Nicolas Mayencourt | Marc K. Peter

# IT-SICHERHEIT für KMU

So navigieren Sie
Ihr Unternehmen sicher
durch Cyber-Turbulenzen

Handelszeitung

Beobachter EDITION

# Vorwort

Liebe Leserin, lieber Leser

Mit der zunehmenden Globalisierung und Digitalisierung steigen die Bedürfnisse und Anforderungen an KMU, die IT-Sicherheit in der langfristigen Planung und im Tagesgeschäft zu berücksichtigen. IT-Risiken sind global und machen an der Landesgrenze nicht halt.

Sicherheit gehört zu den Grundvoraussetzungen für eine funktionierende Schweiz. Dazu gehören Bürgerinnen und Bürger, die Verwaltung und Unternehmen. Gerade KMU sind für das Unternehmertum, für die Innovation und als Arbeitgebende ein wichtiger Erfolgspfeiler für die Schweiz und sollten sich deshalb auch auf technologischer Ebene schützen.

Produkte und Dienstleistungen sind vermehrt hoch technologisiert und an das Internet angeschlossen. Fast jedes KMU steht heute in einer Abhängigkeit von der IT, wodurch das Thema IT-Sicherheit auch zu einem Geschäftsleitungsthema wird. Durch die Anbindung an das globale Internet, die Datenspeicherung auf Plattformen von Dritten und die Notwendigkeit von mehreren Softwarelösungen auf einem Computer wird die IT komplex und schwer kontrollierbar.

Als Inhaber, Geschäftsleitende und Abteilungsleitende tragen Sie so auch in Ihrem KMU die Verantwortung, Risiken zu identifizieren und Konzepte zu implementieren, welche die Kundschaft, Mitarbeitenden und Partnerunternehmen in einer digitalisierten Welt schützen.

Mit dem vorliegenden Ratgeber haben die Autoren einen strukturierten Leitfaden erarbeitet, welcher KMU bei der Entwicklung und Realisierung von deren IT-Sicherheit unterstützt. Er hilft den Verantwortlichen, sich im Thema IT-Sicherheit zu orientieren und Hilfestellungen zu finden.

Die IT-Sicherheit ist Bestandteil dieser Grundvoraussetzung für eine funktionierende Schweiz und Ihr KMU. Wir laden Sie ein, Ihren Beitrag zur IT-Sicherheit für Ihr KMU und die Schweiz zu leisten, und wünschen Ihnen viel Erfolg bei der Einführung Ihres IT-Sicherheitskonzepts.

**UELI MAURER**
BUNDESRAT
Vorsteher des Eidgenössischen Finanzdepartements (EFD)

**DORIS FIALA**
NATIONALRÄTIN
Mitglied der Sicherheitspolitischen Kommission des Nationalrats (SiK)

# WLAN und Akku: Die neuen Grundbedürfnisse des Menschen

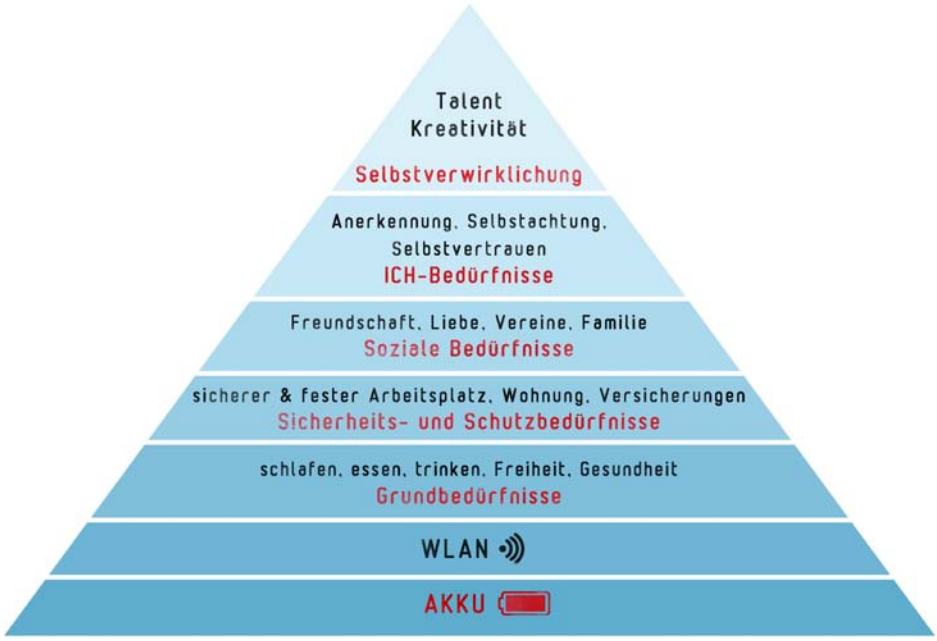
Noch nie wurden so viele Daten übermittelt, archiviert, gespeichert und miteinander vernetzt. Das bringt neben Chancen auch zahlreiche Risiken mit sich.

Gegen Ende der 1990er-Jahre war das Thema IT-Sicherheit eine Randerscheinung, mit der sich lediglich ein paar Tüftler beschäftigten. Das Internet existierte zwar bereits, die meisten Geschäfte wurden aber immer noch analog abgewickelt. Karteikarten und physische Formulare beherrschten den Büroalltag. Häufig gab es in einem Unternehmen gerade einmal einen Computer mit Internetzugriff. Dieser wurde meist von einem einzigen Mitarbeiter bedient, der sämtliche E-Mails beantwortete. Eine Vorstellung, die heute zum Schmunzeln anregt – noch vor 20 Jahren war das allerdings die Realität.

## Von Maschinen abhängig

Im Verlauf der letzten Jahrzehnte hat sich die Bedeutung der Technologie fundamental verändert. Mittlerweile steht in jedem Haushalt in der entwickelten Welt mindestens ein Computer. Die Geräte werden immer kleiner, immer schneller, die Bildschirme immer grösser und höher aufgelöst. Computer haben menschlichen Sinnesorganen nachempfundene Sensoren, Mikrofone, Fingerabdruckleser und Kameras. Sie sind in unseren Hosentaschen, in unseren Büros, Schulen, Sitzungs- und Schlafzimmern, Autos, Haushaltgeräten, Türen, Bahnhöfen, Hallenbädern und Flughäfen. Das Mobiltelefon ist zudem quasi ein Teil unseres Körpers geworden. Unser soziales und berufliches Leben spielt sich darüber ab. Unsere Ausweise, Tickets, Gesundheitsdaten und Zugangscodes sind darauf gespeichert. Sein Besitz hat die Bedeutung eines Menschenrechts. Ohne Mobiltelefon fühlen wir uns geradezu amputiert. WLAN und Akku sind menschliche Grundbedürfnisse geworden.

