interessiert oder nicht. Sehr schnell kommen da sehr persönliche Dinge zum Vorschein. Wir werden also auch dann überwacht, wenn wir gar nicht auf der entsprechenden Seite sind.

Das nachfolgende Bild zeigt die vier Zeitschriften Tages-Anzeiger, Blick, NZZ und 20 Minuten. 190 weitere Seiten wurden von diesen im Hintergrund geladen. Aufgezeichnet wurden diese mit dem Firefox Plug-in Lightbeam.

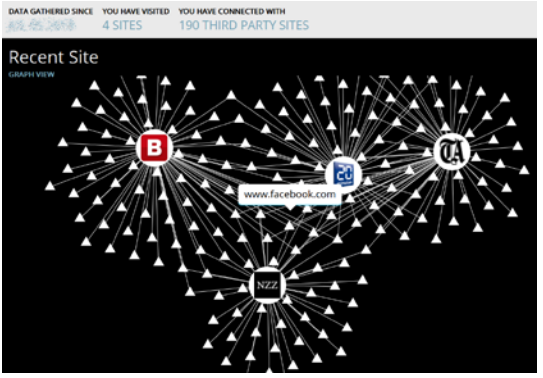


Abbildung 10: Spuren im Netz

# 6 Sicherheitsmassnahmen

Dieses Kapitel beschreibt einige Sicherheitsmassnahmen. Damit ein Verständnis für die Massnahme aufgebaut werden kann, werden auch einige technische Details zu Anwendungen und Protokollen gezeigt.

## 6.1 E-Mail

Als Erfinder der elektronischen Post gilt der Computertechniker Ray Tomlinson. Obwohl es E-Mails seit 1971 gibt und sie eine enorme Wichtigkeit erlangt haben, gilt E-Mail immer noch als unzuverlässiges Übertragungsmedium.

### Aufbau und Protokolle

E-Mails sind intern in zwei Teile geteilt: Den Header mit Kopfzeilen und den Body mit dem eigentlichen Inhalt der Nachricht.

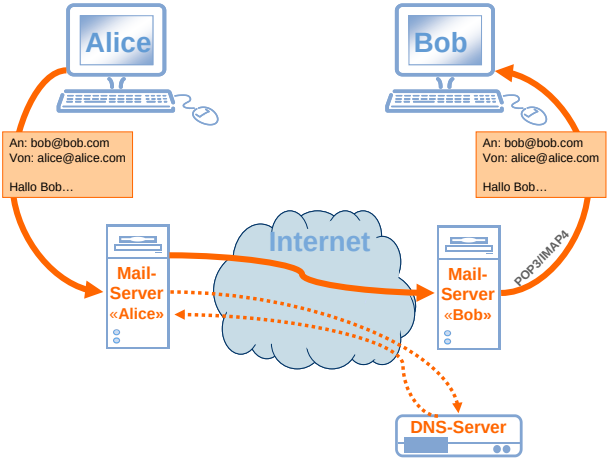


Abbildung 11: E-Mail-Versand

Der Versand von E-Mails erfolgt über das Protokoll SMTP (Simple Mail Transfer Protocol). Es regelt die Sprache der Server. So werden zuerst die Verbindung zum Zielserver aufgebaut und danach Sender und Empfänger mitgeteilt. Im dritten Schritt folgen die Informationen (der Inhalt der E-Mail).

Während SMTP lediglich zum Versenden von E-Mails eingesetzt wird, holen die beiden Protokolle POP3 und IMAP4 die E-Mails auf den lokalen Client.

POP3 (Post Office Protocol Version 3) kennt nur wenige Befehle. Das Ziel ist es, die E-Mails vom Server auf den eigenen Client herunterzuladen und anschliessend vom Server zu löschen.

IMAP4 (Internet Message Access Protocol Version 4) hingegen sieht vor, dass die E-Mails auf dem Server belassen werden und nur der Inhalt zur Bearbeitung auf den lokalen Client heruntergeladen wird.

**Sicherheit**

Alle drei oben beschriebenen Protokolle haben einen grossen Nachteil: Die E-Mails bzw. der Inhalt werden unverschlüsselt übertragen (das heisst in Klartext). Sitzt ein potenzieller Angreifer dazwischen, kann er problemlos alles lesen (sogenannte Man-in-the-Middle-Attacke). Daher wird bei E-Mails oft auch von Postkarte gesprochen, auch diese kann von jeder Person zwischen Sender und Empfänger gelesen werden. (Im Internet sind es die zwischen Empfänger und Sender weiterleitenden Server.) Vertrauliche E-Mails sollten daher NIE unverschlüsselt übertragen werden. Nutzen Sie dazu die Verschlüsselung der E-Mails (nachfolgendes Kapitel) und den verschlüsselten Transport vom und zum Provider.

