Cybersicherheit im 21. Jahrhundert

Andreas Wisler ist Inhaber der Firma goSecurity AG (https://goSecurity.ch). Er ist CISSP, CISA, CDPSE, ISO 22301, 27001 sowie der erste Schweizer ISO 27701 Lead Auditor. Seit über 20 Jahren ist er im IT-Sicherheitsbereich tätig und unterstützt Firmen beim Aufbau eines ISMS und der Erlangung des ISO-27001-Zertifikats. Alle zwei Wochen veröffentlicht er den Podcast «Angriffslustig», zu abonnieren unter https://angriffslustig.ch. Sein Blog ist unter https://27001.blog abrufbar.

Inhaltsverzeichnis

1. Management Summary

Praktisch jeden Tag kann von Cyberangriffen 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.:

- 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.

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 längst den Weg ins Internet gefunden und verdient viel Geld mit Angriffen, Erpressungen, Ransomware und Betrug. Daher ist es essenziell wichtig, sich mit den Bedrohungen auseinanderzusetzen und entsprechende Massnahmen proaktiv zu ergreifen.

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 zehn Jahre. Diese Zeitspanne kann je nach Branche und zum Zweck Beweispflicht auch länger sein.
- öffentlich-rechtliche Vorschriften, z.B. bezüglich Auskunftspflicht, Berufsgeheimnissen usw.
- Strafrecht: Zum Beispiel 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 Informationssicherheitsmanagementsysteme (ISMS) erleichtert und unterstützt diese Aufgabe wesentlich.

Gesetze sind aber nicht der Hauptgrund für den Einsatz von Sicherheitsmassnahmen. Diese verlangen mehrheitlich Elemente, die sowieso für jedes Unternehmen 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, vor allem 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 Backups. Da diese aber nie auf korrekte Funktionsweise überprüft wurden und oft auch nicht in feuersicheren Behältern ausserhalb des Betriebs lagern, kann ein vollständiger Restore (Wiederherstellung) nicht garantiert werden.

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

2.2 Begrifflichkeiten

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

Die **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 Verbindlichkeit in diese Kategorie. Mit der Informationssicherheit sollen Risiken minimiert und dadurch der Schutz vor Gefahren oder Bedrohungen erhöht werden.

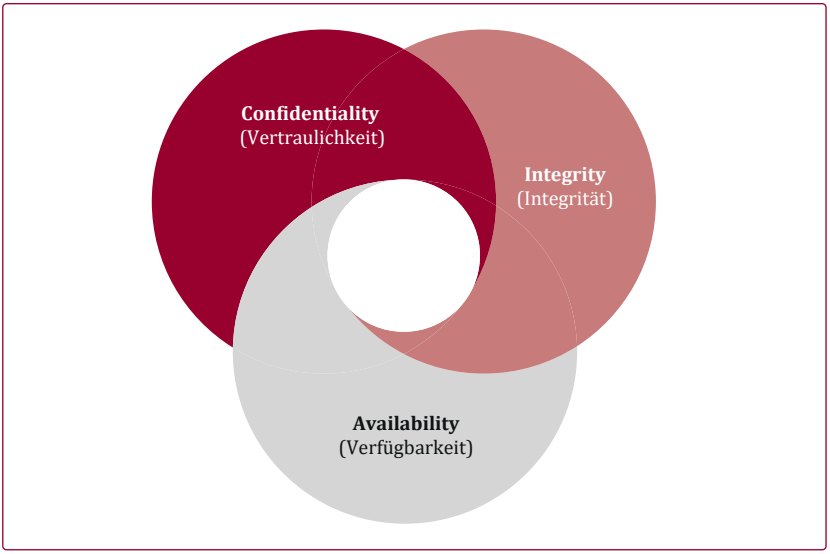

Abbildung 1: Grundbausteine der Informationssicherheit

Vertraulichkeit

Unter Vertraulichkeit (englisch: Confidentiality) wird verstanden, dass nur Personen oder Prozesse Daten einsehen oder offenlegen dürfen, die auch dazu berechtigt sind. Dies bedeutet, dass definiert werden muss, wie der Zugriff auf diese Daten erfolgt. Des Weiteren gehört die sichere Übertragung der Daten in diesen Bereich. Hier werden klassische Verschlüsselungsverfahren eingesetzt. Bei der physischen Bearbeitung muss sichergestellt werden, dass nur berechtigte Personen Zutritt und Zugriff auf diese Daten erhalten.

Integrität

Die Integrität (englisch: Integrity) stellt sicher, dass Veränderungen an Daten nicht unerkannt bzw. unbemerkt möglich sind. Bei starker Integrität wird zudem gefordert, dass Daten in keiner Weise unberechtigt verändert werden können. Klassisch wird dies mit Hash-Werten sichergestellt.

Verfügbarkeit

Die Verfügbarkeit (englisch: Availability) beschreibt, dass die Daten, Systeme oder Prozesse verfügbar sind, wenn sie benötigt werden. Bei Systemen gilt es, Ausfälle mit oder ohne Datenverlust zu minimieren. Ausfälle können passieren, daher gilt es, die notwendige Verfügbarkeit bzw. die maximal akzeptierte Ausfalldauer zu definieren.

Verbindlichkeit

Die Verbindlichkeit/Nichtabstreitbarkeit (englisch: Non-repudiation) wird unter anderem bei Transaktionen angewendet, z.B. bei Abstimmungen. Sie kann in zwei Richtungen angewendet werden: die Nichtabstreitbarkeit des Empfangs von Nachrichten wie auch die Nichtabstreitbarkeit des Sendens von Nachrichten.

Mit **Cybersicherheit** 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.

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

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. Das DSG wurde komplett überarbeitet und wird per 1. September 2023 in Kraft treten.

Gebote zur Einhaltung des Schutzes der Privatsphäre (Art. 6 Grundsätze):

- Personendaten müssen rechtmässig bearbeitet werden.
- Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein.
- Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.
- Sie werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.
- Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.
- Ist die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt wird.

Der Art. 7 verlangt, dass der Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen umgesetzt wird. Dies ist bereits ab der Planung zu berücksichtigen. Die technischen und organisatorischen Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein.

Der Art. 8 geht zudem auf die Datensicherheit ein. Es wird eine dem Risiko angemessene Datensicherheit verlangt, die der Verantwortliche und der Auftragsbearbeiter durch geeignete technische und organisatorische Massnahmen gewährleisten müssen. Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

2.3.3 Internes Kontrollsystem IKS

Das Obligationenrecht fordert mit dem Art. 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 Katastrophenvorsorgeplan 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 Risikoanalyse und darauf basierend erhöhte Sicherheitsmassnahmen unumgänglich.

Um die Entwicklung von Sicherheitskonzepten zu vereinfachen, wurden Standards und Normen geschaffen.