Nicht nur die Menge der übermittelten, archivierten und gespeicherten Daten wächst mit dieser Entwicklung exponenziell, sondern auch deren Vernetzung. Die Sensoren und Rechner zeichnen laufend Daten auf, die über das Netzwerk übermittelt, aggregiert, miteinander verglichen und ausgewertet werden. Geräte können aus Daten Schlüsse ziehen, Prognosen und Kaufangebote erstellen.




Die Maslow'sche Bedürfnishierarchie, ergänzt mit der Technologie, die heute unser Leben bestimmt.

Doch damit nicht genug. Mehr und mehr überlassen wir den Maschinen auch Entscheidungen. Das ist beispielsweise bereits der Fall bei Aktienkäufen und -verkäufen, bei der Dosierung von Medikamenten oder der Steuerung des Schienenverkehrs. Während die Maschinen immer mehr lernen, wissen wir immer weniger darüber Bescheid, was sie eigentlich tun und wozu sie im schlimmsten Fall fähig wären. Und, was beinahe beängstigender ist: Wir wissen nicht mehr, was wir ohne sie noch selbst tun können. Wir sind von den Maschinen abhängig geworden. Eine funktionierende IT mit Netzanschluss ist zu einem zentralen menschlichen Grundbedürfnis geworden.

## IT-Sicherheit als Managementaufgabe

Die digitale Revolution hat nicht nur das Privatleben, sondern auch die Unternehmenswelt auf den Kopf gestellt. Behörden, Institutionen und Organisationen können ohne technische Unterstützung nicht mehr arbeiten oder sind überhaupt nur dank dieser Technologien aktiv. Entsprechend wird die IT-Sicherheit zur zentralen Managementaufgabe avancieren. Denn wenn die Technologie nicht funktioniert, kann der Laden dichtmachen. Schlimmer noch: Es drohen Gefahren, die über das übliche Geschäftsrisiko hinausgehen.

## IT-Geschichte: Die Welt verändert sich

1936 konstruierte der britische Mathematiker Alan Turing die Turing-Maschine. Sie liess sich zwar nur zum Rechnen nutzen, inspirierte aber die Erfinder John Presper Eckert und John William Mauchly zum Bau des Electronic Numerical Integrator and Computer (ENIAC), der zehn Jahre später auf den Markt kam. Er beanspruchte eine Fläche von 10 mal 17 Metern und wog 27 Tonnen. Der erste Computer war entstanden. Seit damals gab es zahlreiche Erfindungen. Einige Höhepunkte der letzten 50 Jahre:

1941 - Erster programmierbarer Computer wird von Konrad Zuse entwickelt.
1960 - Internetprotokolle TCP/IP werden entwickelt.
1965 - Erste Rechenmaus wird von Douglas Engelbart entwickelt.
1970 - Erste kommerzielle EDV-Anlage entsteht: der IBM 370/45.
1980 - Erster IBM-PC kommt auf den Markt.
1984 - Erste E-Mail wird versendet.
1985 - Windows 1.0 kommt auf den Markt.
- Amiga A1000 wird als typischer Heim-PC vorgestellt.
1990 - Tim Berners-Lee begründet am Cern in Genf das World Wide Web (WWW).
1995 - Microsoft bringt Internet Explorer 1.0 auf den Markt. Innert dreier Monate wird die Software 45 Millionen Mal verkauft.
- WWW besteht bereits aus einer Million Websites.
2000 - Dotcom-Blase platzt: Zahlreiche Start-ups in der IT-Branche wurden zu hoch bewertet – Investoren verlieren viel Geld.
- I-love-you-Virus richtet weltweit Schaden in Milliardenhöhe an.
- Weltweit sind 70 Millionen Computer mit dem Internet verbunden.
2005 - Google Maps geht online.
- YouTube wird lanciert. Ein Jahr später wird es von Google übernommen.
2010 - iPad kommt auf den Markt.
- Knapp 2 Milliarden Menschen nutzen das Internet.
- Über 500 Millionen Menschen nutzen Facebook.
- Instagram wird lanciert.
2015 - 1,5 Milliarden Menschen nutzen Facebook.
- 800 Millionen nutzen WhatsApp.
- 400 Millionen nutzen Instagram.
2020 - YouTube macht weltweit einen Umsatz von 15 Milliarden US-Dollar.
- Es gibt 1,5 Milliarden Websites.
- 4 Milliarden Menschen nutzen das Internet.
- 5 Milliarden Menschen nutzen Mobiltelefone.

## In wenigen Schritten zur angriffssicheren Website

Die folgenden Schritte helfen Ihnen, Ihre Website zu sichern.

**Ändern Sie die Standard-Log-in-Informationen**

Wie in allen anderen Fällen ist es auch bei CMS und Webservern keine gute Idee, den Benutzernamen «Admin» und das Passwort «Passwort» zu verwenden. Sie schmunzeln nun vielleicht, aber schwache Passwörter sind äusserst verbreitet. Verzichten Sie deshalb auf besonders beliebte – und auch häufig gehackte – Passwörter wie: 123456, qwerty, admin, maga2020, LLE1234 oder password. Welche Passwortkombinationen besser sind, erfahren Sie weiter hinten in diesem Buch (siehe Seite 130).


Selbst Mark Zuckerberg nutzte ein unsicheres Passwort: «dadada». Das zeigte ein Facebook-Hack im Jahr 2016.

