it-safe.at

IT Sicherheitshandbuch

FÜR KLEINE UND MITTLERE UNTERNEHMEN

8. Auflage

WKO INFORMATION · CONSULTING

it-safe.at ist eine Initiative der Bundessparte Information und Consulting in der WKÖ (BSIC).

WKO
INFORMATION · CONSULTING

IT Sicherheitshandbuch

FÜR KLEINE UND MITTLERE UNTERNEHMEN

8. Auflage

it-safe.at – das IT-Sicherheitsprojekt für KMU

Impressum

Medieninhaber/Verleger:
Wirtschaftskammer Österreich, Bundessparte Information und Consulting, 1045 Wien,
Wiedner Hauptstraße 63; ic@wko.at, http://wko.at/ic

8. Auflage, Oktober 2017

Für den Inhalt verantwortlich: Friedrich Tuma, Mag. Verena Becker, Mag. Ursula Illibauer, Mag. Hannes Leitner
Basislayout: Birgit Altrichter, Michaela Kock – geschmacksache.at
Grafische Umsetzung: www.designag.at
Druck und Herstellungsort: Grasl Druck und Neue Medien GmbH, 2540 Bad Vöslau

Alle Rechte vorbehalten. Nachdruck – auch auszugsweise – nur mit Quellenangabe und nach vorheriger Genehmigung.
Trotz sorgfältiger Prüfung sämtlicher Beiträge in dieser Broschüre sind Fehler nicht auszuschließen, die Richtigkeit des Inhalts ist daher ohne Gewähr. Eine Haftung der Autoren oder der Wirtschaftskammer Österreich ist ausgeschlossen.

INHALT

1. RISIKOMANAGEMENT 10
Erhebung und Klassifizierung der Unternehmenswerte 10
Erhebung der Bedrohungen und Schwachstellen 11
Planung und Umsetzung von Sicherheitsmaßnahmen 12

2. EINHALTUNG RECHTLICHER VORGABEN 13
Allgemeines 13
Bestimmungen zur Geschäftsführerhaftung (UGB, GmbH-Gesetz) 13
Das österreichische Datenschutzgesetz (DSG 2000) 14
EU-Datenschutz-Grundverordnung und Datenschutzanpassungsgesetz 2018 15
Data Breach Notification Duty 19
Die EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) 21
Das Verbandsverantwortlichkeitsgesetz (VbVG) 21
Bestimmungen zu Aufbewahrungsfristen (DSG, BAO) 22
Bestimmungen im Arbeitsrecht (ARBVG, AVRAG, ABGB) 23
Rechtliche Bestimmungen für den Betrieb einer eigenen Website 24

3. IT-STRATEGISCHE ÜBERLEGUNGEN 27
Outsourcing und Cloud Computing 27
Bring Your Own Device (BYOD) 30
Servervirtualisierung 33
Cyberversicherungen 33

4. PERSONELLE MASSNAHMEN 36
Regelungen für Mitarbeiterinnen und Mitarbeiter 36
Verfahren bei personellen Veränderungen 37
Regelungen für den Einsatz von Fremdpersonal 37
Sicherheitssensibilisierung und -schulung 38
Abwehr von Social Engineering-Angriffen 39
Clear Desk/Clear Screen-Policy 40
Entsorgung von Datenträgern und Papierdokumenten 40
Telearbeit 41

5. COMPUTERSICHERHEIT UND VIRENSCHUTZ 43
Auswahl von Passwörtern 43
Zwei-Faktor-Authentifizierung 44
Rechtestruktur auf Arbeitsplatzrechnern 45
Gefahrenquelle Wechselmedien 46
Verschlüsselung von Arbeitsplatzsystemen 46
Regelmäßige Software-Aktualisierungen 48
Nutzungsverbot nicht-betrieblicher Software 49
Mobile IT-Geräte 50
Nutzung von Cloud-Speicherdiensten 52
Virenschutz 54
Technische Virenschutzmaßnahmen 54
Vermeidung bzw. Erkennung von Viren durch den Benutzerinnen und Benutzer 56
Notfallmaßnahmen im Fall von Vireninfektionen 57
Ransomware und Verschlüsselungstrojaner 58

6. NETZWERKSICHERHEIT 62
Firewalls 62
Personal Firewalls 64
Wireless LAN (WLAN) 65
Gäste-WLAN 67

Festlegung einer Internet-Sicherheitsstrategie 68
Gefahren beim Internet-Zugriff 68
Sicherheit von Web-Browsern 69
Soziale Netzwerke 72

7. DATENSICHERUNG UND NOTFALLVORSORGE 75
Datensicherung 75
Datensicherungskonzept und -planung 75
Geeignete Aufbewahrung der Backup-Datenträger 78
Schriftliche Aufzeichnungen der Konfigurationsdaten 78
Sicherungsvarianten im Überblick 79
Datensicherung bei mobilen IT-Systemen (Notebooks, Smartphones etc.) 80
Notfallvorsorge und -wiederherstellung 81
Erhebung der wichtigsten Anwendungen 81
Notfallvorsorge und eingeschränkter Ersatzbetrieb 82
Notfallwiederherstellung 83

8. BAULICHE UND INFRASTRUKTURELLE MASSNAHMEN 85
Baulich-organisatorische Maßnahmen 85
Schützenswerte Gebäudeteile 85
Zutrittskontrolle 86
Schlüsselverwaltung 86
Empfang 87
Geeignete Aufstellung und Aufbewahrung 87
Brandschutz 88
Handfeuerlöscher (Mittel der Ersten und Erweiterten Löschhilfe) 89
Stromversorgung und Klimatechnik 90
Angepasste Aufteilung der Stromkreise 90
Lokale unterbrechungsfreie Stromversorgung (USV) 90
Klimatisierung 91

9. WKO IT SECURITY EXPERTSGROUP 93

10. GLOSSAR 96

© Foto Weinwurm

VORWORT

Die Digitalisierung eröffnet der Wirtschaft völlig neue Wachstumschancen und Beschäftigungsmöglichkeiten.

Gleichzeitig bedeutet dies eine zunehmende Abhängigkeit von einer funktionierenden IT-Infrastruktur.

In der nunmehr 8. Auflage des IT-Sicherheitshandbuchs finden Sie neben praktischen Hinweisen zu Themen wie Risikomanagement, Computersicherheit und Datensicherung auch einen Überblick über die Regelungen, die mit dem neuen Datenschutzrecht ab Mai 2018 auf Sie zukommen. Sie erhalten auch Antworten darauf, wie Sie mit aktuellen Bedrohungen wie z.B. Erpressungstrojanern umgehen sollen.

Die Bundessparte Information und Consulting (BSIC) hat die Initiative „it-safe.at“ ins Leben gerufen, um vor allem kleinen Unternehmen Hilfestellung im Bereich IT-Sicherheit anzubieten. Sie können ein Mehr an Sicherheit bereits durch einfache und rasch umzusetzende Maßnahmen erreichen!

Denken Sie dabei auch an Ihre Mitarbeiterinnen und Mitarbeiter, für die wir ein eigenes Sicherheitshandbuch zusammengestellt haben. Sie finden beide Handbücher und viele weitere interessante Informationen auf der Webseite www.it-safe.at.

Nutzen Sie das Service der BSIC für die Sicherheit Ihres Unternehmens!

KommR Robert Bodenstein, MBA CMC
Bundesspartenobmann

30
35

EINLEITUNG

Die Bundessparte Information und Consulting (BSIC) will mit der Initiative „it-safe.at“ vor allem kleine und mittlere Unternehmen dabei unterstützen, sich mit IT-Sicherheit und Datensicherheit zu beschäftigen.

IT-Sicherheits-Maßnahmen kosten Zeit und Geld kosten, stehen aber in keiner Relation zu dem Schaden, der eintreten kann. Mehr als ein Viertel der Unternehmen sichern ihre Daten nur anlassbezogen oder sogar nie. Ein kompletter Datenverlust (z.B. aufgrund eines Erpessungstrojaners oder einer defekten Festplatte) kann aber existenzbedrohende Folgen für Unternehmen haben.

Jedes Unternehmen muss für sich selbst entscheiden, welche Risiken bewusst in Kauf genommen und welche Risiken mit technischen und organisatorischen Maßnahmen minimiert bzw. vermieden werden sollen.

Ganz wichtig ist auch die ständige Schulung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter. Zu diesem Zweck gibt es – ebenfalls aus der it-safe.at Reihe – ein eigenes „IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter“, das sich speziell an Computer-Anwenderinnen und -Anwender richtet und eine sinnvolle Ergänzung zum vorliegenden Handbuch für KMU darstellt.