Normen und Standards sind in der Regel freiwillig. Verpflichtet sich ein Unternehmen, eine Norm zu erfüllen, wird diese verpflichtend. Normen und Standards stellen somit Anforderungen, die es zu erfüllen gilt. Die Ziele von Informationssicherheitsstandards sind wie folgt:

- Beschreiben von Modellen, anhand derer ein Sicherheitsmanagement systematisch aufgebaut und weiterentwickelt werden kann
- Aufzeigen, welche organisatorischen und technischen Massnahmen erforderlich sind
- Definition von Kriterien, anhand derer überprüft werden kann, ob die umgesetzten Massnahmen angemessen sind

3.1 Anforderungen eines KMU

Die Anforderungen an die Informationssicherheit eines KMU sind vielfältig, sowohl in Bezug auf interne als auch externe Themen. Im folgenden Bild werden diese Anforderungen dargestellt:

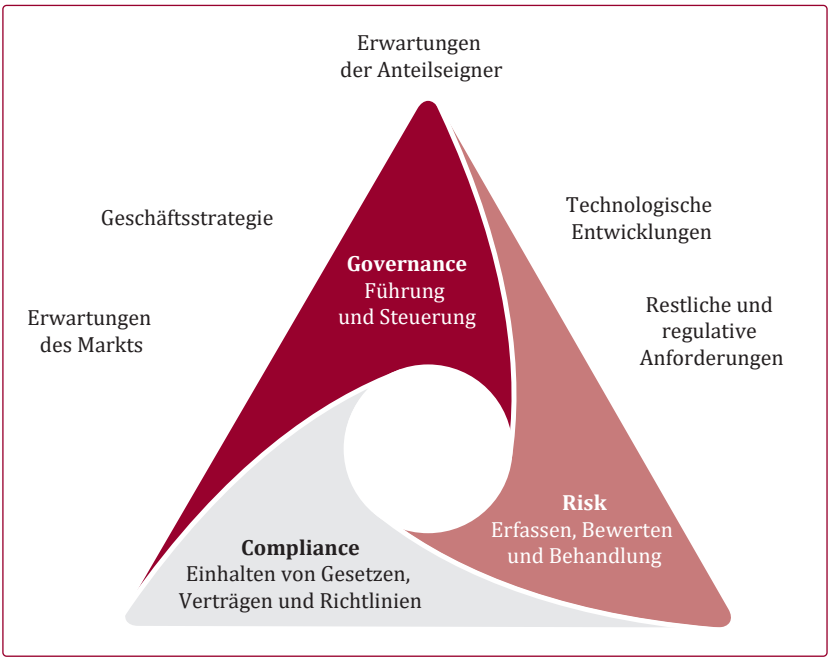

Abbildung 2: Anforderungen an ein KMU

Im Inneren der Darstellung sind die Themen Governance, Risikomanagement und Compliance (GRC) abgebildet.

Governance

Unter Governance wird die Führung und Steuerung des Unternehmens verstanden. Wie ist das Unternehmen strukturiert? Welche Funktionen sind vorhanden? Welche Rechte und Pflichten sind mit diesen Funktionen und Aufgaben verbunden? Ein Organigramm kann hier einen ersten Hinweis auf das Unternehmen liefern. Daraus abgeleitet werden die Funktionen und Aufgaben beschrieben.

Risikomanagement

Das Risikomanagement stellt ein Schlüsselthema dar. Es gilt, Kriterien zum Umgang mit Risiken zu definieren (z.B. wann Risiken als akzeptiert gelten) sowie diese systematisch zu erfassen, zu bewerten und zu behandeln.

Compliance

Unter Compliance wird die Einhaltung von Gesetzen, Verträgen, aber auch internen Richtlinien verstanden. Das Unternehmen muss die anwendbaren Gesetzgebungen und die vertraglichen Anforderungen festhalten, denn nur was bekannt ist, kann auch eingehalten werden. Des Weiteren gehören auch interne Richtlinien dazu. Was wurde im Bereich der Informationssicherheit bereits definiert?

Ausserhalb der Grafik sind die externen Anforderungen abgebildet:

Erwartungen des Markts

Die Kunden, Partner und/oder Lieferanten stellen Erwartungen an ein Unternehmen, z.B. das Erfüllen von vertraglichen Abmachungen, das Erfüllung von Dienstleistungen etc.

Geschäftsstrategie

Das Unternehmen möchte sich in eine Richtung entwickeln, neue Märkte angehen, Umsatzziele erreichen, neue Dienstleistungen erarbeiten, den Mitarbeitenden einen sicheren Arbeitsplatz bieten etc.

Erwartungen der Anteilseigner

Dies kann beispielsweise die Ausschüttung einer Dividende sein, ein gut funktionierendes Unternehmen etc.

Technologische Entwicklungen

Tagtäglich kommen neue Geräte und Technologien auf den Markt. Für ein Unternehmen ist es schwierig, immer auf dem aktuellen Stand zu bleiben. Die Anforderungen und die neuen Technologien erfordern ein ständiges Umdenken.

Rechtliche, regulative Anforderungen

Neue oder veränderte Gesetze müssen erfüllt werden. Dies kann einen bedeutenden Einfluss auf Arbeitsweisen im Unternehmen haben.

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 Informationssicherheitsmanagementsystems (ISMS) unter Berücksichtigung der Risiken. Unternehmen können sich nach diesem Standard zertifizieren lassen. Dieser Standard wurde Ende Oktober 2022 in einer aktualisierten Version veröffentlicht.

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 die vier Themengebiete «Organizational controls» (37), «People controls» (8), «Physical controls» (14) und «Technological controls» (34). In Klammern ist die Anzahl der geforderten Massnahmen aufgeführt.

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://27001.blog.

3.3 Grundschutz nach BSI

Das Deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt umfangreiche Informationen kostenlos zur Verfügung. Informationen dazu sind unter www.bsi.de/gshb abrufbar. Sie dienen dazu, einen Grundschutz in der IT zu erstellen.

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

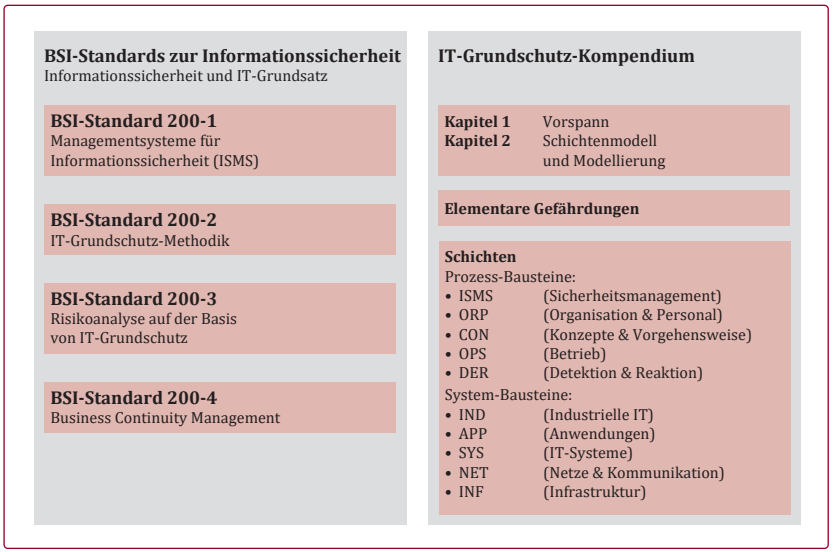

Abbildung 3: BSI-Zertifikate sind kompatibel mit ISO 27001

3.3.1 Standard 200-1

Dieser Standard ist in Deutsch und Englisch verfügbar. Nachfolgend ist eine kurze Zusammenfassung der Kapitel aufgeführt.