**Vorsicht bei gemietetem Hosting**

Die Kriterien, nach denen Sie Ihren Webhoster beziehungsweise ein entsprechendes Angebot aussuchen, hängen auch davon ab, welche Rolle Ihre Website im Tagesgeschäft einnimmt. Dient ein Webauftritt lediglich als elektronische Visitenkarte, die potenziellen Kundinnen Ihr Angebot und Portfolio präsentiert, ist ein kurzfristiger Ausfall der Seite wohl weniger geschäftsschädigend, als wenn Sie einen Webshop betreiben und so ab der ersten Ausfallminute Geld verlieren. Von einem IT-Sicherheitsstandpunkt aus betrachtet, ist es am sichersten, über einen eigenen physischen Server zu verfügen. Es ist gleichzeitig aber auch die teuerste Lösung, weil Sie selbst dafür verantwortlich sind, die Technik auf dem neusten Stand zu halten und die Website zu betreiben. Das erfordert nicht nur Zeit, sondern setzt auch viel Fachwissen voraus, dass Sie sich unter Umständen extern einkaufen müssen.

Viele kleinere Unternehmen entscheiden sich deshalb für einen sogenannten Shared Hosting Server. Sie mieten einen bestimmten Platz in einem Serverraum eines Anbieters dieser Dienstleistung. Dort speichern Sie die Datenbank mit allen Texten und Bildern der Website. Hier besteht dieselbe Gefahr wie bei einem externen Buchungsportal: Die Daten sind nicht mehr in Ihrer Kontrolle. Zudem tragen Sie bis zu einem gewissen Grad auch das Risiko der anderen Mieter dieses Anbieters: Im Fall eines Angriffs ist es möglich, dass eine infizierte Website alle anderen ansteckt.

Bevor Sie sich für einen Webhoster entscheiden, sollten Sie deshalb folgende Informationen in Erfahrung bringen:

- **Sicherheitskonzept:** Teilen Sie einen virtuellen Server mit anderen Website-Besitzerinnen oder können Sie Ihren eigenen Server mieten? Die letztere Variante ist zwar etwas teurer, kann sich aber lohnen, wenn Ihre Unternehmens-Website fürs Tagesgeschäft sehr wichtig ist.
- **Back-up:** Wenn ein Server physisch beschädigt wird oder aber Ihrem Website-Verantwortlichen bei der Aktualisierung ein Fehler unterläuft und versehentlich wichtige Daten gelöscht werden, ist es hilfreich, möglichst schnell auf eine ältere Version der Website zugreifen zu können, um sie so rasch wie möglich wieder instand zu setzen. Überprüfen Sie deshalb, wie häufig ein Back-up durchgeführt, wo und für wie viele Tage es gespeichert wird.
- **Support:** Welche Supportmöglichkeiten werden angeboten und sind diese jederzeit oder nur zu Büroöffnungszeiten verfügbar? Auch hier stellt sich die Frage: Wie schnell müssen Sie im Ernstfall dafür sorgen können, dass Ihre Website wieder online ist? Wenn Sie den nächsten Morgen oder den Wochenbeginn abwarten können, wird dieser Punkt weniger entscheidend sein, als wenn Sie im Augenblick, in dem Sie eine Panne bemerken, die Website wieder zum Laufen bringen müssen.

**Achten Sie bei der Auswahl eines Webhosts auf dessen Sicherheitskonzept, das Back-up-Verfahren und die Support-Möglichkeiten.**

**Beschränken Sie die Zugriffsrechte**

Bei Websites oder CMS mit mehreren Benutzern ist es wichtig, dass jeder Nutzer jene Berechtigungen hat, die er benötigt, um seine Arbeit zu erledigen. Wenn Berechtigungen kurzfristig erweitert werden müssen, ist es essenziell, dass dies tatsächlich nur temporär geschieht und nach Abschluss der Aufgabe wieder korrigiert wird. Wenn Sie zudem eine Kollegin haben, die einen Gastbeitrag für Sie schreibt, stellen Sie sicher, dass ihr Konto keine vollständigen Administratorenrechte hat. Das Konto Ihrer Kollegin sollte nur in der Lage sein, neue Beiträge zu erstellen und eigene Beiträge zu bearbeiten. Es ist nicht nötig, dass sie auch die Website-Einstellungen verändern kann.

**Prüfen Sie Plug-ins/Erweiterungen**

CMS sind auch deshalb so beliebt, weil sie individuell erweitert werden können. Es gibt eine riesige Auswahl von Plug-ins, Add-ons und Erweiterungen, die praktisch jede Funktionalität bieten, die Sie sich vorstellen können. Gleichzeitig ist das die grösste Schwachstelle, da alle diese Erweiterungen einen gewissen Zugriff auf Ihre Daten verlangen und selbst Schwachstellen oder gar Malware beinhalten können. Achten Sie deshalb darauf, dass Sie nur Erweiterungen auf Ihrer Website nutzen, die regelmässig aktualisiert werden. Laden Sie alle Ihre Erweiterungen nur aus vertrauenswürdigen Quellen herunter. Es gibt viele Websites, die kostenlose Versionen von zahlungspflichtigen Premium-Plug-ins anbieten. Diese freien Versionen sind Raub-

# Sicheres Arbeiten mit der Cloud

Clouds sind eine beliebte und günstige Lösung, um Daten zu speichern und mit Kollegen zu kollaborieren, bergen aber auch verschiedene Sicherheitsrisiken.


Der Arbeitsplan in der Cloud – ein Beispiel (Trello).

Der Coiffeursalon «Haarschön» speichert unter anderem die Schichtpläne und die Liste mit den Tageseinnahmen online. Das hat den Vorteil, dass alle Mitarbeitenden mit ihren eigenen Geräten jederzeit und von überallher darauf zugreifen können. Dazu loggen sie sich mit ihrem Online-Account (zum Beispiel einem Google-Konto) in die Cloud ein. Das heisst aber auch: Jeder, der die persönliche E-Mail-Adresse und das dazugehörige Passwort eines Mitarbeiters kennt, kann sich Zugriff auf Unternehmensdaten in der Cloud verschaffen.