Nutzen Sie auch unser Online-Angebot: Testen Sie unter www.it-safe.at mit unserem Online-Ratgeber it-safe, ob Ihr Unternehmen it-sicher ist!

Mit dem Online-Ratgeber zum Thema Datensicherung erhalten Sie nach wenigen Minuten eine konkrete Auswertung, wie Sie Ihre Daten sichern können!

Wir sind natürlich bemüht unsere Produkte laufend zu verbessern und freuen uns daher über jede Form der Anregung. Senden Sie uns Ihre Ideen und Anregungen an ic@wko.at.

1. Risikomanagement

Durch den Einsatz von IT-Systemen und elektronisch gespeicherten Daten entstehen Risiken, die genauso wie alle anderen unternehmerischen Risiken gezielt behandelt werden müssen. Zu diesem Zweck sollten die folgenden Überlegungen angestellt werden.

Erhebung und Klassifizierung der Unternehmenswerte

Voraussetzung für das IT-Risikomanagement ist eine Erhebung und Auflistung aller Unternehmenswerte im IT-Bereich.

Dazu zählen u.a.

- IT-Systeme (Server, PCs, Smartphones, Tablets, Netzwerkgeräte …)
- Software und Lizenzen
- Infrastruktur (USV-Anlagen, Klimaanlagen, Kommunikationsanlagen, …)
- Informationen (Firmendaten, Kundendaten, Verträge, Datenbanken, E-Mails, Handbücher, …)
- Personelle Ressourcen (Know-how, Ausbildung, Erfahrung, …)

Im nächsten Schritt müssen diese Werte nach ihrem Schutzbedarf klassifiziert werden. Dazu sollten zu jedem einzelnen Unternehmenswert die folgenden Überlegungen angestellt werden:

- Wie lange kann das Unternehmen ohne das betreffende IT-System, die betreffenden Daten, bestimmte Mitarbeiterinnen und Mitarbeiter, etc. überleben? Wie schnell müssen diese Werte wieder verfügbar sein, um ernsthafte Schäden zu vermeiden?
- Welcher Schaden entsteht, wenn die betreffenden Daten in die Hände eines Konkurrenzunternehmens fallen oder eine bestimmte Mitarbeiterin oder ein bestimmter Mitarbeiter zur Konkurrenz abwandert? Welche Probleme sind zu erwarten, wenn bestimmte Informationen öffentlich werden, z.B. an die Presse gelangen?
- Welcher Schaden entsteht, wenn z.B. die Buchhaltung oder die Kundendatenbank aus Versehen, durch Manipulation einer Mitarbeiterin oder eines Mitarbeiters, oder aufgrund eines Virenangriffs falsche Einträge enthält?

Anhand dieser Fragen muss festgelegt werden, welche Werte höchste oder hohe Wichtigkeit für das Unternehmen haben und daher besonders gut geschützt werden müssen. Für weniger wichtige Werte können dagegen schwächere Schutzmaßnahmen ausreichen.

Erhebung der Bedrohungen und Schwachstellen

Bevor für IT-Werte Schutzmaßnahmen geplant werden können, müssen die möglichen Bedrohungen erfasst und realistisch eingeschätzt werden.

Typische Bedrohungen sind

- technische Probleme: Hardware- oder Netzwerkausfälle, Fehlfunktionen der Software, Störungen der Stromversorgung oder Klimatisierung, ...
- organisatorische Mängel: Ungenügende Dokumentation, fehlende Schulungen, ungeklärte Zuständigkeiten, fehlende Richtlinien, ...
- fahrlässiges Benutzerverhalten: Bedienungs- und Wartungsmängel, Nichtbeachtung von Sicherheitsmaßnahmen, fehlendes Sicherheitsbewusstsein, ...
- vorsätzliche Handlungen: Computermissbrauch, Datendiebstahl, Verbreiten von Schadsoftware, Social Engineering, Phishing, ...
- höhere Gewalt: Brand- und Wasserschäden, Blitzschlag, Sturmschäden, ...

Für die einzelnen Unternehmenswerte muss eingeschätzt werden, welche dieser Bedrohungen eintreten könnten und wie wahrscheinlich das Eintreten ist. Daraus lassen sich Schwachstellen ableiten, die durch geeignete Sicherheitsmaßnahmen behoben werden können.

Planung und Umsetzung von Sicherheitsmaßnahmen

In Abhängigkeit von der Klassifikation der Unternehmenswerte und den erhobenen Risiken müssen angemessene und zielgerichtete Sicherheitsmaßnahmen geplant und umgesetzt werden.

Informationssicherheit muss gesamtheitlich betrachtet werden. Einem Risiko sollte in der Regel mit einem Mix aus verschiedenen Maßnahmenbereichen begegnet werden. Bei einer einseitigen, z.B. ausschließlich technischen Herangehensweise, ist es leicht möglich, dass eine Schwachstelle über andere Wege ausgenützt werden kann und das Risiko weiterhin besteht.

Aus den folgenden Bereichen können Maßnahmen vorgesehen werden:

- Bauliche und infrastrukturelle Sicherheit: Zutrittskontrolle, Brand- und Wasserschutz, Klimatisierung, Stromversorgung, Einbruchsschutz, ...
- Personell-organisatorische Sicherheit: Sicherheitsrichtlinien, Geheimhaltungsverpflichtungen, Schulung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter, Notfalldokumentation, Versicherungsschutz, ...
- Technische Maßnahmen: Zugangs- und Zugriffsberechtigungen, Datensicherung, Virenschutz, Firewalls, Verschlüsselung, ...

Die umgesetzten Maßnahmen müssen in laufenden Abständen auf ihre Wirksamkeit, Zweckmäßigkeit und Aktualität geprüft und gegebenenfalls angepasst werden. Bei Auftreten neuer Bedrohungen oder bei größeren Änderungen der IT-Infrastruktur (z.B. beim Ankauf neuer Systeme oder Anwendungen) kann es erforderlich sein, die Risikoanalyse neuerlich durchzuführen.

2. Einhaltung rechtlicher Vorgaben

Eine Reihe von Gesetzen ist auch für den Informationssicherheitsbereich relevant: Das österreichische Unternehmensgesetzbuch, das GmbH-Gesetz, die EU-Datenschutz Grundverordnung, etc. Verschiedene rechtliche Bestimmungen haben zusätzlich Auswirkungen z.B. auf die Festlegung von Aufbewahrungsfristen für Protokolle oder Daten.

ALLGEMEINES

Generell hat nach österreichischem Recht jede unternehmerisch tätige Person die Sorgfalt eines ordentlichen Unternehmers walten zu lassen. Zu dieser Sorgfalt gehört die Beachtung aller maßgeblichen Rechtsvorschriften.

Die Unternehmensleitung muss dazu stets ein genaues Bild der Lage des Unternehmens haben. Daher sollte im Unternehmen eine Struktur mit klaren Verantwortlichkeiten und Berichtspflichten vorgesehen werden, die es ermöglicht, Prozesse im Geschäftsablauf zu steuern.

Dies gilt natürlich auch für den Bereich der IT-Sicherheit, da die Verfügbarkeit der IT-Infrastruktur vielfach eine Grundlage des Geschäftsbetriebs darstellt. Mögliche Maßnahmen und Strukturen zur Verbesserung der IT-Sicherheit werden in den nachfolgenden Kapiteln dargestellt.

BESTIMMUNGEN ZUR GESCHÄFTSFÜHRERHAFTUNG (UGB, GMBH-GESETZ)

Aus den Bestimmungen der oben angeführten Gesetze ergibt sich, dass die Verantwortung für Informationssicherheit grundsätzlich immer bei der Unternehmensführung verbleibt. Sicherheitsrelevante IT-Aufgaben können im Rahmen formeller Festlegungen (z.B. einer IT-Sicherheitspolitik) an einzelne Mitarbeiterinnen oder Mitarbeiter delegiert werden; Das Management trägt dennoch insbesondere für die Einhaltung gesetzlicher Bestimmungen die Letztverantwortung.

DAS ÖSTERREICHISCHE DATENSCHUTZGESETZ (DSG 2000)

Das Datenschutzgesetz 2000 (DSG) regelt den Umgang (= jede Art von Verarbeitung, Speicherung, Weiterleitung, etc…) mit personenbezogenen Daten, das sind Angaben über Personen, deren Identität bestimmt oder bestimmbar ist. Zu „Personen" sind auch juristische Personen und Personengemeinschaften zu zählen; bei den Daten wird u.a. zwischen sensiblen (z. B. Gesundheitsdaten, religiöse oder politische Überzeugung) und nicht-sensiblen Daten (z.B. Adressen, Geburtsdatum, Kundendaten) unterschieden. Auch nicht-sensible Daten müssen – wenn auch in geringerem Ausmaß – geschützt werden.

Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke verwendet werden. Die Datenanwendungen, mit denen sie verarbeitet werden, müssen an das Datenverarbeitungsregister (DVR) gemeldet werden; allerdings zählt das DSG auch eine Reihe von Standardanwendungen auf, für die diese Meldung nicht nötig ist (z.B. Rechnungswesen und Logistik, Kundenbetreuung und Marketing für eigene Zwecke, Personalverwaltung für privatrechtliche Dienstverhältnisse). Den Personen, deren Daten verwendet werden, stehen besondere Rechte (Auskunfts-, Richtigstellungs- und Löschungsrecht) zu.

Zu den wichtigsten Inhalten des DSG zählt die Festlegung bestimmter Datensicherheitsmaßnahmen: Die Daten müssen vor Zerstörung und Verlust und vor ordnungswidriger oder unrechtmäßiger Verwendung geschützt werden.

Folgende Punkte sind explizit angeführt (§ 14 DSG 2000):

- die ausdrückliche Festlegung der Aufgabenverteilung zwischen den Mitarbeitern
- die Bindung der Datenverwendung an einen gültigen Auftrag z.B. eines Vorgesetzten
- die Information und Schulung der Mitarbeiter über ihre Pflichten nach dem DSG und internen Datensicherheitsvorschriften
- die Regelung der Zutrittsberechtigungen zu Räumen, in denen Daten verarbeitet werden
- der Schutz der IT-Systeme und Datenträger vor unbefugten Zugriffen
- der Schutz der IT-Systeme vor unbefugter Inbetriebnahme
- die Protokollierung der Datenverwendung
- die Dokumentation der oben angeführten Sicherheitsmaßnahmen in Form eines Datensicherheitshandbuchs

Aus den Vorschriften des DSG ergeben sich einige typische Anforderungen für den Umgang mit personenbezogenen Daten: Alle Mitarbeiterinnen und Mitarbeiter müssen in Form einer Geheimhaltungsverpflichtung zum Datengeheimnis verpflichtet werden. Sie müssen geschult werden, typischerweise in Form von Seminaren oder Richtlinien. Aufgaben und Kompetenzen müssen durch Stellenbeschreibungen, Organisationshandbücher und andere Anweisungen geregelt werden. Zutritts- und Zugriffsschutzmaßnahmen sowie Protokollierung müssen durch entsprechende, vorwiegend technische Einrichtungen gewährleistet sein.

Obwohl die Sicherheitsmaßnahmen des DSG an sich nur für die Verwendung personenbezogener Daten gelten, haben sie auch für die Verarbeitung anderer (nicht personenbezogener) Daten Bedeutung erlangt. Sie bilden eine Art Mindeststandard, der auch im Umgang mit Finanzdaten, Geschäftsgeheimnissen uÄ nicht unterschritten werden sollte.

EU-DATENSCHUTZ-GRUNDVERORDNUNG UND DATENSCHUTZANPASSUNGSGESETZ 2018

Ab 25. Mai 2018 wird das Datenschutzgesetz 2000 durch die EU-Datenschutz Grundverordnung (DSGVO) und das Datenschutzanpassungsgesetz 2018 ersetzt. Die Datenschutz-Grundverordnung ist zwar als EU-Verordnung in jedem EU-Mitgliedstaat unmittelbar anwendbar, sie enthält jedoch zahlreiche Öffnungsklauseln und lässt dem nationalen Gesetzgeber gewisse Spielräume. Es gibt daher auch eine Novelle des österreichischen Datenschutzgesetzes 2000 (das „Datenschutz-Anpassungsgesetz 2018“). Bis zum 25. Mai 2018 müssen daher alle Datenanwendungen im Betrieb an die neue Rechtslage angepasst werden.

Folgende erste Schritte werden empfohlen[1]:

1. VORBEREITUNG

- **Für die Anpassung an die DSGVO zuständige Personen (intern/extern) nominieren**
  *(**Hinweis:** Jemand sollte sich im Betrieb unabhängig von der Verpflichtung einen Datenschutzbeauftragten zu benennen – siehe unten – um datenschutzrechtliche Fragen annehmen. Die Verantwortung bleibt datenschutzrechtlich bei demjenigen, der die Entscheidung trifft, Daten zu verarbeiten.)*
- **Zeit- und Budget-Planung**
  *(**Hinweis:** Davon ist abhängig, ob eine etwaig notwendige Umstellung im Betrieb ausgelagert werden muss/kann oder nicht.)*

1 weiterführende Informationen finden Sie unter: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Informationen-zur-EU-Datenschutz-Grundverordnung.html

2. STATUS QUO-ERHEBUNG (IST-ZUSTAND) UND ANPASSUNGSBEDARF (SOLL-ZUSTAND)

- **Welche personenbezogenen Daten werden verarbeitet?**
  *(**Hinweis:** Eine Bestandsaufnahme wird sinnvollerweise bereits schriftlich erledigt. so kann man die Ergebnisse bereits für das Verarbeitungsverzeichnis – siehe unten – verwenden.)*

- **Welche Datenanwendungen bestehen?**
  – Welche Standardanwendungen liegen derzeit vor?
  *(**Hinweis:** Standardanwendungen gibt es ab 25. Mai 2018 in dieser Form nicht mehr. Sie müssen jedenfalls im Verarbeitungsverzeichnis protokolliert werden.)*
  – Welche Datenanwendungen sind derzeit im DVR registriert?
  *(**Hinweis:** Das DVR ist mittlerweile bereits exportierbar, dh die gemeldeten Datenverarbeitungen können direkt im Verarbeitungsverzeichnis übernommen werden, siehe auch https://www.dsb.gv.at/dvr-online).*
  – Überprüfen Sie Ihre AGB, Datenschutzerklärungen, Impressum, laufende Verträge, Website-Einstellungen, etc.

- **Erfolgt Profiling?**
  *(**Hinweis:** Bei gewissen Formen des Profilings kommen spezielle datenschutzrechtliche Regelungen zur Anwendung.)*

- **Was sind die Zwecke meiner Datenverarbeitungen?**

- **Was ist die Rechtsgrundlage der Datenverarbeitung?**
  – Liegt eine Einwilligung vor?
  *(**Hinweis:** Überprüfen Sie unbedingt bestehende Einwilligungen!)*

- **Welche sensiblen Daten werden verarbeitet?**

- **Werden Kindern Dienste der Informationsgesellschaft angeboten?**

- **Werden Auftragsverarbeiter (derzeit „Dienstleister“) herangezogen?**
  – Gibt es schriftliche Vereinbarungen für die Auftragsverarbeitung?
  – Weist der Auftragsverarbeiter die erforderliche Zuverlässigkeit auf?

- **Wie werden die Informationspflichten (nach der DSGVO) erfüllt?**

- **Wie werden die Betroffenenrechte (nach der DSGVO) erfüllt?**
  – An wen in meinem Unternehmen können sich betroffene Personen für die Ausübung ihrer Betroffenenrechte wenden?

- **Welche Datensicherheitsmaßnahmen sind vorhanden?**
  *(**Hinweis:** Geschäftsmodelle werden durch die DSGVO nicht „verhindert", aber es wird ein wesentlich größerer Wert auf Datensicherheitsmaßnahmen, auf den Schutz der Daten im Betrieb, gelegt werden.)*

- **Wie ist privacy by design/privacy by default implementiert?**

- **Besteht für meine Datenverarbeitungen eine Dokumentationspflicht?**
  – Wie wird die Dokumentationspflicht erfüllt?

- **Welche Vorkehrungen gegen Datenschutzverletzungen existieren schon in meinem Unternehmen?**
  *(**Hinweis:** Es empfiehlt sich, gewisse „Mustervorgänge" bzw Abläufe im Betrieb zu verankern, damit im Ernstfall Automatismen erfüllt werden können.)*

- **Ist für meine Datenverarbeitungen eine Datenschutz-Folgenabschätzung durchzuführen?**
  – Welche Risiken aus der Datenverarbeitung ergeben sich für die Rechte und Freiheiten der Betroffenen?
  – Wie kann ich den Risikoeintritt verhindern oder zumindest minimieren?