Während ISO 27001 die Anforderungen definiert, beantwortet der BSI-Standard unter anderem folgende Fragen:

- Was sind die Erfolgsfaktoren beim Management von Informationssicherheit?

- Wie kann der Sicherheitsprozess vom verantwortlichen Management gesteuert und überwacht werden?
- Wie werden Sicherheitsziele und eine angemessene Sicherheitsstrategie entwickelt?
- Wie werden Sicherheitsmassnahmen ausgewählt und Sicherheitskonzepte erstellt?
- Wie kann ein einmal erreichtes Sicherheitsniveau dauerhaft erhalten und verbessert werden?

Das Kapitel 3 geht auf die Kernkomponenten eines Managementsystems ein. Es sind dies:

- der Sicherheitsprozess, welcher eine Leitlinie, ein Konzept und die Organisation umfasst
- die notwendigen Ressourcen
- die Mitarbeiter, inkl. deren Aufgaben und Verantwortlichkeiten sowie
- die Managementprinzipien

Den zuletzt genannten Managementprinzipien wird ein ganzes Kapitel gewidmet. Bereits die ISO 27001 verlangt im Kapitel 5 «Führung» verschiedene Punkte von der obersten Leitung. Im 200-1 werden diese weiter ausgeführt. Es handelt sich um die folgenden sechs Punkte:

- Übernahme der Gesamtverantwortung für Informationssicherheit
- Informationssicherheit initiieren, steuern und kontrollieren
- Informationssicherheit integrieren
- erreichbare Ziele setzen
- Sicherheitskosten gegen Nutzen abwägen
- Vorbildfunktion

Weitere Punkte im Kapitel 4 sind die Kommunikation und Wissen (4.2), die Erfolgskontrolle im Sicherheitsprozess (4.3) sowie die kontinuierliche Verbesserung des Sicherheitsprozesses (4.4).

Gerade die Kommunikation stellt einen Erfolgsfaktor für die Informationssicherheit dar. Dies beinhaltet unter anderem die Berichte an die

Leitungsebene. Dies beinhaltet Probleme, Ergebnisse von Audits und Überprüfungen, neue Entwicklungen, Veränderungen, aber auch Verbesserungsmöglichkeiten. Auch muss der Informationsfluss im gesamten Unternehmen sichergestellt sein. Werden neue Richtlinien oder Weisungen verabschiedet, müssen diese allen involvierten Personen zugestellt werden. Es muss unter allen Umständen verhindert werden, dass jemand sagt: «Davon habe ich nichts gewusst».

Bei der Erfolgskontrolle geht es um die Überprüfung des aktuellen Stands. In der ISO-Norm wird dies die Managementbewertung genannt (ISO 27001, Kapitel 9.3). Ist das Unternehmen noch auf dem richtigen Kurs? Haben sich Anforderungen geändert? Gibt es Rückmeldungen von interessierten Parteien, aber auch Resultate von Audits? Sind die Informationssicherheitsziele noch passend? Abweichungen und Veränderungen werden schriftlich erfasst und Massnahmen geplant, umgesetzt, kontrolliert und wieder zurückgemeldet. Mit diesen Schritten kann sich ein Unternehmen kontinuierlich weiter verbessern und die Informationssicherheit damit erhöhen.

In kurzen Kapiteln werden die notwendigen Ressourcen (5) und die Einbindung der Mitarbeiter in den Sicherheitsprozess (6) beschrieben.

Ausführlich beschrieben ist der Sicherheitsprozess in Kapitel 7. Unterteilt ist das Kapitel in die Planung (Ermittlung von Rahmenbedingungen, Definition von Sicherheitszielen, Ermitteln eines angemessenen Sicherheitsniveaus), den Aufbau der Sicherheitsorganisation, die Umsetzung, die Aufrechterhaltung und die kontinuierliche Verbesserung. Details zu diesen Themen sind im BSI-Standard 200-2 mit konkreten Beispielen enthalten.

Ebenfalls ausführlich beschrieben wird das Sicherheitskonzept in Kapitel 8. Es ist nach dem PDCA-Ablauf (Plan, Do, Check, Act) aufgebaut.

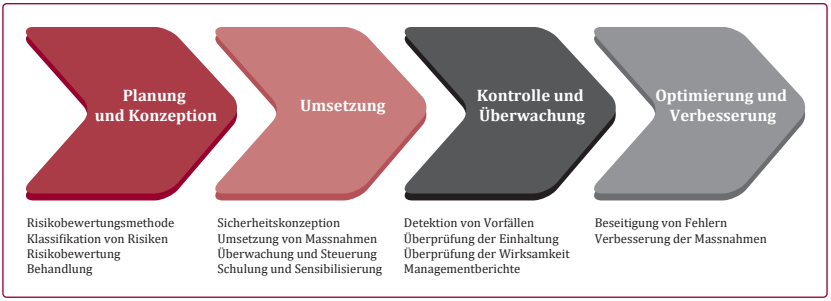

Abbildung 4: Sicherheitskonzept, PDCA

Im Kapitel 9 folgt die Beschreibung des Wegs zu einer erfolgreichen Zertifizierung des ISMS.

Das Kapitel 10 geht auf die IT-Grundschutz-Methodik ein und verbindet das ISMS mit dem IT-Grundschutz-Kompendium. Dieses bereits 1000 Seiten umfassende Werk inkl. weiterführender Informationen ist kostenlos im Internet aufrufbar.

Das Kompendium ist in zehn Bausteine unterteilt und bietet damit eine ganzheitliche Betrachtung der Informationssicherheitsthemen:

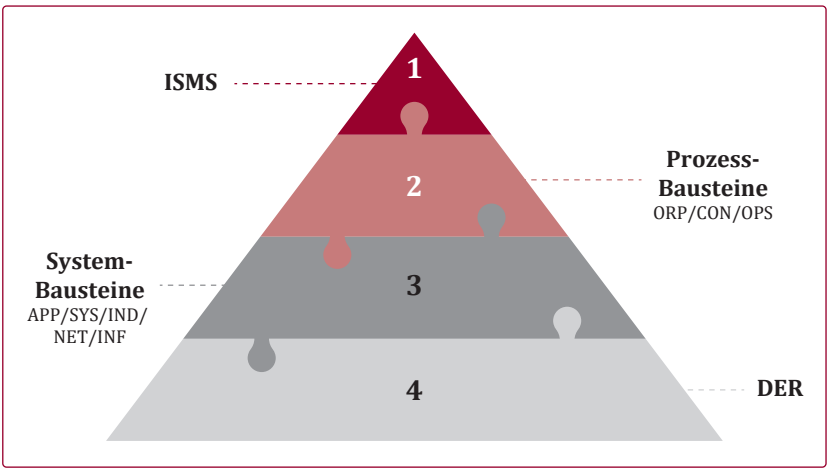

Abbildung 5: BSI-Grundschutz-Bausteine

Die Abkürzungen stehen dabei für:

- ISMS: Informationssicherheitsmanagementsystem
- ORP: organisatorische und personelle Sicherheitsaspekte
- CON: Konzepte und Vorgehensweise
- OPS: Sicherheitsaspekte betrieblicher Art
- APP: Absicherung von Anwendungen und Diensten
- SYS: IT-Systeme
- IND: Sicherheitsaspekte industrieller IT
- NET: Vernetzungsaspekte
- INF: infrastrukturelle Sicherheit
- DER: Detektion und Reaktion von Sicherheitsvorfällen

In jedem dieser Bausteine werden Gefährdungen und konkrete Massnahmen beschrieben, einschliesslich verantwortlicher Personen und Kontrollfragen.