## 6.2 Verschlüsselung

Verschlüsselung wird der Vorgang genannt, bei dem ein klar lesbarer Text (Klartext, Plaintext) mithilfe eines Verschlüsselungsverfahrens in eine «unleserliche», das heisst nicht einfach interpretierbare Zeichenfolge (Geheimtext, Ciphertext) umgewandelt wird. Als entscheidend wichtiger Parameter der Verschlüsselung wird hierbei ein einzelner Schlüssel bzw. ein Schlüsselpaar (K, Key) verwendet.

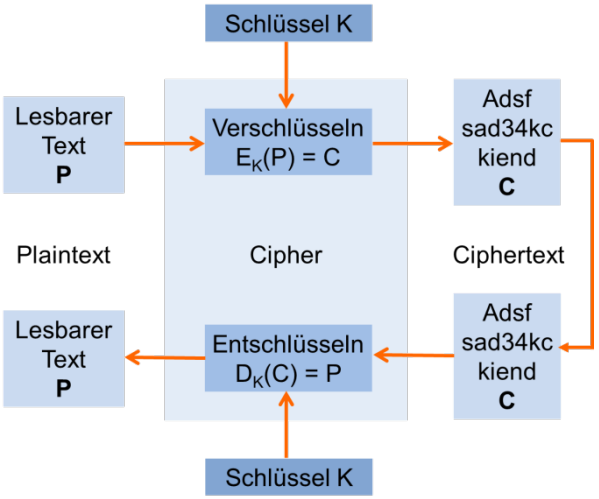


Abbildung 12: Begriffe der Ver- und Entschlüsselung

Diese Arbeit übernehmen Programme. Der Anwender muss sich nur am Rande mit der Verschlüsselung auseinandersetzen. Es stehen zwei Verfahren zur Auswahl: PGP und X.509.

**PGP**

PGP steht für Pretty Good Privacy und wurde 1991 von Phil Zimmermann entwickelt. Die Grundidee war es, Daten sicher zwischen Sender und Empfänger auszutauschen.

PGP basiert auf einer sehr cleveren und schnellen Art der Verschlüsselung. Für den Inhalt der Nachrichten wird ein symmetrisches Verfahren verwendet (Empfänger und Sender verwenden den gleichen Schlüssel). Dies aus dem einfachen Grund, weil symmetrische Verfahren weniger rechenintensiv und damit schneller sind. Damit jedoch die Benutzer dieses geheime Passwort nicht jedes Mal auf einem sicheren Weg (in diesem Fall nicht auch per E-Mail) übermitteln müssen, wird für die Verschlüsselung des Passwortes das asymmetrische Verfahren verwendet (oft auch als Public Key bezeichnet). Dabei besitzt jede Person ein Schlüsselpaar, einen öffentlichen (Public Key) und einen geheimen (Private Key)

Schlüssel. Diese beiden Schlüssel sind mathematisch voneinander abhängig, es ist jedoch nicht möglich (bzw. nur mit einem exorbitanten Aufwand), vom öffentlichen auf den privaten Teil zu gelangen.

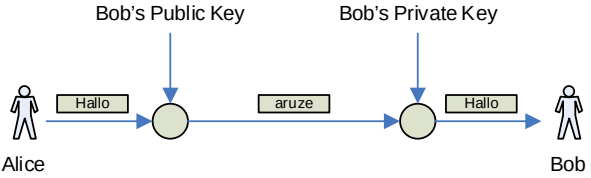


Abbildung 13: Ver- und Entschlüsselung

Zur Verschlüsselung wird jeweils der öffentliche Schlüssel des Empfängers verwendet, entschlüsselt werden kann die Nachricht nur mit dem privaten Schlüssel des Empfängers.

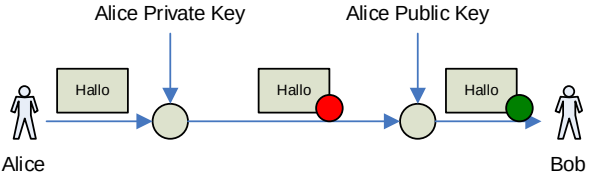


Abbildung 14: Signierung und Verifikation

Damit der Empfänger feststellen kann, dass die E-Mail tatsächlich vom Sender kommt, kann die E-Mail signiert werden (digitales Unterschreiben). Dazu wird der eigene private Schlüssel verwendet. Die Echtheit und Unversehrtheit der E-Mail kann mit dem öffentlichen Schlüssel des Senders überprüft werden.

Die Sicherheit von PGP basiert auf Zertifikaten und dem Web-of-Trust-Verfahren. Die Idee hinter dieser «Technik» ist, dass sich die Benutzer gegenseitig die Echtheit des öffentlichen Schlüssels bestätigen. Dies soll verhindern, dass sich ein fremder Benutzer als eine bekannte Person ausgeben kann.