- **Ist eine vorherige Konsultation bei der Aufsichtsbehörde notwendig?**

- **Brauche ich einen Datenschutzbeauftragten?**

- **Welcher Datenverkehr mit dem EU-Ausland besteht und auf welcher Rechtsgrundlage?**

- **Besonderheiten Arbeitnehmerdatenschutz**
  – Überprüfung von Dienstverträgen, Betriebsvereinbarungen, Dienstordnungen, etc.
  – Rechtzeitige Kommunikation mit dem Betriebsrat

- **Wie weise ich nach, dass meine Datenverarbeitungen DSGVO-konform erfolgen?** (z.B. Dokumentation der Einwilligungserklärungen, Verarbeitungsverzeichnis, Dokumentation der ergriffenen Sicherheitsmaßnahmen, Dokumentation der Risikoabschätzung, Protokollierung oder Dokumentation der Weisungen an den Verantwortlichen oder dem Auftragsverarbeiter unterstellte Personen, Dokumentation der Verpflichtung der Mitarbeiterinnen und Mitarbeiter des Auftragsverarbeiters zur Vertraulichkeit, etc.)

3. MASSNAHMENPLAN

- Zeitliche und budgetäre Planung (Priorisierung der Ziele)
- Maßnahmen festlegen
- Maßnahmen umsetzen

Hinsichtlich **Datensicherheit** legt Artikel 32 der DSGVO sehr ähnlich zu den bisherigen Bestimmungen im DSG fest, dass unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen der **Verantwortliche** (*vormals:* datenschutzrechtlicher Auftraggeber) und der **Auftragsverarbeiter** (*vormals:* datenschutzrechtlicher Dienstleister) geeignete technische und organisatorische Maßnahmen treffen müssen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Darunter ist laut DSGVO folgendes zu verstehen:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung,
- Sicherstellung, dass Mitarbeiterinnen und Mitarbeiter und sonstige unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten.

Bei Datensicherheit spielt aber natürlich auch privacy by design und privacy by default eine Rolle. Privacy by design, oder **Datenschutz durch Technikgestaltung**, bedeutet, dass sowohl bei der Planung als auch bei der Datenverarbeitung selbst der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu berücksichtigen haben, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dabei sind der Stand der

Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen (z.B. Pseudonymisierung).

Privacy by default, oder **Privatsphäre durch geeignete Voreinstellungen**, meint, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen hat, die sicherstellen, dass durch entsprechende Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

DATA BREACH NOTIFICATION DUTY

Wenn bekannt wird, dass (personenbezogene) Daten „systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht“, müssen diese Betroffenen unverzüglich informiert werden. Das gilt allerdings nicht, wenn nur ein „geringfügiger Schaden“ zu erwarten ist oder „die Information aller Betroffenen … einen unverhältnismäßigen Aufwand“ erfordert (§ 24 Abs 2a DSG).

Der Datenmissbrauch kann aufgrund der folgenden Ereignisse eintreten:

- Unbefugter Zugriff auf Daten, z.B. durch Außentäter (Hacking-Angriff) oder nicht berechtigte Mitarbeiterinnen und Mitarbeiter
- Diebstahl von IT-Komponenten und Datenträgern (PCs, Notebooks, USB-Sticks, Papierdokumente, Ausdrucke, …)
- Verlust von IT-Komponenten und Datenträgern (Notebooks, USB-Sticks, Smartphones, …)

Zu beachten ist, dass der Schaden nicht bereits eingetreten sein muss. Es genügt die Möglichkeit, dass zukünftig daraus ein Schaden (in finanzieller Hinsicht, in Bezug auf das Ansehen oder hinsichtlich einer körperlichen Gefährdung der Betroffenen) entstehen könnte. Dieser muss allerdings auch schwerwiegend sein, ein voraussichtlich geringfügiger Schaden führt nicht zum Entstehen einer Informationspflicht.

Die Information der Betroffenen kann grundsätzlich in jeder möglichen Form erfolgen. Abgesehen von direkten Kommunikationsformen, z.B. durch Brief- oder E-Mail-Versand, ist auch die Veröffentlichung in Tageszeitungen denkbar. Zu bedenken sind dabei aber die Nachprüfbarkeit der Benachrichtigung (die bei einem eingeschriebenen Brief gegeben ist, nicht aber bei einer E-Mail) und die möglichen negativen Auswirkungen auf den Ruf des Unternehmens, die z.B. bei einer breiten Veröffentlichung in der Zeitung eintreten könnten.

Aufgrund der unklaren Formulierungen der Data Breach Notification Duty ist fallweise abzuwägen, ob und wie der Informationspflicht nachgekommen werden muss. Im Zweifelsfall sollte eine fachkundige Rechtsberatung eingeschaltet werden.

Auch die **DSGVO** sieht die Verpflichtung des Verantwortlichen zur **Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde** vor (Artikel 33), dies möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Wenn dem Auftragsverarbeiter ein data breach bekannt wird, muss er das dem Verantwortlichen unverzüglich melden, damit dieser seinen Meldepflichten nachkommen kann. **Auch die betroffenen Personen müssen informiert werden,** wenn ein **hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen entstanden ist, außer:

- der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen, damit die Daten unzugänglich werden (zB Verschlüsselung),
- der Verantwortliche hat generell sichergestellt, dass das hohe Risiko aller Wahrscheinlichkeit nach nicht mehr besteht, die Benachrichtigung aller einzelnen Personen wäre mit einem unverhältnismäßigen Aufwand verbunden. Achtung: In diesem Fall muss aber stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme erfolgen um die Betroffenen zu informieren.

DIE EU-RICHTLINIE ÜBER MASSNAHMEN ZUR GEWÄHRLEISTUNG EINES HOHEN GEMEINSAMEN SICHERHEITSNIVEAUS VON NETZ- UND INFORMATIONSSYSTEMEN IN DER UNION (NIS-RICHTLINIE)

Mit der NIS-Richtlinie soll EU-weit ein hohes Sicherheitsniveau der Netz- und Informationssysteme erreicht werden. Sie ist am 8. August 2016 in Kraft getreten und muss bis Mai 2018 in allen EU-Mitgliedstaaten in nationales Recht umgesetzt werden.

In Österreich wird die Richtlinie durch ein Bundesgesetz umgesetzt werden. Oberste Ziele dabei sind die Prävention gegen Sicherheitsvorfälle, die Netz-und Informationssysteme betreffen, sowie die Gewährleistung einer raschen und professionellen Reaktion auf solche Sicherheitsvorfälle.

Dabei werden verbindliche Sicherheitsbestimmungen und Berichtspflichten für die „Betreiber wesentlicher Dienste“ festgelegt. Betroffen sind vor allem kritische Infrastrukturen, etwa im Bereich Energie, Verkehr und Banken oder bei der Gesundheits- und Trinkwasserversorgung. Die Betreiber dieser Dienste sind von den Mitgliedstaaten zu bestimmen und werden mittels Bescheid darüber informiert. Kriterien sind zum Beispiel, ob der betreffende Dienst für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten wesentlich ist, und ob ein Sicherheitsvorfall eine erhebliche Störung seiner Bereitstellung bewirken würde.

Auch Anbieter digitaler Dienste wie Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste müssen Maßnahmen ergreifen, um die Sicherheit ihrer Infrastruktur zu gewährleisten. Zusätzlich sind sie verpflichtet, größere Zwischenfälle den nationalen Behörden zu melden. Für Anbieter digitaler Dienste sind die Sicherheits- und Berichtspflichten jedoch weniger streng. Für Unternehmen mit weniger als 50 Mitarbeiterinnen und Mitarbeitern werden diese Verpflichtungen nicht gelten.

DAS VERBANDSVERANTWORTLICHKEITSGESETZ (VBVG)

Das Verbandsverantwortlichkeitsgesetz regelt die Verfolgung juristischer Personen (auch Unternehmen) für Straftaten, die ihre Entscheidungsträger oder Mitarbeiter begangen haben. Es kommt zur Anwendung, wenn eine Straftat entweder zu Gunsten des Verbandes begangen oder wenn sie durch die Unterlassung bestimmter Sorgfaltspflichten ermöglicht oder wesentlich erleichtert wurde. Letzteres ist insbesondere der Fall, wenn Straftaten von Mitarbeiterinnen oder Mitarbeitern nicht durch technische, organisatorische oder personelle Maßnahmen verhindert wurden. Als Strafen sind Geldbußen vorgesehen, die je nach Ertragslage des Verbands und der Schwere des Vergehens bis zu 1,8 Millionen Euro betragen können.

Aus dem VbVG ergeben sich auch verstärkte Anforderungen an die IT-Sicherheitsmaßnahmen eines Unternehmens: Wenn eine Mitarbeiterin oder ein Mitarbeiter eine Straftat unter Verwendung der vom Unternehmen zur Verfügung gestellten IT-Systeme begeht und das Unternehmen die gebotene Sorgfalt zur Verhinderung dieser Tat außer Acht gelassen hat, kann das Unternehmen selbst verfolgt werden. Dazu kann es u.U. ausreichen, wenn die Beschäftigten ihren Internetzugang für den Bezug von Kinderpornographie verwenden und vom Unternehmen keinerlei Vorkehrungen gegen diese Verwendung getroffen wurden.