3.3.2 Standard 200-2

Der ebenfalls kostenlos verfügbare Standard mit dem Titel «IT-Grundschutz-Methodik» kann in Deutsch auf der Homepage des BSI heruntergeladen werden.

Diese Methodik beschreibt, wie ein ISMS in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des Informationssicherheitsmanagements und der Aufbau einer Organisationsstruktur sind dabei wichtige Elemente. Es orientiert sich an den drei Vorgehensweisen Standard-, Basis- und Kernabsicherung.

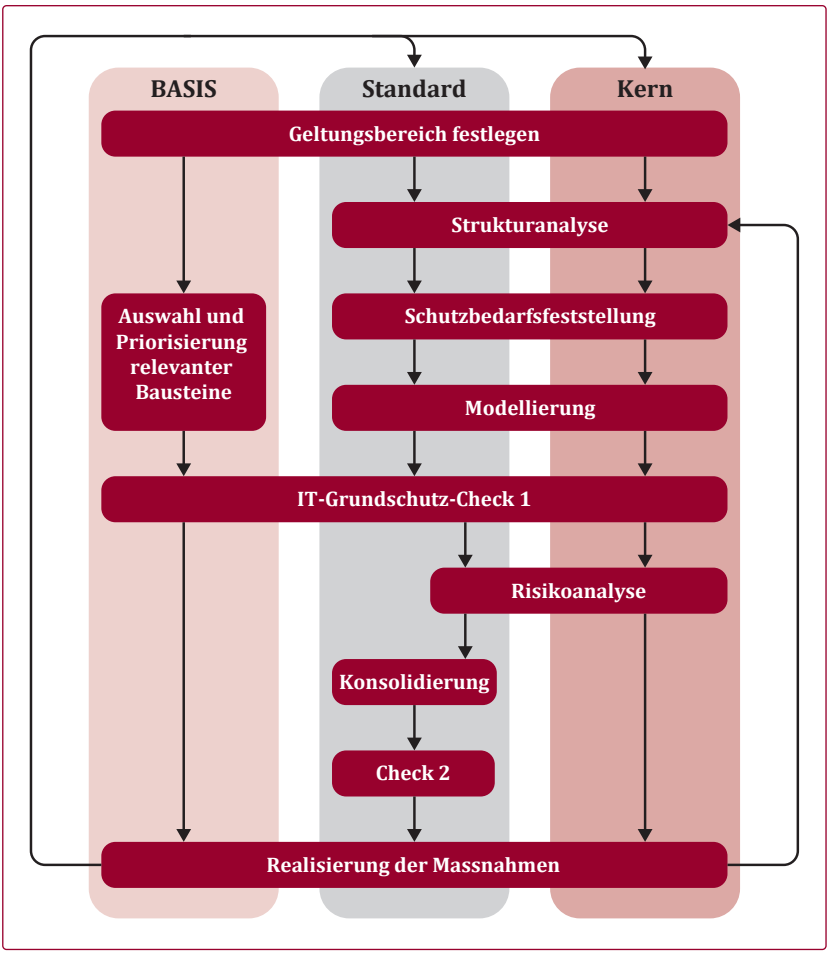

Abbildung 6: Basis-, Standard- und Kernabsicherung

- Basisabsicherung: ermöglicht einen Einstieg in die Thematik. Es ist eine breit angelegte Erstabsicherung. Die Massnahmen werden nicht bis ins letzte Detail umgesetzt verlangt.
- Kernabsicherung: ermöglicht den Sicherheitsprozess auf besonders gefährdete Geschäftsprozesse oder Werte (im Standard «Kronjuwelen» genannt) zu legen. Nachteilig ist, dass allenfalls ebenfalls wichtige Geschäftsprozesse nicht betrachtet werden.
- Standardabsicherung: ermöglicht den im Standard 200-1 beschriebenen Ansatz vollständig umzusetzen. Als Endergebnis kann eine Zertifizierung nach ISO 27001 durchgeführt werden.

Wie das Bild zeigt, steigt der Aufwand an die Umsetzung. Im ersten Schritt wird der Anwendungsbereich definiert. Es ist möglich, auch Teilbereiche eines Unternehmens durch den Prozess zu führen und nicht das gesamte. Dies ergibt beispielsweise Sinn, wenn ein kritischer Bereich vorhanden ist, z.B. der Betrieb eines Rechenzentrums. Eine Unterteilung muss jedoch gut überlegt werden, steigt damit doch der Aufwand zur genauen Definition der Schnittstellen. Bei kleineren Unternehmen ergibt dies oft keinen Sinn, da dadurch der Aufwand sogar steigen kann.

Im Kapitel 4 wird die Organisation des Sicherheitsprozesses aufgezeigt. Der Kapitelaufbau entspricht dem Standard 200-1, zeigt aber konkrete Beispiele für grosse, mittelgrosse und kleine Institutionen. Weiter werden Rollen wie der Informationssicherheitsbeauftragte, das IS-Managementteam, die Bereichs- und Projektsicherheitsbeauftragte, der ICS-Informationssicherheitsbeauftragte, der IS-Koordinierungsausschuss, die Datenschutzbeauftragte inkl. deren Aufgaben sowie das Zusammenspiel mit anderen Einheiten oder dem Bezug von externen Spezialisten sehr detailliert aufgezeigt.

Das Kapitel 5 geht auf die Dokumentation im Sicherheitsprozess ein. Ein wichtiger Aspekt sind die Klassifikation von Informationen und der Informationsfluss. Die Kapitel 6 bis 8 beschreiben im Detail die Vorgehensweise der Basis-, Kern- und Standardabsicherung. In der Strukturanalyse wird erfasst, welche Mittel vorhanden sind. Dies umfasst die Erfassung der Prozesse, der Anwendungen, der Systemen, Netzwerkkomponenten, Räume, Menschen und Kommunikationsverbindungen. Danach wird der Schutzbedarf festgelegt. Dieser geht von den Prozessen aus und vererbt sich auf die Anwendungen, von dort auf die Systeme usw. Wenn diese Tätigkeit abgeschlossen ist, werden die genutzten Bausteine aus dem Kompendium bestimmt und einem Soll-Ist-Vergleich unterzogen. In jedem Baustein sind mehrere Massnahmen beschrieben, und es gilt nun die Frage zu beantworten, ob diese im eigenen Unternehmen umgesetzt sind (ja, teilweise, nein). Alles, was einen erhöhten Schutzbedarf hat, der nicht mit dem Grundschutz-Kompendium abgedeckt werden kann, muss zusätzlich einer Risikoanalyse unterzogen werden. Alle Resultate werden anschliessend konsolidiert und nochmals kurz auf Vollständigkeit überprüft, bevor es dann an die Umsetzung der offenen Massnahmen geht.