## Checkliste für sichere Back-ups

Wenn Sie sicherstellen möchten, dass Ihr KMU eine effektive Back-up-Lösung hat, prüfen Sie, folgende Anforderungen:

- ☐ **Redundanz:** Die Daten sollten mehrfach gesichert sein, damit beim Ausfall eines Sicherungssystems auf ein weiteres zugegriffen werden kann.
- ☐ **Mehrere Standorte:** Die Mehrfachsicherung soll an verschiedenen physischen Standorten erfolgen, damit bei Zwischenfällen mit physischen Schäden auf die Daten eines anderen Standorts zugegriffen werden kann.
- ☐ **Mehrere Methoden:** Kombinieren Sie verschiedene Back-up-Methoden und -Medien, um den verschiedenen Datentypen und den jeweiligen Sicherheitsanforderungen gerecht zu werden (Archivdaten, aktuelle Betriebsdaten, Langzeitsicherungs- versus Kurzzeitsicherungsbedürfnisse).
- ☐ **Automatisierung und Alarmierung:** Die Back-up-Überwachung soll automatisiert erfolgen und mit einem Alarmierungssystem verknüpft sein, damit etwa ein unvollständiges Back-up umgehend gemeldet wird.
- ☐ **Überwachung:** Laufende Back-up-Prozesse sollen permanent überwacht werden, damit allfällige Unregelmässigkeiten frühzeitig erkannt und bei Bedarf die Alarmierung und die entsprechenden Massnahmen ausgelöst werden.
- ☐ **Sicherungsprotokolle:** Erstellen Sie Sicherungsprotokolle über die ausgeführten Back-ups in denen festgehalten wird, wer welche Sicherung vorgenommen hat und wo diese gelagert wurde.
- ☐ **Analyse:** Die Sicherungsprotokolle der Back-ups sollen regelmässig daraufhin analysiert werden, ob sie komplett und wiederherstellfähig sind, um so allfällige Schwachstellen frühzeitig zu erkennen.
- ☐ **Simulation:** Die Datenwiederherstellung soll periodisch simuliert und getestet werden, damit sie im Ernstfall die gewünschte Sicherheit bietet und die Abläufe bei den verschiedenen Verantwortlichen klar sind.
- ☐ **Überprüfung:** Überprüfen Sie regelässig die gewählte Back-up-Strategie hinsichtlich ihrer Kompatibilität mit dem aktuellen Geschäftsmodell und passen Sie sie an veränderte Abläufe an. Auch ein Restore-Test – also die Überprüfung, ob die Nutzung eines Back-ups in der Realität funktionieren würde – gehört dazu.
- ☐ **Dokumentation:** Legen Sie eine Dokumentation der aktuellen Back-up-Prozesse an, damit bei Personalmutationen die Abläufe nachvollziehbar bleiben.

# Schweigen ist Silber, Kommunizieren ist Gold

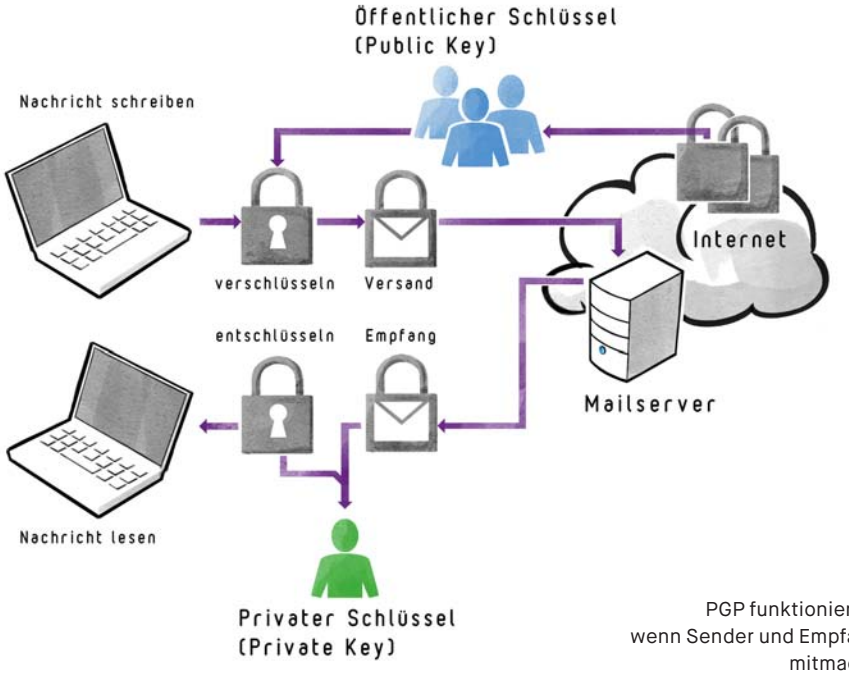
Menschen kommunizieren miteinander und auch Mitarbeitende tun es. Um die IT-Sicherheit zu erhöhen, ist es wichtig, Arbeitnehmende für mögliche Gefahren zu sensibilisieren.

Täglich werden weltweit gegen 300 Milliarden E-Mails versendet. Auch Messaging-Dienste und Voice over IP (VoIP) werden intensiv genutzt – vielfach auch ausserhalb der Kontrolle der IT und ohne Richtlinien für die Mitarbeitenden. Dasselbe gilt für die sozialen Medien, die besonders viele Informationen für potenzielle Hackerangriffe (siehe Seite 48) im öffentlichen Raum preisgeben. Dieses Kapitel zeigt, wie Sie sich und Ihre Mitarbeitenden auf die Gefahren im digitalen Zeitalter vorbereiten und diese reduzieren können.

«Da wir mit sensiblen Daten arbeiten, bitte ich euch, nur über sichere Kanäle mit unseren Kundinnen und Kunden zu kommunizieren», erklärt Daniela Dentalis ihrem Team. «Das bedeutet: Über E-Mail oder Messaging-Dienste solltet ihr keine Auskunft zu medizinischen Fragen geben. Es ist auch nicht in Ordnung, Röntgenbilder per E-Mail zu versenden.» Sie habe einen Onkel, erklärt sie weiter, dessen E-Mail-Adresse beinahe gleich wie ihre lautet. «Regelmässig erhalte ich seine E-Mails, weil sich die Absender vertippen. Da waren schon Unterlagen für eine Hypothek dabei oder Operationsberichte. Alles schützenswerte Daten. E-Mail ist dafür nicht der richtige Kanal. Wir wollen diesbezüglich ein Vorbild sein und bei unseren Kunden einen zuverlässigen Eindruck hinterlassen.»

## E-Mail

Eine E-Mail ist lediglich eine im Klartext verschickte Textdatei und vergleichbar mit einer Postkarte: Sobald sie abgeschickt wurde, kann jeder mitlesen, der Zugriff auf den Datenfluss hat. Viele E-Mail-Anbieter sorgen heute zwar dafür, dass der Transportweg mit SSL-Verschlüsselung gesichert ist. Verlassen sollte man sich darauf allerdings nicht; und in jedem Fall können der sendende und der empfangende Anbieter mitlesen. Es gibt allerdings verschiedene Verfahren, um E-Mails vertraulicher zu gestalten.