Zur Abwehr einer strafrechtlichen Verfolgung muss das Unternehmen nachweisen, dass es seinen Sorgfaltspflichten nachgekommen ist. Das ist insbesondere durch die Einführung einer straffen, gut dokumentierten Unternehmensorganisation möglich. Für typische Unternehmensrisiken sollten eigene Verantwortliche eingesetzt und ein Risikomanagement eingeführt werden. Für IT-Risiken bedeutet das im Wesentlichen die Bestellung einer oder eines IT-Sicherheitsbeauftragten und die Erstellung von IT-Sicherheitsrichtlinien bzw. einer IT-Sicherheitspolitik.

BESTIMMUNGEN ZU AUFBEWAHRUNGSFRISTEN (DSG, BAO)

Bei der Archivierung von Daten müssen verschiedene gesetzliche Vorschriften zu Aufbewahrungsfristen beachtet werden. Z.B. schreibt das DSG vor, dass Protokolle, die die Nachverfolgung von Datenzugriffen ermöglichen, drei Jahre aufbewahrt werden müssen. Die Bundesabgabenordnung verlangt, dass Bücher, Aufzeichnungen und Belege sieben Jahre aufbewahrt werden; dies gilt auch für deren Aufbewahrung in elektronischer Form (Buchhaltungsdaten, elektronische Rechnungen, gegebenenfalls auch E-Mails).

Die Verantwortung für die sichere Aufbewahrung und Wiedergabe dieser Daten liegt dabei beim Unternehmen, d.h. eine derartige Langzeitarchivierung muss gut geplant werden: Über den Datenträgerbestand sollte ein Bestandsverzeichnis geführt werden; die archivierten Datenträger müssen regelmäßig geprüft werden; günstigerweise sollte eine Kopie vorliegen, falls das Original unlesbar wird. Vor allem aber muss bei der Planung der Langzeitarchivierung darauf geachtet werden, dass die Daten in einigen Jahren noch nutzbar sind.

Bei einem Wechsel oder einer neuen Version der Buchhaltungssoftware muss geprüft werden, ob die alten Datenbestände verwendet werden können. Andernfalls müssen die Installationsmedien der alten Software aufbewahrt oder besser noch eine betriebsfähige Installation des alten Programms, eventuell auf einem älteren Rechner, beibehalten werden.

BESTIMMUNGEN IM ARBEITSRECHT (ARBVG, AVRAG, ABGB)

Im Zusammenhang mit Arbeitsverhältnissen empfiehlt es sich, sowohl die dienstliche Nutzung der unternehmerischen IT-Infrastruktur zu regeln als auch deren private Nutzung. So können etwa Regelungen und Beschränkungen der Nutzung des Internet und der E-Mail-Infrastruktur getroffen, sowie der angemessene Umgang mit Unternehmens- und Kundendaten festgelegt werden. Immer mehr an Bedeutung gewinnt auch die Nutzung von Social Media, zumal wenn dabei ein Firmenauftritt verwendet oder sonst im dienstlichen Interesse aufgetreten wird oder wenn das private Profil durch die Angabe von Daten mit dem Unternehmen in Verbindung gebracht werden kann.

Regelungen hierzu werden idealerweise bereits bei Beginn des Dienstverhältnisses im Dienstvertrag oder in einem Zusatz zum Dienstvertrag vereinbart. Auch wenn dies verabsäumt wurde, ist eine nachträgliche Dienstanweisung möglich und entsprechend zu beachten. In Betrieben mit Betriebsrat können zudem sowohl Betriebsinhaber als auch Betriebsrat den Abschluss einer Betriebsvereinbarung über die Nutzung der betrieblichen Infrastruktur oder zu allgemeinen Verhaltensvorschriften verlangen.

Bei der dienstlichen Nutzung ist insbesondere an Regelungen zum Schutz der Unternehmens- und Kundendaten und zur Gewährleistung eines reibungslosen Arbeitsablaufs zu denken. Es kann etwa die Einhaltung bestimmter Abläufe bei der Behandlung des Postein- oder -ausgangs festgelegt, Richtlinien zum Öffnen von Anhängen erlassen oder die (Nicht-)Verwendung bestimmter Programme oder Programmversionen angeordnet werden.

Im Bereich der Privatnutzung können Regeln zur und Beschränkungen der privaten Nutzung des Internet oder des dienstlichen E-Mail-Accounts eingeführt werden. In den allermeisten Fällen wird eine begrenzte Privatnutzung des Internet, etwa für e-banking oder zum Surfen während der Ruhepausen erlaubt, grundsätzlich ist aber auch ein gänzliches Verbot der Privatnutzung denkbar. Insbesondere bei dienstlichen E-Mail-Accounts empfiehlt sich zur Vermeidung von Streitigkeiten ein Verbot der Privatnutzung oder zumindest eine Pflicht zur Kennzeichnung von

privaten E-Mails. Im Fall von ungeplanten Abwesenheiten oder bei einem Austritt ist der Zugriff auf dienstliche E-Mails zwar jedenfalls zulässig, private Nachrichten dürfen jedoch weder gelesen noch einfach gelöscht werden.

Darüber hinaus kann die Einhaltung der Anweisungen und Vereinbarungen durch Kontrollmaßnahmen sichergestellt werden. Bei der Kontrolle sind jedoch umfangreiche betriebliche Mitbestimmungsrechte zu berücksichtigen. So bedürfen etwa Maßnahmen, die die Menschenwürde berühren (z.B. Videoüberwachung bestimmter Räumlichkeiten, Protokollierung der Internetzugriffe) jedenfalls der Zustimmung des Betriebsrats. Ist kein Betriebsrat eingerichtet, hat jede einzelne Mitarbeiterin und jeder einzelne Mitarbeiter zuzustimmen. Bei der Wahl der Kontrollmaßnahme ist nach dem Prinzip der Verhältnismäßigkeit vorzugehen und unter den technischen Möglichkeiten das gelindeste zweckentsprechende Mittel zu wählen. Maßnahmen, die die Menschenwürde verletzen (z.B. lückenlose Videoüberwachung, dauernde Ortung des Diensthandys), sind generell untersagt.
Bei der Formulierung von arbeitsrechtlichen Anweisungen und Vereinbarungen ist eine umfassende Beratung im Einzelfall empfehlenswert. Bei Fragen hilft Ihnen gerne Ihre Landeskammer.

RECHTLICHE BESTIMMUNGEN FÜR DEN BETRIEB EINER EIGENEN WEBSITE

Bei der Einrichtung einer eigenen Firmen-Website sind verschiedenste Rechtsmaterien zu beachten. Hier sind nur die Wichtigsten angeführt:

- Das Mediengesetz: Jede Website muss ein Impressum bzw. eine Offenlegung aufweisen, das zumindest Name und Anschrift des Medieninhabers sowie den Unternehmensgegenstand enthält. Abhängig von den veröffentlichten Inhalten können noch zusätzliche Informationen (grundlegende Ausrichtung, Eigentümerstruktur, Vertretungsorgane, Beteiligungen…) notwendig werden.
- Das E-Commerce-Gesetz: Sofern über die Website Online-Geschäfte abgewickelt werden sollen, sind weitere Angaben nach § 5 ECG (Kontaktadressen, Firmenbuchnummer, zuständige Behörden und Vertretungen…) zu machen.
- Das Telekommunikationsgesetz: Wenn Cookies eingesetzt oder Benutzerzugriffe protokolliert werden, müssen die Betroffenen darüber in geeigneter Weise informiert werden. Die Ermittlung dieser Daten darf nur nach Zustimmung der Benutzerinnen und Benutzer erfolgen. Im mindesten Fall müssen ihnen Möglichkeiten angeboten werden, die Datenermittlung zu unterbinden.

- Das Datenschutzgesetz kommt bei persönlichen Anmeldungen und Beiträgen der Benutzerinnen und Benutzer, aber auch bei über die Website erhobenen Daten, z.B. zur Zusendung von Informationsmaterial, ins Spiel. Es ist außerdem hinsichtlich der Verwendung personenbezogener Daten (Cookies, IP-Adressen) zu beachten.
- Das Urheberrechtsgesetz regelt die Nutzung und Kennzeichnung von fremden Inhalten wie Fotos, Filmen, Tonaufnahmen oder Programmcode auf der eigenen Website. Bei Links zu anderen Websites muss erkennbar sein, dass es sich um fremde Inhalte handelt; außerdem dürfen keine geschützten Inhalte zugänglich gemacht werden.