Die Kapitel 9 bis 11 gehen schlussendlich noch auf die Umsetzung, die Aufrechterhaltung und kontinuierliche Verbesserung sowie die Zertifizierung nach ISO 27001 ein.

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 geführt 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.

4.1.1 Physische Bedrohungen

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

Checkliste physischer Bedrohungen: Wurden folgende Bedrohungen überprüft und die Resultate in die Risikoanalyse integriert?

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

- Gasleitungen
- Lager von Explosivstoffen
- Anflugschneise Flughafen
- Verfügbarkeit von Transportmitteln
- ungesicherter Zugang

4.1.2 Bedrohungen im IT-Bereich

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

- Ausfall von Netzteilen
- Recovery von Backups 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.

4.1.3 Bedrohungen im Telekommunikationsbereich

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

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 immer mehr vom Stören und Zerstören mit Malware hin zu schädlichem Code in Browserinhalten

(via infizierter Webseite, sog. Drive-by). Oft kommt dabei nicht nur ein Mittel zum Einsatz, sondern eine Kombination davon.

Eine ernst zu nehmende Gefahr sind auch 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 (auch 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.

4.1.4 Bedrohungen bei mobilen Endgeräten

Grundsätzlich gelten hier auch fast alle Bedrohungen aus dem Bereich der Telekommunikation. Erschwerend kommt hinzu, 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 (Remote-Gaming, Chatten, Teilnahme an Tauschbörsen usw.).

4.1.5 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 Risikoanalyse 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:

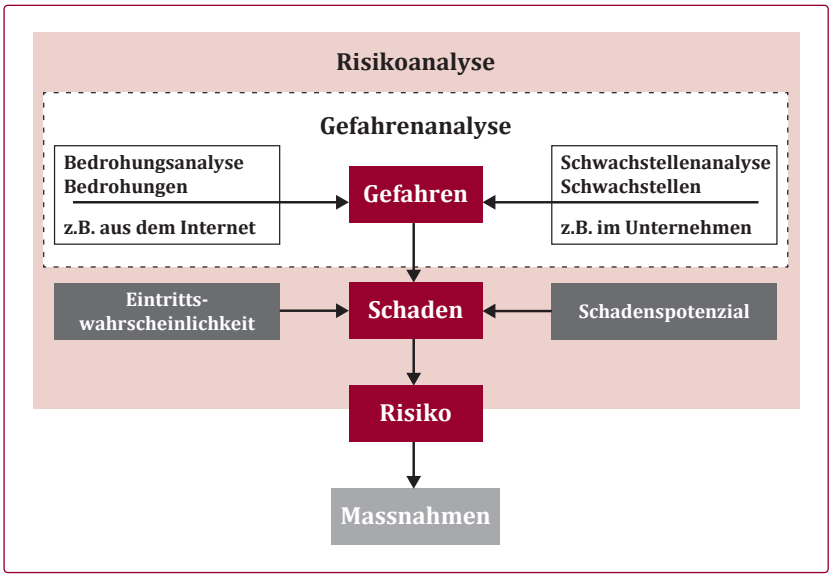

Abbildung 7: Übersicht über Risikoanalysen

Zuerst werden die vorhandenen Bedrohungen aufgelistet und eingestuft (z.B. tief, mittel, hoch), danach die vorhandenen Schwachstellen. Trifft eine Gefährdung auf eine Schwachstelle, dann existiert eine Gefahr. Aus einer Gefahr kann ein Schaden mit einer gewissen Schadenshöhe und mit einer entsprechenden Eintrittswahrscheinlichkeit entstehen. Dies ergibt ein Risiko.

Wichtige Begriffe:

- Ein **Risiko** ist definiert als eine auf ein spezifisches Objekt bezogene Gefahr, die hinsichtlich Eintrittswahrscheinlichkeit 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 Eintrittswahrscheinlichkeit 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** (0–10)	**[S] Schadenshöhe** (p.a. CHF 50.–)	**[R] Risiko** (W×S/50)
a) Datenverlust	Privatdaten (E-Mails, Fotos, Buchhaltung, …)	8	100	800
	Geschäftsdaten (Adressen, Office-Dateien, Buchhaltung, …)	8	200	1600
b) fehlende Datenintegrität (Vollständigkeit)	Privatdaten (E-Mails, Fotos, Buchhaltung, …)	3	10	30
	Geschäftsdaten (Adressen, Office-Dateien, Buchhaltung, …)	4	50	200
c) Einsicht/Preisgabe sensibler Daten (Confidentiality)	Privatdaten (E-Mails, Fotos, Buchhaltung, …)	3	10	30
	Geschäftsdaten (Adressen, Office-Dateien, Buchhaltung, …) Geschäftsschädigung	4	500	2000

Abbildung 8: Risikoanalyse

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

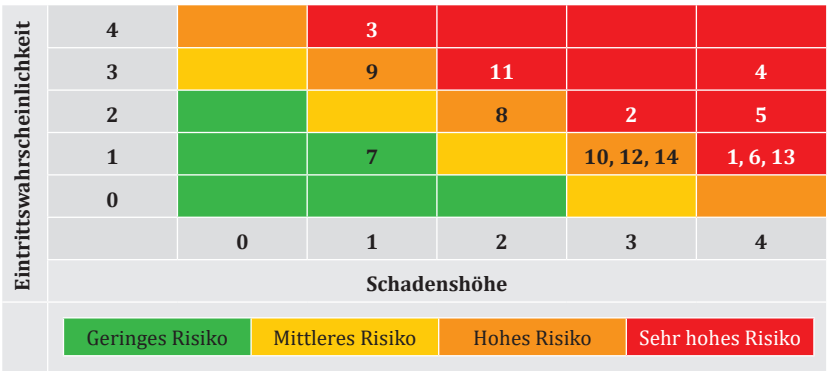

Abbildung 9: Risikoübersicht

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 Risikomanagement.

4.2.1 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 10: Risikoanalyse

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

4.2.2 Risiken managen

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

Beim Risikomanagement 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.

4.2.3 Risiken minimieren

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 Antivirenprogramm 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 Risikomanagementprozess.
- 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 Katastrophenvorsorgeplan.
- Schliessen Sie Supportverträge bei geschäftskritischen Prozessen.
- Bei sehr seltenen, aber grossen Risiken kann eine Risikoversicherung zweckmässig sein.

4.3 Business Continuity Management

Ein effektives Business Continuity Management (BCM) (zu Deutsch auch Katastrophenvorsorgeplan 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 Backups
- Ausbildungsplan
- periodische Notfallübungen

Das wichtigste Element des BCM ist die Business-Impact-Analyse (BIA). Diese dient dazu, kritische Prozesse zu identifizieren und zu bewerten. Dabei werden Prozesse mit hohem Einfluss auf andere Prozesse und auch Abhängigkeiten von Prozessen untereinander erfasst.