PGP funktioniert nur, wenn Sender und Empfänger mitmachen.

Ein Beispiel dafür ist die Verschlüsselung mit «Pretty Good Privacy», kurz PGP. Per PGP lassen sich E-Mails zwischen zwei Personen hinreichend gut («pretty good») verschlüsseln. Sie sind dann sowohl auf dem Server des Anbieters wie auch bei der Übermittlung im Internet vor ungewollten Mitlesenden geschützt. Die Bedingung ist jedoch, dass auch der Empfänger mitmacht.

Die Verschlüsselung funktioniert mit zwei Schlüsseln – einem privaten und einem öffentlichen. Wenn Sie eine E-Mail an Ihren Geschäftspartner senden, verschlüsseln Sie diese mit seinem öffentlichen Schlüssel, den er Ihnen zu diesem Zweck zur Verfügung stellt. Als Empfänger kann er die Mailnachricht nur dann entschlüsseln, wenn er im Besitz des dazugehörigen privaten Schlüssels ist. Eine Möglichkeit, die Angaben zu Ihrem öffentlichen Schlüssel mit Ihren Kunden zu teilen, ist, sie in die Signatur Ihrer E-Mails einzufügen oder aber auf Ihrer Homepage zu publizieren. Oft werden Schlüssel über sogenannte Keyserver wie gnup.org oder openpgp.org ausgetauscht, wovon wir jedoch aufgrund des Missbrauchspotenzials abraten.

**Sensible Daten sollten nicht per E-Mail oder Messaging-Dienste verschickt werden.**

Um den benötigten PGP-Schlüssel zu erzeugen und zu verwalten, benötigen Sie GnuPG, ein freies Kryptografiesystem, das dem Ver- und Entschlüsseln von Daten

dient. Diese Software ist für die meisten Betriebssysteme kostenlos verfügbar. Wenn Sie einen PGP-Schlüssel erzeugt haben, benötigen Sie nur noch eine Mail-Software, die eine solche Verschlüsselung unterstützt. Diese gibt es für Desktop-Systeme wie auch für Mobiltelefone. Allerdings gilt es zu beachten, dass Ihr privater, geheimer Schlüssel auf dem jeweiligen Gerät gespeichert sein muss, auf dem Sie PGP verwenden. Handelt es sich dabei um ein mobiles Gerät, besteht eine gewisse Gefahr, dass das Gerät gestolen wird und damit auch der private Schlüssel in falsche Hände gerät. Das kann gravierende Folgen haben: Wer Ihren privaten Schlüssel stiehlt, kann vertrauenswürdig als Sie handeln. Seien Sie also sehr darauf bedacht, den privaten Schlüssel zu schützen.

### Checkliste: Sicher mailen

- ☐ Behandeln Sie Ihre E-Mail-Adresse vertraulich. Publizieren Sie diese nicht unnötig im Netz oder in sozialen Netzwerken. Ändern Sie entsprechend die Datenschutzeinstellungen.
- ☐ Denken Sie daran, dass Text und Anhänge einer E-Mail etwa so vertraulich sind wie eine Postkarte. Schreiben Sie nur die nötigsten Informationen hinein und versenden Sie keine vertraulichen Daten. Wenn Sie dies müssen, verschlüsseln Sie diese und schützen Sie Dateien mit einem Passwort – zum Beispiel als komprimierte Zip-Datei mit Passwort.
- ☐ Schützen Sie Ihr E-Mail-Postfach mit einem starken Passwort. Ändern Sie dieses regelmässig und speichern Sie es nicht im Browser oder im E-Mail-Programm ab. Professionelle Passwortmanager können genutzt werden. Bedenken Sie jedoch, dass Ihre Passwörter teilweise in der Cloud und somit im Ausland gespeichert werden.
- ☐ Nutzen Sie verschiedene E-Mail-Konten für verschiedene Zwecke; also für berufliche Kommunikation, private Kommunikation, zum Anmelden bei Webdiensten, fürs Online-Shopping oder Newsletter-Abonnements etc.
- ☐ Rufen Sie E-Mails nicht über unsichere, offene, unverschlüsselte WLAN-Verbindungen und öffentliche Computer ab. Die Wahrscheinlichkeit, dass jemand mitliest, ist sehr hoch. Nutzen Sie stattdessen einen VPN-Zugang, um sich sicher im Netz zu bewegen (siehe Seite 44).
- ☐ Wenn Sie einen sehr hohen Schutz wünschen, schalten Sie in Ihrem E-Mail-Programm die automatische Vorschau aus. Laden Sie externe Inhalte wie Bilder in HTML-E-Mails nur bei Bedarf und von vertrauenswürdigen Absendern herunter.
- ☐ Stellen Sie sich bei jeder Nachricht, bevor Sie sie lesen oder Anhänge öffnen, zumindest folgende Fragen: Kennen Sie den Absender? Wie lautet seine

E-Mail-Adresse? Ist diese plausibel? Betrifft Sie der Betreff wirklich? Ist die Nachricht wirklich für Sie gedacht oder klingt Sie eher allgemein? Erwarten Sie von diesem Absender eine Datei? Haben Sie mit diesem Absender normalerweise über E-Mail-Kontakt?

- ☐ Geben Sie niemals Passwörter oder Login-in-Daten ein, wenn Sie in einer E-Mail dazu aufgefordert werden – das ist höchstwahrscheinlich versuchter Datenklau. Geben Sie Ihr Passwort nur auf dem effektiven Portal ein, in das Sie sich einloggen wollen. Die Adresse geben Sie besser selbst ein, als einem Link zu folgen.
- ☐ Klicken Sie nicht auf Links von unbekannten Absendern.
- ☐ Antworten Sie nicht auf offensichtlichen Spam – auch nicht, um dem Absender mitzuteilen, dass Sie damit nicht einverstanden sind. Verzichten Sie bei Spam zudem darauf, auf Unsubscribe-Links zu klicken – damit bestätigen Sie nur Ihre E-Mail-Adresse.
- ☐ Gefälschte Absender erkennen Sie im Header einer E-Mail-Nachricht. Sie sehen diesen, wenn Sie den kompletten Text der Mail anzeigen lassen oder indem Sie auf die «Antwort»- beziehungsweise «Antworten an»-Adresse achten.