Vor allem dann, wenn Sie über Ihre Website Online-Geschäfte abwickeln wollen, kann die gesetzeskonforme Umsetzung und Gestaltung schwierig werden. Die WKO stellt für diese Zwecke eigene Informationsangebote zur Verfügung. In vielen Fällen kann es aber auch erforderlich sein, professionelle Hilfe in Anspruch zu nehmen.

KONTROLLFRAGEN

- Sind Sie sich Ihrer unternehmerischen Verantwortung im Bereich der IT-Sicherheit bewusst?
- Gibt es in Ihrem Unternehmen eine IT-Sicherheitsbeauftragte oder einen IT-Sicherheitsbeauftragten? Verfügen Sie über dokumentierte IT-Sicherheitsrichtlinien, die den Mitarbeiterinnen und Mitarbeitern kommuniziert und in regelmäßigen Abständen überprüft werden?
- Ist die Verantwortung für Datenschutz in Ihrem Unternehmen eindeutig festgelegt? Wird diese mit der erforderlichen Sachkenntnis und Sorgfalt wahrgenommen? Erfolgt ein angemessener Schutz kritischer Daten und eine Protokollierung der Nutzung?
- Ist der Betrieb auf die Erfordernisse und Neuerungen durch die DSGVO und die Novelle des DSG 2000 bereits geprüft und umgestellt worden?
- Kennen Sie die Aufbewahrungsfristen und Löschungsverpflichtungen für Ihre Branche und kennen Sie die entsprechenden Daten, die in Ihrem Unternehmen anfallen? Können Sie die Aufbewahrungsfristen und Löschungsverpflichtungen erfüllen?
- Sind Sie sich darüber bewusst, dass Sie bei Verlust oder Verdacht auf Missbrauch personenbezogener Daten die Betroffenen informieren müssen?
- Haben Sie arbeitsrechtliche Vorschriften, wie etwa die Privatnutzung des dienstlichen E-Mail-Accounts berücksichtigt?
- Haben Sie bei der Gestaltung Ihrer Website alle gesetzlichen Vorgaben, die für den gesetzeskonformen Betrieb notwendig sind, geprüft und erfüllt?

3. IT-strategische Überlegungen

OUTSOURCING UND CLOUD COMPUTING

Cloud Computing, die Nutzung verschiedener IT-Dienstleistungen über das Internet, ist inzwischen gut etabliert und wird in verschiedenen Formen angeboten. Gerade Klein- und Mittelbetriebe können Kostenersparnisse und oft auch Sicherheitsvorteile erzielen. Zuvor müssen allerdings zentrale Fragen, unter anderem im Sicherheitsbereich, geklärt werden.

Bei Cloud Computing können Unternehmen und Privatpersonen IT-Ressourcen oder Anwendungsdienste eines Service-Anbieters verwenden. Je nach Cloud-Modell werden bloße Infrastruktur (Rechenleistung, Speicherplatz, Netzwerkanbindung), Plattformen (Betriebssysteme, Web-Umgebungen) oder fertige Anwendungen (z.B. für ERP, CRM und BI, aber auch für Office- und E-Mail-Anwendungen) bereitgestellt. Diese Dienste werden vom Service-Anbieter ortsunabhängig und virtualisiert betrieben. Sie können von jedem Ort aus genutzt werden.

Es ist damit häufig möglich, einfache IT-Anforderungen – wenn z.B. ausschließlich Office-Programme und E-Mail sowie eine einfache Buchhaltung betrieben werden –vollständig über einen Cloud-Anbieter abzuwickeln und auf eigene Server zu verzichten. Auch die Ortsunabhängigkeit ist dabei von Vorteil, da auch im Außeneinsatz oder von zuhause auf die Cloud-Dienste zugegriffen werden kann.

Neben den Vorteilen des Cloud Computing-Einsatzes, wie

- **Kostenersparnisse** bei Kapitalinvestitionen sowie unter Umständen bei laufenden Kosten
- **Entlastung oder Einsparung einer eigenen IT-Abteilung**
- **Elastizität und Skalierbarkeit,** da zusätzliche Dienstleistungen kurzfristig zugekauft werden können und auch die Leistung flexibel angepasst werden kann
- **Geschwindigkeitsvorteile,** insbesondere gegenüber veralteter eigener Hardware
- **höhere Verfügbarkeit** im Vergleich zu einem eigenen, kleinen Rechenzentrum

sind aber auch die Risiken zu berücksichtigen, wie

- **Anbieterabhängigkeit,** vor allem beim Wechsel zu einem anderen Service-Anbieter (Lock-in-Effekt), aber auch bei Support und Fehlerbehebung
- **Verlust der Kontrolle** über Daten und Prozesse sowie mangelnde Transparenz
- **Leistungsstörungen** (z.B. Einstellung der Leistung bei Zahlungsverzug)
- **Lizenzfragen**
- **schwierige Rechtsdurchsetzung** gegenüber ausländischen Cloud-Anbietern (insb. in Drittstaaten)
- und vor allem auch Risiken in den Bereichen **Datenschutz** und **IT-Sicherheit**

Unternehmen, die den Umstieg auf Cloud Computing planen, müssen sich des Risikos bewusst sein, dass in der Cloud die Daten und IT-Ressourcen geographisch verteilt sind. Cloud-Nutzerinnen und -Nutzer haben daher oft keine Ahnung, wo sich ihre Daten befinden und ihre Dienstleistungen erbracht werden. Das Ausmaß der Gefährdungspotenziale ist dabei von dem in Anspruch genommenen Servicemodell abhängig.

US-Unternehmen haben mit einem neuen Abkommen, dem Safe Harbor Nachfolger, das EU-US-Datenschutzschild („EU-US-Privacy Shield"), wieder die Möglichkeit, sich in eine vom US-Handelsministerium geführten Liste („Privacy Shield List") eintragen zu lassen, wenn sie sich zur Einhaltung der vereinbarten verbindlichen Anforderungen („Privacy Shield Principles") durch eine Selbstzertifizierung gegenüber dem US-Handelsministerium verpflichten. Seit dem 1. August 2016 können vom US-Handelsministerium Bescheinigungen an diese US-Unternehmen ausgestellt werden, dh der Datentransfer in die USA ist wieder einfacher ohne vorherige Genehmigung zu handhaben. Für österreichische Unternehmer, welche Daten an diese US-Unternehmen übermitteln oder überlassen, kann das eine große Erleichterung darstellen, da eine vorherige Genehmigung der Datenschutzbehörde entfällt.

Dennoch bieten nach der Entscheidung des Europäischen Gerichtshofs (EuGH) in der Sache Max Schrems gegen Facebook Irland, in welcher der EuGH das Safe Harbor - Abkommen zwischen der Europäischen Union und den USA für ungültig erklärt hat, verschiedene Cloud-Anbieter an, Daten ausschließlich in bestimmten Cloud-Rechenzentren innerhalb der EU zu verarbeiten. Der Nachfrage nach einer „europäischen Cloud" wurde Rechnung getragen. Besonders heikel ist die Verarbeitung der sogenannten **sensiblen Daten** in einer Cloud-Umgebung: Nach § 4 Z 2 DSG 2000 sind Daten **natürlicher** Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben besonders schutzwürdig. Diese Daten unterliegen einem allgemeinen Verwendungsverbot, welches nur durch die in § 9 DSG 2000 taxativ aufgezählten Ausnahmen aufgehoben wird.

Die DSGVO führt diese Aufzählung fort (Artikel 9: personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person) und lässt die Verarbeitung ebenfalls in nur sehr eingeschränktem Ausmaß zu. Ähnliches gilt bei strafrechtlich relevanten Daten (Artikel 10). In diesem Fall ist allerdings auch eine Verarbeitungsmöglichkeit im nationalen Datenschutz-Anpassungsgesetz vorgesehen.[1] Abgesehen von diesen Ausnahmen ist

1 siehe hierzu auch EU-Datenschutz-Grundverordnung (DSGVO): Grundsätze und Rechtmäßigkeit der Verarbeitung - Voraussetzungen für die Rechtmäßigkeit der Verarbeitung: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Grundsaetze-und-Rechtmaes.html

die Verarbeitung sensibler Daten nur mit einer ausdrücklichen Zustimmung der Betroffenen möglich. Es stellt sich daher grundsätzlich die Frage, ob sensible Daten überhaupt im Rahmen von Cloud Computing verwendet werden sollen.

Aber auch bei nicht personenbezogenen Daten, die einen hohen Grad an Vertraulichkeit und Integrität erfordern – wie z.B. Rezepturen und andere Geschäftsgeheimnisse, Forschungsdaten u.Ä. –, sollten sich Cloud-Nutzerinnen und -Nutzer überlegen, ob diese Daten wirklich in einer Cloud-Umgebung verwendet werden sollen. Die Verarbeitung von personenbezogenen Daten sowie von Daten, die einen hohen Grad an Vertraulichkeit und Integrität erfordern, ist in einer Cloud nur zu verantworten, wenn der Anbieter genau darlegt, wie seine „Internet-Wolke" im Detail aufgebaut ist.