**X.509**

Einen anderen Weg schlägt X.509 ein. X.509 wurde erstmals 1988 veröffentlicht und setzt ein striktes

hierarchisches System von vertrauenswürdigen Zertifizierungsstellen (engl. certificate authority, kurz CA) voraus, die Zertifikate erteilen können. Dieses Prinzip steht im Gegensatz zum vorher beschriebenen Web-of-Trust-Modell. X.509 kommt übrigens immer dann zum Einsatz, wenn Sie eine verschlüsselte Internetseite besuchen (erkennbar am HTTPS). Die gleiche Grundlage wird auch für die Verschlüsselung von E-Mails verwendet.

Im Internet finden sich zahlreiche Zertifizierungsstellen, die solche Zertifikate ausstellen. Die eigene Identität muss dabei mit einem Ausweis bestätigt werden. Sobald dies geschehen ist, übernimmt die ausstellende Stelle die Garantie, dass die Person wirklich die Person ist, auf welche das Zertifikat lautet. Für diesen Service wird ein jährlicher Betrag verlangt. Die Zertifikate sind dementsprechend auch nur ein bis drei Jahre gültig und müssen dann erneuert werden (im Gegensatz zu PGP, wo Zertifikate «unendlich» lange gültig sind). Der grosse Vorteil liegt aber darin, dass ich mich nicht um die Kontrolle der Person kümmern muss, sondern mich «blind» auf diese Unternehmen verlassen kann.

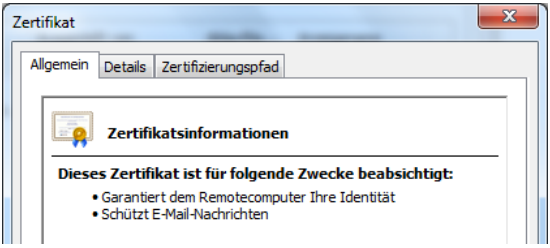


Abbildung 15: Zertifikat

Nun stellt sich die Frage, wieso ich diversen Zertifizierungsstellen blind vertraue. Die Antwort liegt im eigenen Computer. Als Grundvoreinstellung sind diverse Stellen bereits als vertrauenswürdig eingestuft. Sie gelangen im Internet-Explorer via Extras – Internetoptionen – Inhalte – Zertifikate – Vertrauenswürdige Stammzertifizierungsstellen zur Antwort.

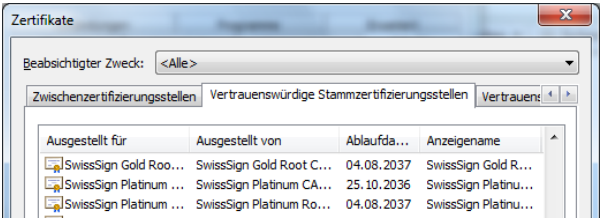


Abbildung 16: Vertrauenswürdige Zertifikate

## 6.3 Netzwerksicherheit

Neben den Clients ist auch der Schutz des gesamten Netzwerkes ein wichtiges Thema. Netzwerksicherheit ist dabei kein einzelner feststehender Begriff, sondern umfasst alle Massnahmen zur Planung, Ausführung und Überwachung der Sicherheit in Netzwerken. Diese Massnahmen sind keinesfalls nur technischer Natur, sondern beinhalten auch organisatorische Fragestellungen (z.B. Richtlinien, in denen geregelt wird, was die Betreiber des Netzwerkes dürfen sollen), betriebliche Fragestellungen (wie kann ich Sicherheit im Netzwerk in der Praxis anwenden, ohne gleichzeitig den Ablauf des Betriebs zu stören?) und enden nicht zuletzt mit rechtlichen Fragestellungen (was für Massnahmen dürfen eingesetzt werden?).

Das Thema Sicherheit beginnt mit der Frage, wie ein Netz gegen den Zugriff von aussen geschützt werden kann (z.B. mittels einer Firewall). Anwender können die Ressourcen des Netzwerks erst nach einer Identifizierung und einer anschliessenden Authentifizierung und Autorisierung nutzen. Damit eine Kompromittierung eines Rechners im Netzwerk erkannt werden kann, werden Rechner oft überwacht (Stichwort Intrusion Detection System, IDS). Potenzieller Datenverlust durch fehlerhafte Software, Fehlbedienung, Fahrlässigkeit oder Altersverschleiss der Hardware wird durch eine Datensicherung verhindert (Stichwort Back-up). Sicherheitslücken in der Software können durch das rechtzeitige Einspielen von Software-Updates geschlossen werden. Nicht freigegebene Software kann (und sollte) verboten werden. Durch Schulung der Anwender kann ein Si-

cherheitsbedürfnis oder Problembewusstsein entstehen und dabei das Verständnis geweckt werden, dass die Daten eines Netzwerkes sehr wertvoll sind. Dadurch soll der Anwender Verständnis für die Massnahmen aufbringen und diese nicht unterlaufen, indem er komplizierte Passwörter auf Zettelchen schreibt und diese an seinen Monitor klebt. Schliesslich kann der physische Zugang zum Netzwerk selbst noch mithilfe von Zugangskontrollen beschränkt werden.