## Instant Messenger

Über einen Instant Messenger werden Nachrichten in Echtzeit ausgetauscht: Sobald eine Nachricht verschickt wird, erscheint sie auch schon beim Empfänger. Neben reinen Textnachrichten können über einen Instant Messenger auch Bilder oder Audiodateien verschickt werden; Videotelefonie, Audionachrichten und Unterhaltungen in der Gruppe sind ebenfalls möglich. Neben der bestehenden Internetverbindung fallen in der Regel keine weiteren Kosten für den Versand der Nachrichten an. Bekannte Messenger-Dienste sind unter anderem: WhatsApp, Threema, Telegram, iMessage, Google Hangouts, Signal, Facebook Messenger und Jabber. Messenger-Dienste sind nicht nur im privaten Bereich äusserst beliebt. Auch im Geschäftsumfeld geschieht es häufig, dass, kaum haben Geschäftspartner ihre Mobiltelefonnummer ausgetauscht, die Konversation über WhatsApp oder einen ähnlichen Kanal fortgeführt wird. Sie sollten sich allerdings gut überlegen, welche Informationen Sie über diese Kanäle versenden, denn es gibt drei grosse Risiken im Einsatz von Messenger-Diensten im Geschäftsalltag:

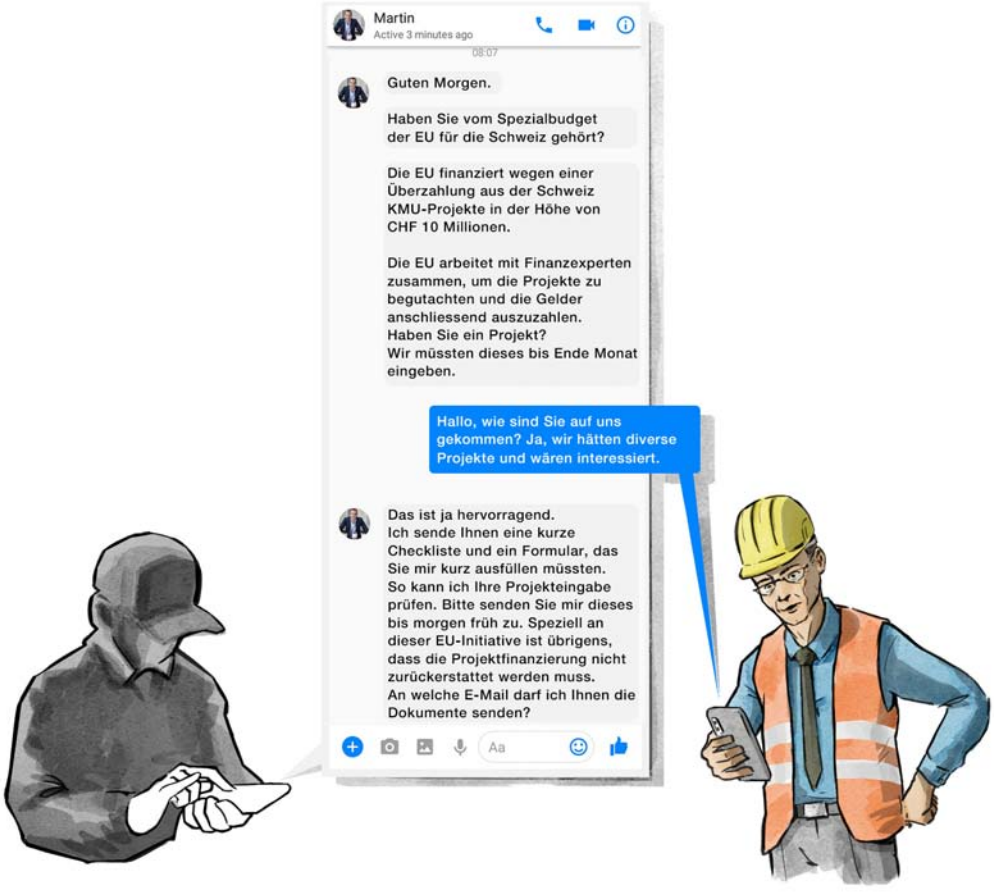
**Datenschutz**
Ein zentrales Problem ist, dass die Anbieter, die meist nicht im selben Land tätig sind wie Sie, die Hoheit über die übermittelten Daten erhalten (siehe Seite 70). Was Sie

**Wenn Sie Geschäftsinformationen via WhatsApp und Co. verschicken, verlieren Sie die Datenhoheit und damit die Kontrolle über Ihre Inhalte.**