Vor der Nutzung von Cloud-Technologien sollten Unternehmen daher eine Risikoanalyse durchführen. Bei dieser Risikoanalyse sollte – abhängig vom untersuchten Cloud-Dienst – eine Auseinandersetzung mit folgenden Fragen erfolgen:

- Welche Datenschutz- und Datensicherheitsstandards hat der Cloud-Anbieter umgesetzt?
- Wie ist die Cloud aufgebaut? Wo, d.h. auf welchen Systemen, in welchen Rechenzentren, in welchen Ländern werden die Daten gespeichert?
- Sichert der Cloud-Anbieter zu, dass die Daten nicht in Staaten außerhalb der EU (Drittstaaten) gespeichert und verarbeitet werden?
- Wie gewährleistet der Cloud-Anbieter die Verschlüsselung von Daten (Netzwerk und Speicherung)?
- Wie gewährleistet der Cloud-Anbieter den Zugriffsschutz auf Daten?
- Welche Verfahren zur Information des Auftraggebers werden bei Datenverlust angewandt?
- Wie sehen die Notfallmaßnahmen bei Service-Ausfall aus?

Eine sehr wichtige Rolle bei der Inanspruchnahme von Cloud Computing spielen die Service Level-Vereinbarungen (SLA). Im Rahmen dieser werden Verfügbarkeits- und Performanceanforderungen an den Cloud-Provider vereinbart und in den Dienstleistervertrag eingebunden. Im Zusammenhang mit der Unterschreitung oder sogar Nichterfüllung von SLA sollten entsprechende Pönalevereinbarungen getroffen werden.

Es empfiehlt sich, SLA für folgende Leistungen des Outsourcing-Anbieters zu vereinbaren:

- Verfügbarkeit
- Performance
- Reaktionszeit
- Wiederherstellungszeit
- Wartungszeiten
- Sicherheitsmaßnahmen

Schließlich ist noch zu beachten, dass der Übergang zu Cloud-Computing immer mit einem massiven Kontroll- und Souveränitätsverlust über die eigene IT einhergeht: Sowohl Leistungserbringung als auch Fehlerbehebung liegen vollständig in der Hand des Anbieters, ohne dass der Kunde darauf Einfluss nehmen kann. Dadurch können sich insbesondere im Supportbereich Probleme ergeben, z.B. wenn eine Störung oder ein Fehler nicht zufriedenstellend behoben wird. Auch ein Wechsel des Cloud-Anbieters kann schwierig werden, wenn der bisherige Anbieter keine Unterstützung anbietet und das IT-Fachwissen im eigenen Unternehmen nicht mehr vorhanden ist.

Ein Teil dieser Probleme kann durch entsprechend gestaltete Verträge abgefangen werden, ihre Umsetzung in die Praxis ist aber oft fraglich. IT-Dienstleistungen sollten daher nur zu Cloud-Anbietern ausgelagert werden, deren Geschäftsgestaltung man vertraut. Im Idealfall sollte man zuvor – z.B. im Rahmen eines Pilotprojekts – mit dem Anbieter positive Erfahrungen gesammelt haben.

BRING YOUR OWN DEVICE (BYOD)

Mit „Bring your own device“(„Bring dein eigenes Gerät“) wird die Strategie bezeichnet, Mitarbeiterinnen und Mitarbeitern den Einsatz ihrer privaten IT-Geräte für berufliche Tätigkeiten zu erlauben. Daraus entstehen neue Gefahrenpotenziale und rechtliche Fragen, die im Vorfeld überlegt und geklärt werden müssen.

Aus unternehmerischer Sicht bietet BYOD zunächst eine Reihe von Vorteilen:

- Kosten für neue Hardware können eingespart werden.
- Mitarbeiterinnen und Mitarbeiter sind auch außerhalb der Arbeitszeiten leichter erreichbar.

- Mitarbeiterinnen und Mitarbeiter sind besser motiviert, wenn sie neue Smartphones oder Tablets für ihre Arbeit einsetzen können.
- Mitarbeiterinnen und Mitarbeiter können ihre Geräte selbst aussuchen, ohne auf bestehende Hard- und Software-Angebote des Arbeitgebers angewiesen zu sein.
- Die Notwendigkeit, mehrere Mobilgeräte mit sich zu tragen, entfällt.

Bei näherer Betrachtung relativieren sich diese Vorteile aber oft wieder. Folgende Punkte sind zu bedenken:

- Um für BYOD-Geräte überhaupt Support leisten zu können, müssen die Auswahlmöglichkeiten auf bestimmte Betriebssysteme, Hersteller und Gerätetypen eingeschränkt werden.
- Wichtige Sicherheitsvorgaben, insbesondere die strikte Trennung zwischen privaten und beruflichen Daten, sind ohne zusätzliche kostenpflichtige Software (Mobile Device Management-Programme) nicht umsetzbar. Eventuell müssen aus Sicherheitsgründen auch Umbauten der IT-Infrastruktur (zusätzliche Server für den Remotezugang, Trennung von Netzwerkbereichen) erfolgen.
- Bei Beschädigung oder Verlust des privaten Geräts haftet grundsätzlich der Arbeitgeber, sofern der Schaden aufgrund der dienstlichen Tätigkeit entsteht. Dadurch können hohe Aufwände für die Reparatur oder Wiederbeschaffung entstehen.
- Weitere Kosten können für zusätzliche Softwarelizenzen anfallen, da viele Apps nur dann kostenlos verwendet werden dürfen, wenn sie ausschließlich für private Zwecke genutzt werden.

Die größten Probleme liegen aber im Sicherheitsbereich: Durch BYOD wird die Kontrolle des Unternehmens über die eingesetzte Hard- und Software durchbrochen. Unternehmensdaten werden auf Geräten gespeichert, die von der eigenen IT-Mannschaft nicht verwaltet und überprüft werden können. Die Haftung des Unternehmens für Verletzungen des Datenschutzes oder der Geheimhaltung besteht aber unverändert, gleichgültig, ob die Daten auf BYOD-Geräten oder firmeneigener Hardware liegen. Damit haftet das Unternehmen letztlich für Sicherheitsprobleme auf Geräten, die es kaum kontrollieren kann.

Wenn BYOD eingeführt werden soll, ist daher der Einsatz von Mobile Device Management-Software dringend empfohlen. Damit lassen sich auf den Geräten getrennte private und dienstliche Bereiche einrichten, die separat betrieben und verwaltet werden. Apps für den Privatbereich können weiterhin frei installiert werden, können aber nicht auf betriebliche Daten zugreifen. Im dienstlichen Teil werden dagegen die Sicherheitsvorgaben des Unternehmens umgesetzt.

Wird keine derartige Software eingesetzt, kann die Sicherheit des Unternehmens nur dann gewährleistet werden, wenn sich die Beschäftigten zuverlässig an Vorgaben halten, die sie in der freien Nutzung ihrer eigenen Geräte einschränken. Dies erlegt den Mitarbeiterinnen und Mitarbeitern große Verantwortung auf und darf nur bei entsprechender Sensibilisierung eingeführt werden.

In jedem Fall ist es unerlässlich, noch vor dem Einsatz von BYOD alle Rahmenbedingungen zu prüfen und klare Regelungen einzuführen. Diese sollten zumindest folgende Punkte behandeln:

- Welche Geräte dürfen für BYOD verwendet werden (Hersteller, Gerätetypen, Betriebssystemversionen)?
- Welche Sicherheitsmaßnahmen müssen auf BYOD-Geräten mindestens gesetzt werden (Mobile Device Management-Software, Passwortschutz, Antivirus-Software etc.)?
- Muss eine Mobile Device Management-Software eingeführt werden?
- Welche Apps dürfen installiert werden, welche nicht?
- Welche sicherheitsrelevanten Einstellungen müssen auf den Geräten gesetzt werden?
- Welche nicht-technischen Vorsichtsmaßnahmen sind bei der Arbeit auf BYOD-Geräten zu beachten? Dürfen sie z.B. an Andere verliehen oder in öffentlichen Bereichen genutzt werden?
- Wie ist bei Verlust oder Diebstahl von BYOD-Geräten vorzugehen? Wann muss die Verlustmeldung spätestens erfolgen?
- Welche Unternehmensdaten dürfen auf BYOD-Geräte gespeichert werden?
- Wie können diese Daten gesichert werden? Darf dazu auch Cloud-Speicher verwendet werden?
- Welche Rechte hat die IT-Abteilung? Darf sie BYOD-Geräte überprüfen oder vom Firmennetzwerk ausschließen?
- Wie wird beim Ausscheiden von Beschäftigten mit den Daten auf deren BYOD-Geräten verfahren?