## 6.4 Firewall

Das Ziel einer Firewall ist, den Datenverkehr zwischen Netzen mit verschiedenen Vertrauensstufen abzusichern. Ein typischer Einsatzzweck besteht darin, den Übergang zwischen einem lokalen Netzwerk (LAN) und dem Internet (kein Vertrauen) zu kontrollieren. Oft wird auch von einer dritten Zone als DMZ (demilitarisierte Zone oder auch Perimeter-Zone genannt) gesprochen. Hier werden die vom Internet erreichbaren Server platziert.

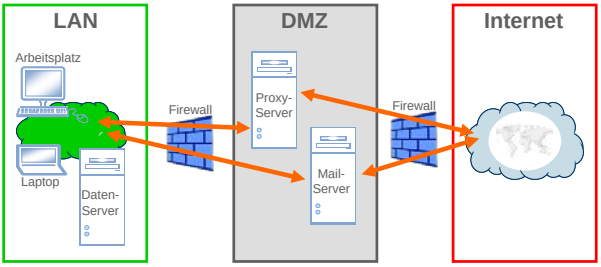


Abbildung 17: DMZ zwischen Firewalls

Die Softwarekomponente einer Firewall arbeitet auf den Schichten 2 bis 7 des OSI-Referenzmodells. Das heisst, je höher die Schicht, umso mehr Dienste kann die Firewall anbieten. Nachfolgend sind die wichtigsten Arbeiten einer Firewall kurz beschrieben:

- Paketfilter: Die einfache Filterung von Datenpaketen anhand von Zielport, Quell- und Zieladresse.
- Stateful Inspection ist eine erweiterte Form der Paketfilterung. Die zustandsgesteuerte Filterung merkt sich den Status einer Verbindung und kann einem zusam-

menhängenden logischen Datenstrom ein neues Datenpaket zuordnen. Diese Information kann als weiteres Filterkriterium herangezogen werden.

- Eine Application-Layer-Firewall beachtet zusätzlich zu den reinen Verkehrsdaten auch noch den Inhalt der Netzwerk-Pakete. Deshalb kann die Firewall mithilfe eines Content-Filters die Nutzdaten auswerten oder nicht erwünschte Anwendungsprotokolle blockieren.
- Content-Filter dienen dem Herausfiltern von ActiveX und/oder JavaScript aus angeforderten HTML-Seiten, Filtern von vertraulichen Firmeninformationen, Sperren von unerwünschten Webseiten anhand von Schlüsselwörtern und Blockieren von Malware in Webseiten und E-Mails.
- Web Application Firewalls untersuchen den HTML-Verkehr zusätzlich auf bekannte Angriffsmuster wie SQL Injection, XSS, Session Hijacking u.v.m.

### Firewall-Regeln

Im Regelwerk einer Netzwerk-Firewall wird definiert, welcher Verkehr erlaubt und welcher verboten ist. Die Regeln werden für jede Verbindung der Reihe nach geprüft, und die erste zutreffende Regel wird angewendet.

Eine Firewall-Regel setzt sich aus sechs Komponenten zusammen:

- Absender-IP-Adresse (auch Netzwerk-Adressen wie z.B. 192.168.0.0/24)
- Ziel-IP-Adresse
- Netzwerkprotokoll (TCP, UDP, ICMP, ...)
- Port-Nummer (bei TCP und UDP)
- Aktion (erlauben, verwerfen oder ablehnen)
- Loggen ja/nein

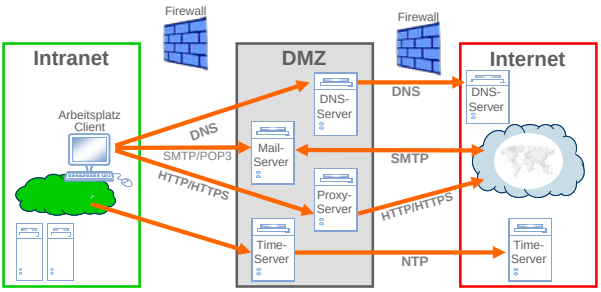

Abbildung 18: DMZ, Internet, Intranet

## 6.5 Personal Firewall

Eine Personal Firewall wird auf dem eigenen Rechner installiert und überwacht sämtliche Netzwerkverbindungen. Sie schützt den PC vor ungewollten ein- und ausgehenden Verbindungen.

Der Vorteil von Personal Firewalls liegt sicherlich im Schutz des eigenen PCs. Sie verhindern jeden Zugriff auf den Rechner, ausser er wurde speziell erlaubt. Dies ist aber auch der Nachteil: In einem Netzwerk kann nicht mehr einfach so auf den Rechner zugegriffen werden, auch nicht für Supportzwecke durch den Administrator.