In einem ersten Schritt werden die Prozesse in einem Unternehmen angeschaut. Dabei ist wichtig, diese zuerst ohne Bewertung oder grosse Diskussionen anzuschauen. Auch eher triviale Prozesse wie den Briefkas-

ten leeren, gehören da dazu. Gleichzeitig wird erfasst, ob Prozesse von anderen Prozessen abhängig sind.

Erst wenn alle erfasst sind, werden in den Prozessen auch die beiden Werte RPO und RTO bestimmt.

- RTO (Recovery Time Objective): Wie lange darf ein Geschäftsprozess/System ausfallen? Es ist also der Zeitbedarf, der vom Zeitpunkt des Schadens bis zur vollständigen Wiederherstellung der Geschäftsprozesse reicht.
- RPO (Recovery Point Objective): Welcher Datenverlust kann in Kauf genommen werden? Dies gibt den maximalen Zeitraum an, der zwischen zwei Datensicherungen liegen darf.

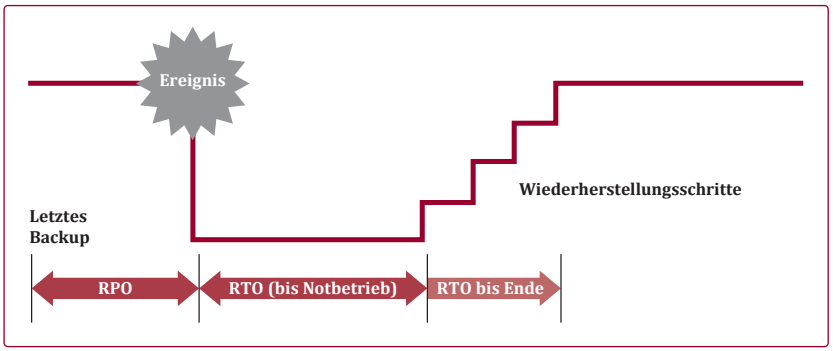

Abbildung 11: RTO und RPO im zeitlichen Ablauf

Im zweiten Schritt werden die verarbeiteten Daten angeschaut. Dies können Kundendaten, technische Dokumente und Anleitungen, Strategien, interne Dokumente von Mitarbeitenden, Prozesslisten und vieles weitere sein. Diese Daten werden nach ihrer Kritikalität bewertet (Vertraulichkeit, Integrität, Verfügbarkeit).

Im dritten Schritt werden die genutzten Anwendungen, Gebäude, involvierten Mitarbeitenden, Lieferanten und weitere Abhängigkeiten erfasst und mit den Prozessen verknüpft. Diese Elemente erben damit die vorher definierte Kritikalität.

Bei elektronischer Verarbeitung wird im vierten Schritt erfasst, auf welchen Systemen die Anwendungen laufen. Dabei wird nicht unterschieden, ob diese Systeme virtuell oder physisch sind. Jedoch muss bei virtu-

ellen Systemen angegeben werden, auf welcher Hardware diese laufen. Je nachdem können nun auch die Netzwerke und die genutzten Räume (z.B. Serverräume, Switch-Schränke etc.) in einen Zusammenhang gebracht werden.

Bei der erwähnten Vererbung werden drei Arten unterschieden:

- Maximumprinzip: Dabei wird die höchste Kritikalität übernommen (bezogen je auf die Vertraulichkeit, die Integrität und die Verfügbarkeit).
- Verteilungseffekt: Wenn genügend Redundanzen vorhanden sind, kann z.B. die Verfügbarkeit reduziert werden. Dies ist beispielsweise dann der Fall, wenn Systeme in zwei redundanten Rechenzentren betrieben werden. Damit kann eines ausfallen, ohne dass der Prozess davon negativ beeinflusst wird.
- Kumulationseffekt: Die Kritikalität wird erhöht. Typisch ist dies bei Hardware-Systemen, auf denen eine grosse Anzahl von virtuellen Maschinen betrieben wird. Die einzelnen virtuellen Systeme sind unkritisch, da aber bei einem Hardware-Ausfall viele gleichzeitig ausfallen, wird die Anforderung an die Verfügbarkeit des Servers erhöht.

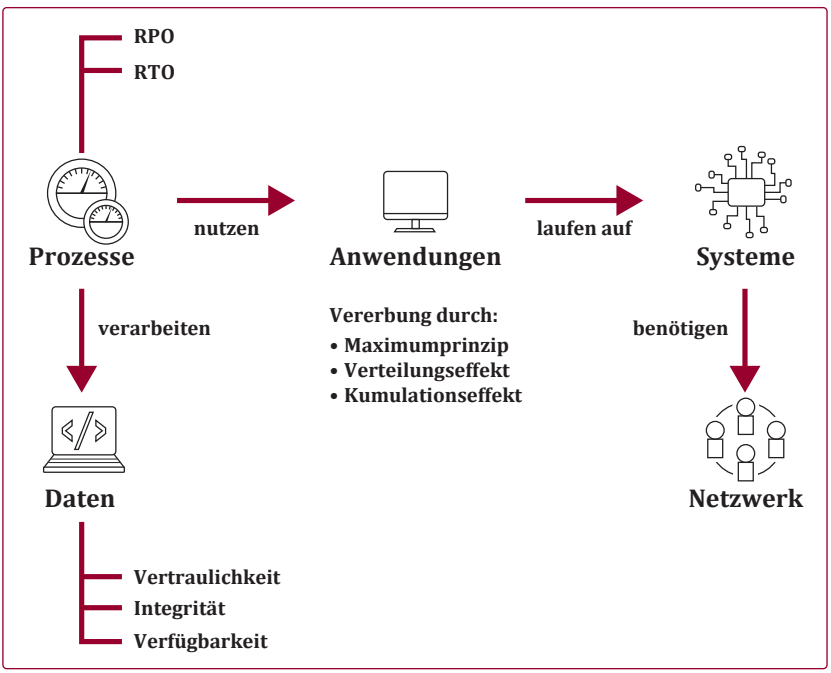

Abbildung 12: Vererbung der Kritikalität

4.4 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 Checkliste:

- sichere Passwörter anwenden (Kombination von Zahlen, kleinen und grossen Buchstaben plus Sonderzeichen, im Minimum zehn, besser zwölf 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 Anhängen und Kurzlinks (E-Mails von Unbekannten löschen, keine Anhänge öffnen und keine Links daraus anklicken)
- Antivirenprogramm nie ausschalten
- Phishing-Angriffe erkennen
- keine Auskünfte an unberechtigte Personen erteilen
- bei seltsamen Vorfällen den Support anrufen

Diese Punkte können z.B. während eines Steh-Lunches oder einer Schulung anhand von Beispielen erklärt werden. Als Abschluss kann ein Flyer verteilt werden. Ein möglicher Flyer ist beispielsweise die Aktion «Geschichten aus dem Internet» (Season 1) sowie «Geschichten aus dem digitalen Alltag» (Season 2 und 3) des Bundesamts für Kommunikation BAKOM. Kostenlos verfügbar unter www.websters.swiss.