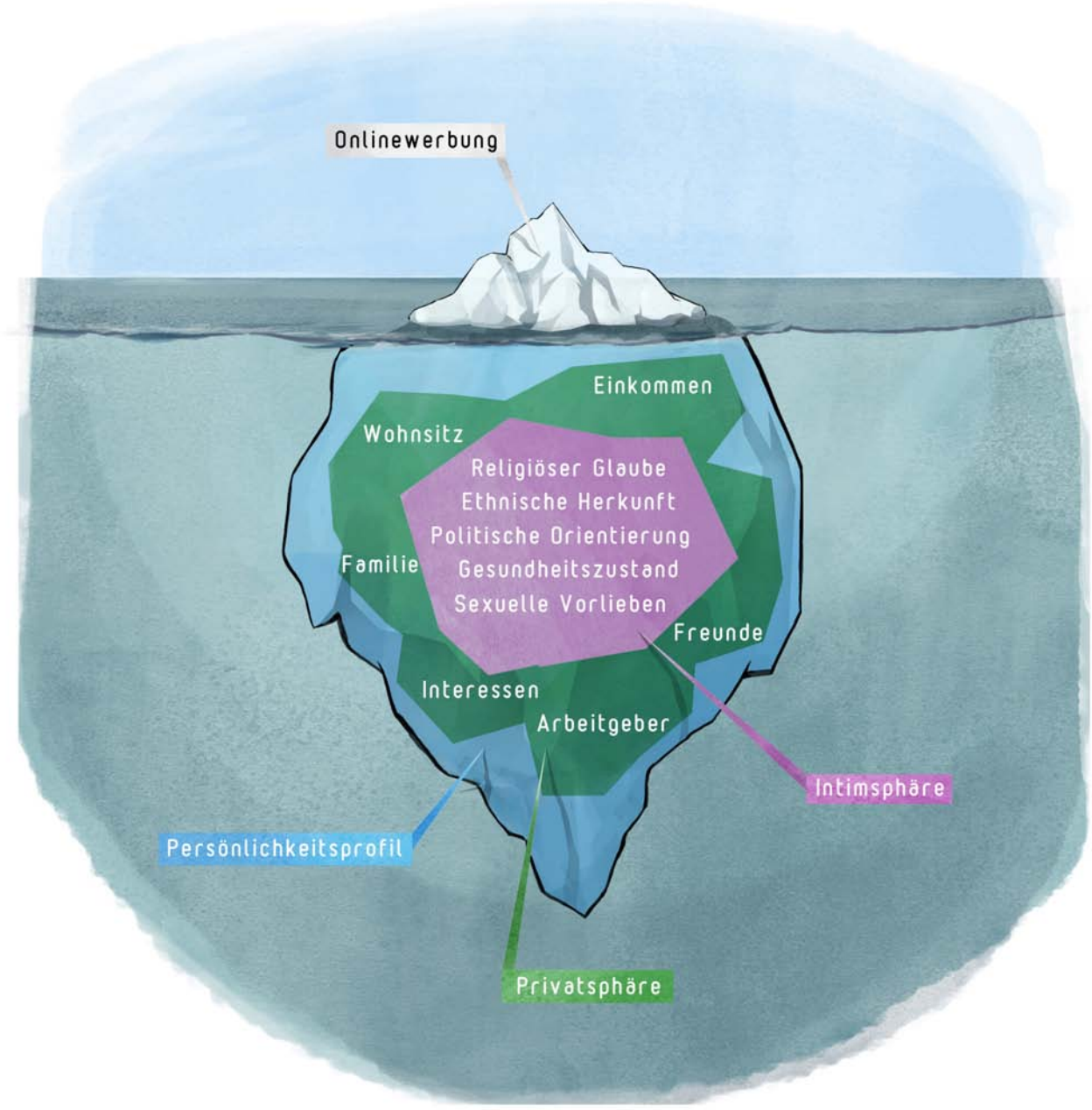
also über einen Messenger übermitteln, gehört nicht mehr Ihnen. Auch die Sicherung der Daten übernimmt der Anbieter. Sie können Ihren Geschäftspartnern somit weder Vertraulichkeit noch Sicherheit der Kommunikation garantieren.

**Malware**

Mit der wachsenden Beliebtheit von Instant Messaging gibt es leider auch immer mehr Schädlinge und Angreifer: Viren, Würmer und Trojaner für Messaging-Systeme nehmen stark zu. Diese Malware wird wie bei den E-Mails über angeklickte Links oder versendete Bilder und Videos übertragen. Durch die Echtzeitfunktion verbreiten sich Würmer und Viren in Netzwerken innerhalb kürzester Zeit.




Versuche, Sie zu unsauberen Geschäften zu verleiten oder auszutricksen, sind auch über Messenger-Dienste beliebt. Es geht dabei vor allem darum, Ihnen Geld zu stehlen.




Beispiel, aus welchen Daten sich ein Persönlichkeitsprofil erstellen lässt.

Die Arbeit im Homeoffice birgt ihre ganz eigenen Gefahren.

dadurch unsicher. Auf USB-Sticks gespeicherte Daten können verloren gehen oder entwendet werden. Es braucht deshalb ein Konzept, das regelt, wo und wie im Homeoffice Unternehmensdaten gespeichert werden dürfen und sollen. Wichtige Firmendaten müssen gesichert, ein Back-up erstellt und alle sensiblen Daten verschlüsselt gespeichert werden. Mögliche Lösungen sind zuverlässige Cloud-Dienste oder der Zugriff auf die Firmenablage via VPN.

## So sind Sie auch im Homeoffice sicher

Damit die IT-Sicherheit auch im Homeoffice von Ihnen und Ihren Mitarbeitenden gewährleistet werden kann, lohnt es sich, folgende Tipps zu befolgen:

**Nutzen Sie eine VPN-Verbindung**
Wenn Sie ein VPN nutzen, werden Daten verschlüsselt übertragen (siehe Seite 44). Zudem können Zugriffe administriert und protokolliert werden. Im Falle eines Missbrauchs oder Datendiebstahls kann schnell rekonstruiert werden, was geschehen ist und wo die Schwachstelle liegt. Konfigurieren Sie die Zugriffsrechte so, dass Mitarbeitende nur jene Daten lesen und bearbeiten können, die sie zum Erledigen ihrer Aufgabe benötigen.

**Kommunizieren Sie nur über Unternehmenskonten**
Nutzen Sie keine privaten Telefone, E-Mail-Konten oder Messenger-Dienste für das Übermitteln von Unternehmensdaten. Diese sind nicht gesichert, oft nicht oder zumindest nicht ausreichend verschlüsselt und leiten in vielen Fällen Ihre Daten an Server im Ausland weiter. Berufliche E-Mails dürfen aus denselben Gründen nicht auf private Postfächer umgeleitet werden. Ebenso wichtig: Vertrauliche Dokumente gehören nicht in den E-Mail-Anhang (siehe Seite 80).

**Öffnen Sie E-Mails nicht im Browser, sondern in Kollaborationssoftware**
Wenn Sie E-Mails direkt im Browser lesen und versenden, besteht eine erhöhte Gefahr, dass eine Angreiferin mitliest. Internetbrowser können zudem eher kompromittiert und manipuliert werden als eine spezialisierte Kollaborationssoftware (siehe Seite 93).

**Beobachten Sie den Datenverkehr**
Halten Sie das Firmennetzwerk im Auge. Protokollieren Sie Zugriffe von aussen, über VPN. Stellen Sie sicher, dass die Mitarbeitenden nur auf Daten zugreifen können, die sie zum Erledigen ihrer Arbeit benötigen. Eine mögliche Lösung ist eine zentrale Firewall im Unternehmen, welche die VPN-Tunnel der Homeoffice-Mitarbeitenden steuert.