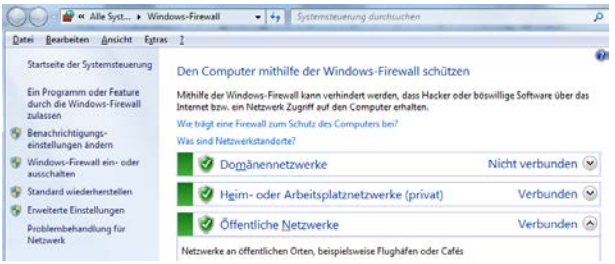


Abbildung 19: Windows-Firewall

Microsoft hat seit Windows XP Service Pack 2 eine einfache Personal Firewall eingebaut. Sie verhinderte Zugriffe von aussen, filterte jedoch nichts vom Rechner ins Netzwerk. Mit Einführung von Windows Vista filtert die Firewall in beide Richtungen. Seit Windows 7 ist eine zusätzliche Desktop-Firewall nicht mehr notwendig. Vorteil dieser Lösung ist, dass die Firewall via die zentrale Steuerung des Active Directories eingestellt werden kann (via Gruppenrichtlinien).

Auch bei einem Gerät von Apple gilt es die Firewall zu aktivieren. Standardmässig ist sie es nicht.

## 6.6 Intrusion Detection

Intrusion Detection System (IDS) überwacht und protokolliert den gesamten Datenverkehr des Netzwerkes in Echtzeit. Es erlaubt, Unregelmässigkeiten

zu erkennen und abzuwehren, und unterstützt somit eine Firewall.

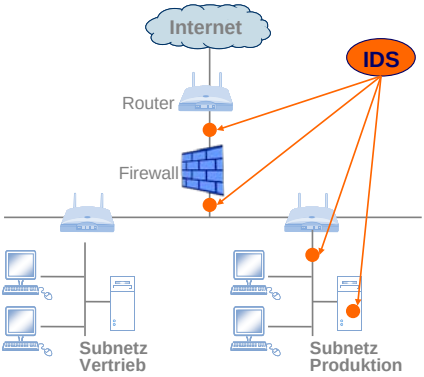


Abbildung 20: Intrusion Detection System

Die Konfiguration ist aber mit grossem Aufwand verbunden. Installiert ist ein IDS schnell, bis es aber korrekt läuft, braucht es einiges an Wissen, Erfahrung und Geduld.

**Netzwerküberwachung, Alarmierung**

Die Überwachung und Alarmierung stellt ein wichtiges Instrument zur Kontrolle des Netzwerkes dar. Es stehen dabei sehr viele kommerzielle, aber auch kostenlose Programme zur Auswahl.

Die Alarmierung kann zum Beispiel per E-Mail oder SMS erfolgen. Als Variablen können die Systeme mit den ausgewählten Diensten sowie der Tag und die Zeit verändert werden. So ist eine bis aufs letzte Detail angepasste Alarmierung möglich. Zusätzlich stehen im Internet Dutzende von Erweiterungen zur Auswahl. So ist es möglich, die USV zu überwachen, SQL-Server auf Herz und Nieren zu kontrollieren usw.

**Logfile-Kontrolle**

Ein oft mühsames Thema ist die Kontrolle der anfallenden Daten(-Berge). Niemand wälzt sich gerne durch die vielen Zeilen. Doch genau hier liegt ein enormes Potenzial, Fehler frühzeitig zu erkennen und notwendige Massnahmen einzuleiten. Es muss ein

täglicher Job für sehr wichtige Systeme und ein wöchentlicher für alle anderen Server und Dienste sein, sich mit den Logs auseinanderzusetzen. Für den Administrator muss dies ein Bestandteil seiner Pflichten sein und darf auf keinen Fall infolge anderer «wichtigerer» Arbeiten verschoben werden. Unterstützung bekommt der Administrator durch SIEM-Anwendungen (Security Incident & Event Management), welche Daten automatisch aus- und bewerten können.

## 6.7 Patchen

Allmonatlich erscheint von verschiedenen Herstellern die Aufforderung, die neuesten Patches (Software-Aktualisierungen) einzuspielen. Praktisch für jede Software erscheinen in unregelmässigen Abständen Aktualisierungen, die es gilt zu installieren. Statistiken zeigen auf, dass neue Schwachstellen immer schneller ausgenutzt werden. Inzwischen sind wir bei Attacken angelangt, die schon am gleichen Tag Lücken ausnutzen, die gerade erst veröffentlicht wurden. Auf einen Patch zu verzichten, ist daher ein gefährliches Spiel mit dem Feuer. Es bleibt der dringende Rat, Patches möglichst schnell nach Bekanntmachung zu installieren.