Weitere Möglichkeiten sind:

- Schulungen
- Web Based Trainings
- Poster
- E-Mails
- simulierte Phishing-Angriffe
- Videos
- Bildschirm-Hintergrundbilder
- diverse Give-aways
- und viele weitere

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 13: SPiced hAM (Quelle: iStock)

Mit Spam ist in der IT-Welt jegliche Art von unerwünschten E-Mails gemeint. Aktuell sind ca. zwei Drittel aller E-Mails Spam.

5.1.1 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. Wie Google suchen Roboter nach E-Mail-Adressen auf der Webseite oder in Newsforen. 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 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.

5.1.2 Schutz vor Spam

Die einfachste Regel ist, die E-Mail-Adresse gleich vertraulich zu behandeln wie die eigene Postadresse oder die Kreditkartenangaben. 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 Einmaladressdienste. Eine frei definierbare 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 Absenderadresse (IP) auf einer schwarzen Liste, wird der Empfang verweigert (sog. 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 Schwellenwert 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.

Weitere Techniken versuchen, das Virenprogramm 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 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 (sog. 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 aktuellen 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 Geräts. Nur wenn Aktualisierungen für das Handy angeboten und rechtzeitig eingespielt werden, kann der Schutz hochgehalten 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. Dazu kann mit der Maus auf den Link gefahren werden, ohne zu klicken, und die Zieladresse wird angezeigt. Sieht diese anders aus als erwartet, sollte nicht geklickt werden.

5.6 Social Media

Soziale Medien erfreuen sich grosser Beliebtheit, sei dies Facebook, Instagram, TikTok im privaten oder Xing und LinkedIn im geschäftlichen Umfeld. Getweetet, gepostet, gelikt wird ständig und überall. Vielleicht ist diese Information für sich allein 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.

5.7 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 beim 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.

5.8 Spuren im Netz

Heute hinterlässt jeder Klick 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 ergibt 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 zehn bis 50 weitere Webseiten nach. Oft sind dies auch Google, Facebook und weitere soziale Netzwerke. 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 Chrome Plug-in Lightbeam (kostenlos verfügbar).

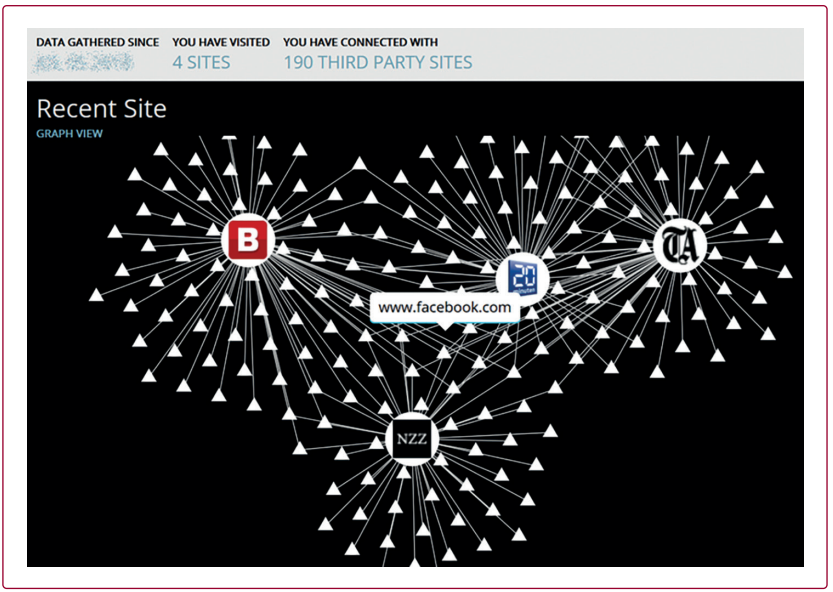

Abbildung 14: Spuren im Netz

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 Verschlüsselung

Verschlüsselung wird der Vorgang genannt, bei dem ein klar lesbarer Text (Klartext, Plaintext) mithilfe eines Verschlüsselungsverfahrens in eine «unleserliche», d.h. 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.

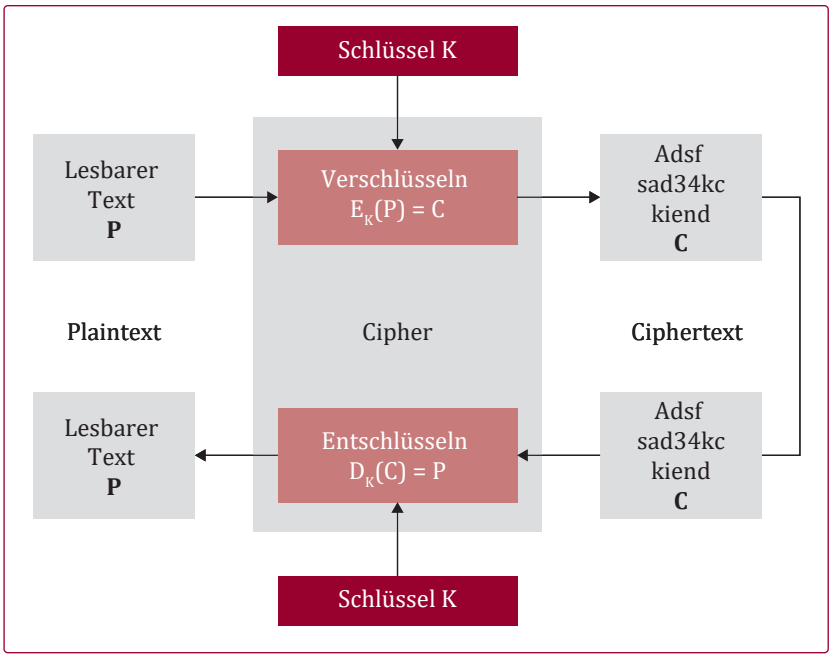

Abbildung 15: Begriffe der Ver- und Entschlüsselung

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.

6.1.1 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 Passworts 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.

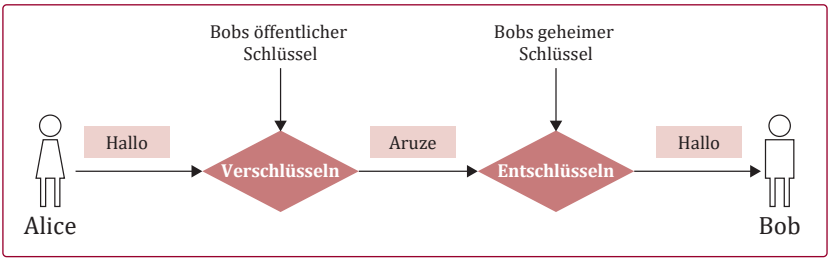

Abbildung 16: Asymmetrische Ver- und Entschlüsselung

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

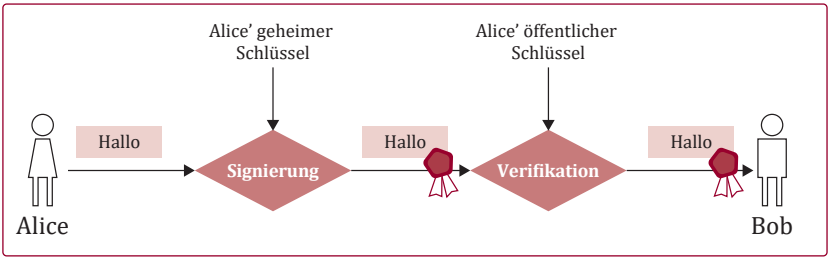

Abbildung 17: Asymmetrische Signierung und Verifikation

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 die Unversehrtheit der E-Mail können mit dem öffentlichen Schlüssel des Senders überprüft werden.