**Richten Sie Zugangskontrollen und Schutzmassnahmen ein**
Auch zu Hause können immer wieder Situationen entstehen, in denen Unbefugte Zugriff auf Ihre IT erhalten oder Daten einsehen können – zum Beispiel dann, wenn sich Handwerker in der Wohnung aufhalten oder wenn Sie mit dem Laptop auf dem Balkon arbeiten. Ergreifen Sie in diesen Situationen entsprechende Massnahmen, die Zugriffe und Einblicke verhindern:

- Schützen Sie Ihr Gerät mit einem Passwort und aktivieren Sie diesen Passwortschutz, sobald Sie sich – auch nur kurz – von dem Gerät entfernen.
- Installieren Sie einen Sichtschutz.
- Lassen Sie keine vertraulichen Dokumente und Ausdrucke herumliegen.
- Telefonieren Sie auf dem Balkon nicht über Vertrauliches.

## Der grosse Test: Stellen Sie Ihre IT-Sicherheit auf die Probe

Mit der folgenden Vorlage können Sie den aktuellen Sicherheitszustand Ihrer Unternehmung selbst erheben. Dabei werden Fragen zu sämtlichen in diesem Buch näher beschriebenen Bereichen gestellt. In den entsprechenden Kapiteln im Buch finden Sie Massnahmen und Empfehlungen, die erklären, wie Sie die Sicherheit verbessern können. Sie können jederzeit in diesen Testzyklus einsteigen. Ob Sie mitten im Betrieb sind oder grössere Investitionen in Hard- und Software planen – Sie können damit den aktuellen Zustand oder den zu erwartenden Zustand nach der Investition testen.

Testen Sie Ihr Wissen.

Die Erhebung läuft ganz einfach ab: Immer dann, wenn Sie eine Frage nicht mit einem klaren «Ja» beantworten können, besteht dringender Handlungsbedarf. Verweise in Klammern zeigen Ihnen, wo Sie im vorliegenden Buch weitere Informationen und Tipps zum Thema finden. Denken Sie, wenn Sie die Fragen beantworten, insbesondere an Ihre definierten Schutzziele: Welche Daten Sie also wovor schützen wollen und ob das mit den vorhandenen Massnahmen gewährleistet ist.

**1. Organisation**

- Ist in Ihrem KMU klar definiert, wer für die IT-Sicherheit verantwortlich ist?
- Hat die verantwortliche Person das notwendige Wissen und die Fähigkeiten, um mit IT-Sicherheit umzugehen, und bildet sie sich regelmässig weiter?
- Hat die verantwortliche Person die notwendige hierarchische Stellung und entsprechende Kompetenzen, um IT-Sicherheits-Massnahmen umzusetzen?
- Ist eine Regelung für einen Krisenfall vorhanden? Kann im Fall einer Krisensituation der Betrieb sichergestellt werden?

(→ siehe Seite 122, Business-Continuity-Management)

**2. Sensibilisierung**

- Gibt es Richtlinien für den sicheren Umgang mit IT-Geräten und mit Daten innerhalb Ihres Unternehmens?
- Werden diese Richtlinien und IT-Sicherheitsmassnahmen konsequent und systematisch umgesetzt und regelmässig überprüft?
- Werden die Mitarbeitenden regelmässig geschult und sensibilisiert für den sicheren Umgang mit Daten und Geräten?
- Werden die Mitarbeitenden dazu motiviert, sicherheitsrelevante Vorfälle zu melden – ohne dabei sanktioniert zu werden?

(→ siehe Seite 94, Die Mitarbeitenden sensibilisieren)

**3. Datenschutz**

- Sind Ihnen die gesetzlichen Vorschriften bezüglich Datenspeicherung und -verarbeitung bekannt?
- Kennen Sie und Ihre Mitarbeitenden Ihre Pflichten im Zusammenhang mit den Vorschriften bezüglich personenbezogener Daten?
- Werden die aktuell geltenden Vorschriften zum Datenschutz in Ihrem Betrieb konsequent und korrekt umgesetzt?
- Sind sensible Daten auf Ihren Systemen verschlüsselt?
- Ist in Ihrem Betrieb der physische Zugang zur Rechner-, Server- und Netzwerkinfrastruktur vor dem Zugriff Dritter zweckmässig geschützt?

(→ siehe Seite 98, Datenschutz)

**3. Back-up**

- Wenden Sie einen Daten-Back-up-Prozess an?
- Überprüfen Sie regelmässig die Funktionsfähigkeit und Lesbarkeit des Back-ups?
- Wird das Back-up physisch getrennt abgelegt?
- Ist sichergestellt, dass verlorene oder zerstörte Daten in nützlicher Frist wiederhergestellt werden können? Testen Sie regelmässig, ob das funktioniert?

(→ siehe Seite 72, Back-up)

**4. Netzwerk**

- Kennen Sie Ihr Netzwerk und dessen Aufbau genau?
- Wissen Sie, wo sich was befindet?
- Ist die Netzwerkdokumentation auf dem neuesten Stand?
- Sind die Benutzerinnen und Benutzer Gruppen zugeteilt, die ihrer Funktion entsprechen?
- Werden die Systeme regelmässig durch Software-Updates angepasst?
- Werden alle Änderungen protokolliert?
- Nutzen Sie eine Firewall?
- Haben Sie einen Schutz gegen Malware, Viren und Würmer?

(→ siehe Seite 34, Netzwerke)

**5. Kommunikation**

- Gibt es eine unternehmensinterne Weisung, welche klar beschreibt, welche Daten Sie per E-Mail übermitteln dürfen und welche nicht?
- Werden Ihre E-Mails verschlüsselt?
- Wird Instant Messaging bei Ihnen zu Geschäftszwecken eingesetzt?
- Nutzen Sie VoIP-Telefonie?

(→ siehe Seite 80, Kommunikation)

**6. Zugangsmanagement**

- Stellen Sie die Identifikation, Kontrolle und Administration der Benutzer so sicher, dass alle einer Gruppe zugewiesen sind?
- Nutzen Sie Zwei-Faktor-Authentifizierung?
- Wird der Zugriff auf die Systeme kontrolliert und protokolliert?
- Lassen Sie zu, dass mobile Geräte an das Unternehmensnetz angeschlossen werden?
- Werden mobile Geräte kontrolliert, bevor Sie auf Unternehmensdaten zugreifen dürfen?
  (→ siehe Seite 128, Zugangsmanagement)