## 6.8 Back-up/Restore

Das Back-up ist die Lebensversicherung für die eigenen Daten. Passiert ein Zwischenfall – zum Beispiel der Ausfall einer Harddisk, ein Brand oder ein versehentliches Löschen von Daten – kann schnell und einfach wieder auf diese Daten zugegriffen werden. Erstaunlich ist, dass gerade bei vielen Heimbenutzern und kleineren Firmen dies nicht gemacht wird! **Dies ist ein grob fahrlässiges Versäumnis.**

### Welche Daten müssen gesichert werden?

Als Erstes stellt sich die Frage, was überhaupt gesichert werden soll und muss. Dies global zu beantworten, ist praktisch nicht möglich. Zu unterschiedlich sind die Anforderungen. Daher gilt es vor dem Einsatz eines Back-up-Systems zu überlegen,

welche Daten für das Überleben der Firma notwendig sind. Nicht zu vergessen sind die portablen Geräte wie Smartphones, USB-Sticks, Laptops usw. Anschliessend müssen die verschiedenen Abteilungen und Personen für ihren Bereich angeben, auf welche Daten sie in welcher Zeit wieder zugreifen müssen. Mit diesen Angaben kann anschliessend mit der Planung des Back-ups begonnen werden.

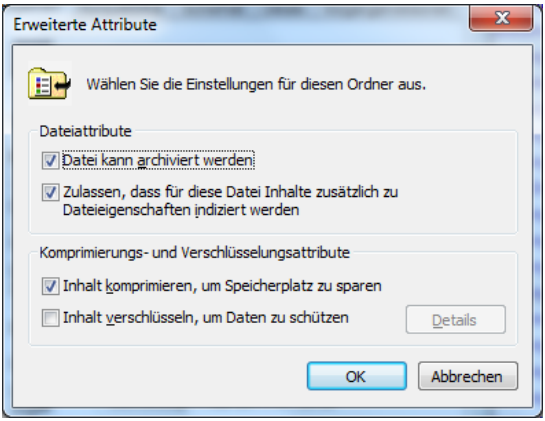


Abbildung 21: Attribute

Back-up-Systeme orientieren sich bei der Datensicherung am Archiv-Attribut der einzelnen Dateien. Das Erstellen oder Ändern einer Datei bewirkt, dass diese Datei mit einem aktivierten Archiv-Attribut versehen wird. Ein aktiviertes Archiv-Attribut signalisiert, dass diese Datei gesichert werden sollte. Je nach Sicherungstyp wird nach der Datensicherung bei den gesicherten Dateien dieses Archivattribut deaktiviert.

### Arten des Back-ups

Die Durchführung des Back-ups kann auf verschiedene Arten erfolgen:

- Beim **Full-Back-up** werden immer alle markierten Daten gesichert.
- Beim **differenziellen Back-up** werden alle Veränderungen seit dem letzten Full-Back-up gesichert.

- Beim **inkrementellen Back-up** werden nur die Daten gesichert, die seit dem letzten Back-up verändert wurden.
- Bei der **Synchronisation** werden die Daten an zwei Standorten immer auf dem gleichen Stand gehalten.

**Lagerung der Datenträger**

Die Sicherungsmedien gehören zwingend an einen anderen Ort. Deponieren Sie diese zum Beispiel in einem Banksafe oder zumindest in einem anderen Brandabschnitt.

**Wiederherstellung von Daten**

Einzelne Dateien wiederherzustellen, gehört für Administratoren fast schon zu den täglichen Arbeiten. Sehr schnell ist eine Datei absichtlich oder unabsichtlich gelöscht und muss von den Sicherungsbändern zurückgeholt werden. Ob dabei auch in einem Notfall schnell auf die Daten zurückgegriffen werden kann, ist aber meistens nicht bekannt. In regelmässigen Abständen, mindestens nach einer Anpassung des Back-up-Plans, muss ein Desaster-Recovery (d.h. eine vollständige Wiederherstellung) durchgeführt werden.

**Kontrollen**

Mit dem Durchführen des Back-ups alleine ist es jedoch nicht getan. Nach jeder Sicherung sollte das Ergebnis kontrolliert werden. Meistens genügt ein Blick in die Log-Datei des entsprechenden Programms. Wurden alle Daten gesichert? Sind Störungen aufgetreten (Daten gesperrt, zu wenig Platz auf dem eingelegten Medium oder Ähnliches)? Wie sieht der Zustand des Bandes aus? Welches Medium muss als Nächstes eingelegt werden? Dies sind Fragen, die jeden Tag beantwortet werden müssen.

## 6.9 Cloud

Das Thema Cloud ist u.a. deshalb sehr populär, weil man IT-Dienstleistungen zu einem gewünschten Zeitpunkt in bestimmter Form beziehen kann. Die Cloud wird für verschiedene Arten genutzt:

- Bei Infrastructure as a Service (IaaS) wird anstelle des klassischen Kaufs von Rechnerinfrastruktur diese gemietet.
- Bei Software as a Service (SaaS) wird Software nicht länger als Lizenz an einen Benutzer verkauft, sondern lediglich die Benutzung als Service zur Verfügung gestellt. Besonders vorangetrieben wurde diese Entwicklung durch Webservices, die in der Regel pro Aufruf abgerechnet werden.
- Bei Platform as a Service (PaaS) ist der Ansatz, eine integrierte Laufzeit- und evtl. auch Entwicklungsumgebung als einen Dienst zur Verfügung zu stellen, für den der Nutzer bei Benutzung zahlen muss.