6.1.2 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 immer dann zum Einsatz, wenn Sie eine verschlüsselte Internetseite besuchen (er-

kennbar 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 zwei Jahre gültig und müssen dann erneuert werden (im Gegensatz zu PGP, wo Zertifikate «unendlich» lange gültig sein können). 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.

Zertifikatsinformation

Dieses Zertifikat ist für folgende Zwecke beabsichtigt:
- Garantiert dem Remotecomputer Ihre Identität
- Schützt E-Mail-Nachrichten

- Weitere Infos finden Sie in den Angaben der Zertifizierungsstelle.

Ausgestellt für: Andreas Wisler

Ausgestellt von: SwissSign RSA SMIME NCP exntended ICA 2021-1

Gültig ab 18.7.2022 **bis** 18.7.2025

Sie besitzen einen privaten Schlüssel für dieses Zertifikat.

Abbildung 18: Zertifikat des Autors

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.

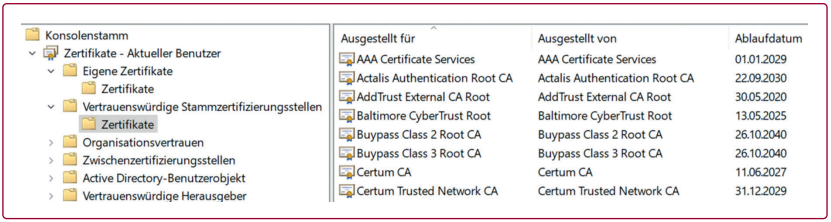

Abbildung 19: Vertrauenswürdige Stammzertifizierungsstellen

6.2 Netzwerksicherheit

Neben den Clients ist auch der Schutz des gesamten Netzwerks 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 Netzwerks dürfen), 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 **Backup**). 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 Sicherheitsbedürfnis oder Problembewusstsein entstehen und dabei das Verständnis geweckt werden, dass die Daten eines Netzwerks 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.

6.2.1 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.

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 zusammenhängenden logischen Datenstrom ein neues Datenpaket zuordnen. Diese Information kann als weiteres Filterkriterium herangezogen werden.
- Eine Application-Level-Firewall beachtet zusätzlich zu den reinen Verkehrsdaten auch noch den Inhalt der Netzwerkpakete. 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.

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 Netzwerkadressen 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

6.2.2 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.

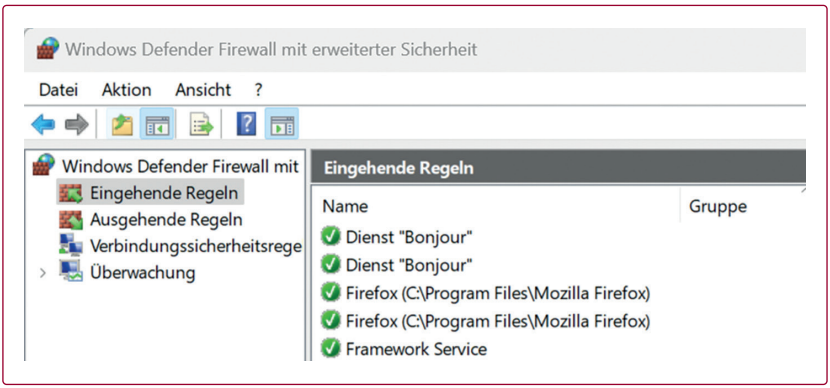

Abbildung 20: Windows-Firewall

Wie bei Windows gilt es auch bei einem Gerät von Apple die Firewall zu aktivieren. Bei Apple ist diese nicht standardmässig aktiv.

6.3 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 nach 15 Minuten nach Bekanntwerden einer Lücken starten. 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.

6.4 Backup/Restore

Das Backup ist die Lebensversicherung für die eigenen Daten. Passiert ein Zwischenfall – z.B. der Ausfall einer Harddisk, ein Brand oder ein versehentliches Löschen von Daten – kann mit Zurückspielen (Restore) des Backups 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.

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 Backup-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 Backups begonnen werden.

6.4.1 Arten des Backups

Die Durchführung des Backups kann auf verschiedene Arten erfolgen:

- Beim Full Backup werden immer alle markierten Daten gesichert.
- Beim differenziellen Backup werden alle Veränderungen seit dem letzten Full Backup gesichert.
- Beim inkrementellen Backup werden nur die Daten gesichert, die seit dem letzten Backup verändert wurden.
- Bei der Synchronisation werden die Daten an zwei Standorten immer auf dem gleichen Stand gehalten.

6.4.2 Lagerung der Datenträger

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

6.4.3 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 Backup-Plans, muss ein Desaster-Recovery (d.h. eine vollständige Wiederherstellung) durchgeführt werden.

6.4.4 Kontrollen

Mit dem Durchführen des Backups allein 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 Bands aus? Welches Medium muss als Nächstes eingelegt werden? Dies sind Fragen, die jeden Tag beantwortet werden müssen.

6.5 Cloud

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

- Bei Infrastructure as a Service (IaaS) wird anstelle des klassischen Kaufs von Rechnerinfrastruktur diese gemietet.
- Bei Platform as a Service (PaaS) ist der Ansatz, eine integrierte Laufzeit- und eventuell auch Entwicklungsumgebung als einen Dienst zur Verfügung zu stellen, für den der Nutzer bei Benutzung zahlen muss.
- 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.

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 (verschiedene Bestrebungen sind seit einigen Jahren da, dies vertraglich zu ändern). 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.

Abkürzungen und Quellen

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
BCM	Business Continuity Management
BIA	Business-Impact-Analyse
CA	Certificate Authority, Zertifizierungsstelle
CISO	Chief Information Security Officer
DSG	Datenschutzgesetz

DMZ	Demilitarisierte Zone
DDoS	Distributed Denial of Service
HTML	Hyper Text Markup Language
http	Hyper Text Transfer Protocol
IS	Informationssicherheit
ISMS	Informationssicherheitsmanagementsysteme
IT	Informationstechnologie
IaaS	Infrastructure as a Service
IKS	Internes Kontrollsystem
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IDS	Intrusion Detection System
KMU	Kleine und mittlere Unternehmen
LAN	Local Area Network, lokales Netzwerk
PDCA	Plan-Do-Check-Act
PaaS	Platform as a Service
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RBL	Remote Black Lists
SLA	Service Level Agreements
SaaS	Software as a Service
SQL	Structured Query Language
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
XSS	Cross Site Scripting

Abbildungsverzeichnis