Die Abrechnung erfolgt nutzungsabhängig, das heisst, es werden nur die tatsächlich genutzten Dienste bezahlt. Ein weiterer zentraler Punkt des Konzeptes ist, dass die Bereitstellung basierend auf der Kombination aus virtualisierten Rechenzentren und modernen Webtechnologien wie Webservices vollautomatisch erfolgen kann und somit keinerlei Mensch-Maschine-Interaktion mehr erforderlich ist.

Wichtig bei Cloud-Lösungen ist die Überlegung der Datenhoheit. Das Schweizerische Datenschutzgesetz erlaubt das Auslagern von schützenswerten Daten nur in Länder mit einem analogen Datenschutz. Dies ist z.B. in Amerika nicht gegeben. Weiter gilt es zu beachten, dass Cloud-Lösungen oft mit weiteren Kunden geteilt werden. Sollten Schwachstellen gefunden werden, ist es allenfalls möglich, dass eigene Daten «verschwinden» oder unerlaubt kopiert werden. Zudem muss im Hinterkopf daran gedacht werden, dass unter anderem der Administrator des Cloud-Anbieters Zugriff auf die Daten hat.

## 6.10 Biometrie

Biometrische Verfahren verwenden Merkmale eines Menschen, welche sich nicht verändern, wie zum Beispiel Fingerabdruck, Gesichts- oder Handgeometrie. Ergänzt werden diese mit verhaltensorientierten Merkmalen, wie beispielsweise Tippdynamik, Unterschrift oder Stimme.

Von einem sicheren biometrischen Authentifizierungssystem wird erwartet, dass es fehlerfrei zwischen Berechtigten und Unberechtigten unterscheiden kann, selbst wenn eine leichte Abweichung des Merkmals auftritt. Eine Abweichung könnte zum Beispiel durch eine veränderte Stimmlage oder durch unreine Fingerabdrücke entstehen. Je toleranter das System gegenüber Abweichungen ist, umso höher wird auch die Gefahr, dass Unberechtigte irrtümlicherweise Zugang erhalten. Je niedriger die Systemtoleranz ist, umso häufiger werden Berechtigte fälschlicherweise zurückgewiesen.

Die Sicherheit und Qualität biometrischer Authentisierungssysteme kann teilweise mit folgenden «Messwerten» verglichen werden:

- FAR (False Acceptance Rate)
  Die Rate/Wahrscheinlichkeit, dass Unberechtigte irrtümlicherweise als Berechtigte erkannt werden.
- FRR (False Reject Rate)
  Die Rate/Wahrscheinlichkeit, dass Berechtigte irrtümlicherweise als Unberechtigte erkannt werden.
- EER (Equal Error Rate)
  An dem Punkt, wo sich die Kurven für FRR und FAR schneiden, liegt der EER.

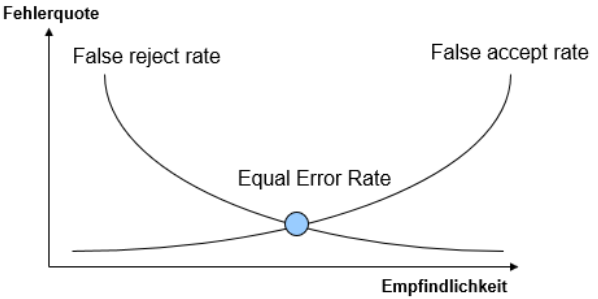


Abbildung 22: Biometrische Kennzahlen

# 7 goSecurity GmbH

Für die gezielte Erhöhung Ihrer IT-Sicherheit haben wir die richtigen Experten. Diese sind darauf spezialisiert, vorhandene und potenzielle Schwachstellen in Ihrer IT-Infrastruktur aufzuspüren. Mit den Resultaten unserer Überprüfungen und Beratungen können Sie Ihre IT-Sicherheit gezielt erhöhen.

Sie profitieren zudem von unserer Unabhängigkeit. Weder der Verkauf von Software oder Hardware noch Implementierungen gehören zu unserem Portfolio. Erlangen Sie die Sicherheit, Ihre Kontrollfunktion gegenüber den Stakeholdern wahrgenommen zu haben.

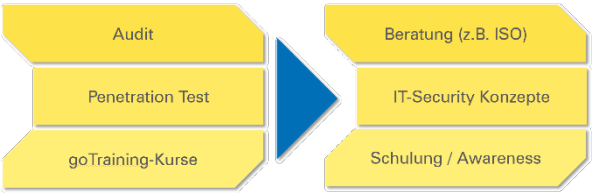


Abbildung 23: Dienstleistungen der goSecurity GmbH

**Audit**

Ihre Infrastruktur, Ihre Anforderungen an die IT-Sicherheit und Ihre individuellen Wünsche stehen beim Audit im Fokus. Mit den Resultaten können Sie Schwachstellen in Ihrer IT-Infrastruktur systematisch beheben. Der Umfang beinhaltet viele Elemente wie Serverraum, Serverkonfigurationen, Netzwerk, Firewall, Back-up und auch der Wissensstand der Mitarbeiter wird berücksichtigt.

**Penetration Test**

Erfahren Sie, wie tief ein Hacker in Ihre IT-Infrastruktur eindringen kann. Tools, manuelle Arbeitsschritte und viel Erfahrung werden dabei von unseren Experten kombiniert. Mit dem ausführlichen Bericht sind Vorgehen und gefundene Schwachstellen für Sie nachvollziehbar dokumentiert.

**Konzepte / Beratung**

Durch unsere Tätigkeit sehen wir viele unterschiedliche Lösungsansätze und erleben deren Vor- und Nachteile in der Praxis. Lassen Sie Ihre IT-Security-Konzepte durch uns erstellen und nutzen Sie unser IT-Security-Fachwissen.

**ISO 27001 Zertifizierungsbegleitungen**

ISO 27001 ist ein weltweit angewendeter Standard für die Zertifizierung eines Informationssicherheits-managementsystems (ISMS). Dieses hat zum Ziel, die Informationen basierend auf einer Analyse der Geschäftsrisiken bezüglich Vertraulichkeit, Integrität und Verfügbarkeit zu schützen.

Wir helfen Ihnen bei allen Schritten, erstellen mit Ihnen zusammen die notwendigen Dokumente und bereiten Sie optimal zur Zertifizierung vor.

**Kurse / Schulung / Awareness**

Lernen Sie in unseren Kursen, wie ein Hacker Schwachstellen sucht und ausnutzt. Wenden Sie das erworbene Wissen an, um Ihre IT-Infrastruktur optimal zu schützen. Auch individuelle Awareness-Trainings für IT-Mitarbeiter oder Benutzer führen wir bei Ihnen vor Ort durch.

Weitere Informationen über die Dienstleistungen und das Team sowie viele nützliche Informationen finden Sie im Internet unter www.goSecurity.ch.

goSecurity GmbH
Schulstrasse 11
8542 Wiesendangen
+41 52 511 37 37

# 8 Autor & BPX

**Andreas Wisler**
Dipl. Ing. FH, CISSP, CISA, ECSA, CEH, ISO 22301 + 27001 Lead Auditor, IT-Sicherheitsbeauftragter nach BSI

Inhaber und Senior Security Consultant bei der goSecurity GmbH. Weiter unterrichtet er an der FHNW IT-Sicherheitsthemen.

**Weiterbildung in Informationssicherheit**:

www.hslu.ch

www.fhnw.ch

www.zhaw.ch

www.goTraining.ch

Dieses Booklet wird ergänzt durch die Homepage www.cyber-sec.ch mit vielen Anleitungen, Tipps und Tricks zu den beschriebenen Themen. Zusätzlich werden auf www.bpx.ch/digital-kmu/ neue, aktuelle Themen aufgeschaltet.

**BPX steht für Best Practice Xperts**

**Martin Dalla Vecchia**
lic. rer. pol.
Dalla Vecchia GmbH

Herausgeber der BPX-Booklets

BPX.

Die Informationssicherheit wird immer wichtiger. Praktisch jeden Tag kann von neuen Schwachstellen und Gefahren gelesen werden. Der Autor Andreas Wisler zeigt in diesem Buch aktuelle Bedrohungen und erklärt entsprechende (Gegen-) Massnahmen. Das organisierte Verbrechen hat längst den Weg zur Cyber-Kriminalität gefunden. Es geht heute nicht mehr um Ruhm und Ansehen, sondern um Geld, um viel Geld.

Die Verantwortung für den ordnungsgemässen Betrieb eines Unternehmens liegt per Gesetz beim Management. Für das Management ist es wichtig, die gesetzlichen Anforderungen zu kennen, um entsprechende Massnahmen planen und umsetzen zu können. Verschiedene Standards wie ISO 27001 oder die BSI-Grundschutzkataloge können dabei ein geeignetes Werkzeug sein. Massnahmen sollten dem Risiko entsprechend angepasst sein. Dieses Buch geht ebenso auf diesen Risiko-Prozess ein wie auf die zahlreichen Sicherheitsmassnahmen, die Funktionsweise der Verschlüsselung, den Schutz durch Firewalls oder das Back-up als Lebensversicherung der Daten.

Mit diesem Buch erfahren Sie in Kürze alles Wichtige, um Ihre Informationssicherheit nachhaltig zu erhöhen.

Rheinfelden/Schweiz
BPX-Edition 2018
www.bpx.ch

20 CHF

978-3-905413-58-8

goSecurity
EXPERTEN FÜR IHRE IT-SICHERHEIT