Bitte beachten Sie, dass die Verwendung privater, elektronischer Geräte wie Smartphones, Tablets oder Notebooks zu betrieblichen Zwecken eine Vielzahl von rechtlichen Problemen aufwirft (insbesondere aus den Bereichen Arbeitsrecht, Allgemeines Zivilrecht, Datenschutzrecht, Urheberrecht und Lizenzrecht), auf die hier nicht näher eingegangen werden kann.

SERVERVIRTUALISIERUNG

Servervirtualisierung ist eine Technologie, die es ermöglicht, auf wenigen „physischen" Servern eine Vielzahl „virtueller" Server zu betreiben. Auf diese Weise werden Kosten reduziert und Energie eingespart, indem die enormen Leistungsressourcen moderner Hardware auf verschiedene „virtuelle Maschinen" aufgeteilt werden.

Viele Serveranwendungen (wie z.B. der Betrieb eines Mailservers oder Domänencontrollers) verbrauchen nur sehr wenig Rechenleistung. Die Serverhardware wird bestenfalls in Form kurzer Lastspitzen beansprucht, über weite Strecken bleiben die Ressourcen ungenützt. Durch Virtualisierung können die bisherigen Einzelserver als virtuelle Maschinen auf einem physischen Server zusammengefasst werden. Dadurch sinken die Stromkosten für Serverbetrieb und Klimatisierung sowie die Hardwarekosten. Leistungseinbußen sind in den meisten üblichen Anwendungsfällen nicht zu bemerken.

Ein weiteres wichtiges Argument für Servervirtualisierung ist die Möglichkeit, Hochverfügbarkeitslösungen zu realisieren: Mehrere physische Server lassen sich so miteinander verbinden, dass sie automatisch den Betrieb der virtuellen Maschinen eines ausgefallenen Systems übernehmen. Ausfallszeiten können auf diese Weise mit geringem Zusatzaufwand minimiert werden. Virtualisierungssoftware wird einerseits als eigenständiges Produkt mit breitem Funktionsumfang angeboten. In allen aktuellen Serverbetriebssystemen sind aber bereits entsprechende Funktionen enthalten, die oft völlig ausreichen und keine Zusatzkosten verursachen.

Servervirtualisierung ist inzwischen eine gut ausgereifte und verbreitete Technologie, die in IT-Umgebungen aller Größen eingesetzt wird. Sie erfordert allerdings ein relativ hohes Maß an Know-how und Erfahrung. Insbesondere für die Ersteinrichtung und Einführung eines derartigen Systems ist daher das Beiziehen eines sachkundigen Partners zu überlegen. Der weitere Betrieb kann dann von den eigenen IT-Mitarbeiterinnen und -Mitarbeitern betreut werden.

CYBERVERSICHERUNGEN

Selbst wenn Unternehmen umfangreiche Maßnahmen treffen, gibt es 100% Sicherheit im IT-Bereich leider nicht. Auch in Österreich bieten Versicherungen daher immer mehr Produkte an, um Cyberrisiken „auszulagern". Ein entsprechender Versicherungsschutz kann hier eine wichtige Vorsorgemaßnahme für Unternehmen darstellen. Dabei ist es wichtig, großen Augenmerk auf das optimale Versicherungsprodukt zu legen.

Wenn Hacker bei einem Online-Webshop Kreditkartendaten stehlen, eine DDos-Attacke einen Betrieb tagelang lahmlegt oder sämtliche Unternehmensdaten durch einen Erpressungstrojaner verschlüsselt werden, sind oft hohe finanzielle Schäden die Folge. Betroffen sind Unternehmen jeder Größe und Branche. Cyberversicherungen sollen im Ernstfall die Kosten für die Wiederherstellung der IT-Systeme, Wiederbeschaffung der Daten, Kosten durch Betriebsstillstand und Schäden an Dritten z.B. durch Verstoß gegen Datenschutzvorschriften oder unbewußte Weitergabe von Schadsoftware decken.

Die Versicherungen setzen sich aus einer Haftpflichtversicherung und einer Eigenschadenversicherung zusammen. Sie sind modular aufgebaut und können daher auf das Unternehmen abgestimmt zusammengestellt werden.

- Das Deckungsmodul Cyber-Krisenmanagement stellt dem Versicherungsnehmer im Schadenfall einen Experten zur Seite, der den Versicherungsnehmer bei der Erforschung von Schadensursache, Abwehr und Minderung des Schadens unterstützt.
- Das Deckungsmodul Cyber-Erpressung bietet Schutz vor Erpressung im Zusammenhang mit einer bereits erfolgten oder angedrohten Cyber-Attacke. Davon kann auch die Bezahlung von Lösegeld bei einem Angriff durch Ransomware erfasst sein.
- Das Deckungsmodul Cyber-Kreditkartenschaden zielt auf Unternehmen die Bankdaten von Kunden verwalten oder Vereinbarungen mit Kreditkartenunternehmen haben, ab.
- Durch das Deckungsmodul Cyber-Betriebsunterbrechung wird ein durch Betriebsunterbrechung entstandener Vermögensschaden gedeckt.
- Die Cyber-Haftpflichtversicherung zielt auf Haftungsansprüchen von Dritten ab. Dabei geht es um reine Vermögensschäden inklusive immaterieller Schäden, z.B. durch Datenschutzverletzungen. Der Versicherungsschutz umfasst typischerweise auch die Abwehr von Haftungsansprüchen und Versicherungsschutz im Straf- und Verwaltungsstrafverfahren.

Was ist beim Abschluss einer Cyberversicherung zu beachten:

- Bestehende Produkte am Markt unterscheiden sich oft in wesentlichen Details. Die Auswahl des optimalen Versicherungsschutzes ist schwierig. Vor dem Abschluss ist eine entsprechende Risikoanalyse wichtig, um den konkreten Versicherungsbedarf für das individuelle Unternehmen zu ermitteln und so das optimale Produkt auszuwählen.
- Vorsicht ist dabei geboten, ob das Versicherungsprodukt Obliegenheiten (z.B. Kontrollpflichten der Unternehmensleitung) für den Versicherungsnehmer enthält, die den Versicherungsschutz gefährden. Bei großen Unternehmen können z.B. „Stand der Technik“-Klauseln oder ein entsprechendes IT-Krisenmanagement vereinbart werden.

- Typischerweise wird das Vermögen des versicherten Unternehmens durch eine Cyberversicherung nicht gedeckt. Dadurch fallen z.B. geleistete Zahlungen aufgrund von Cyberbetrug (z.B. CEO-Fraud) nicht unter den Versicherungsschutz.
- Der Antrag selbst erfolgt für kleine und mittlere Unternehmen meist unkompliziert mit einem einseitigen Formular, für große Unternehmen gibt es detailliertere Risikofragebögen.

Wichtig ist, dass die Risikofragen, vor allem betreffend Datensicherung wahrheitsgetreu beantwortet werden.

Es versteht sich von selbst, dass die Cyberversicherung kein „Allheilmittel" ist. Sie kann entsprechende IT-Sicherheitsmaßnahmen sinnvoll ergänzen, aber niemals Ersatz dafür sein.

KONTROLLFRAGEN

- Sind Sie sich der Risiken bewusst, die bei der Auslagerung von IT-Services auftreten können?
- Kennen Sie die datenschutzrechtlichen Vorgaben, die zu beachten sind, wenn Sie Daten zu einem Dienstleister (insbesondere außerhalb der EU) auslagern?
- Haben Sie mit dem externen Dienstleister Service Level-Vereinbarungen abgeschlossen? Wurden dabei auch Ihre spezifischen Sicherheitsanforderungen berücksichtigt?
- Ist die Verwendung von Privatgeräten für berufliche Tätigkeiten (BYOD) in Ihrem Unternehmen erlaubt? Wurden alle dafür notwendigen Regelungen erstellt?
- Ist eine Cyberversicherung für Ihr Unternehmen sinnvoll? Falls ja, sind die unternehmensspezifischen Risiken hinreichend gedeckt?

4. Personelle Maßnahmen

IT-Sicherheit kann auch bei besten technischen Maßnahmen nur funktionieren, wenn die Mitarbeiterinnen und Mitarbeiter ausgeprägtes Sicherheitsbewusstsein besitzen und in der Lage sind, die Vorgaben in der täglichen Praxis umzusetzen. Schulung und Sensibilisierung für Fragen der IT-Sicherheit sind daher unbedingt notwendig.

REGELUNGEN FÜR MITARBEITERINNEN UND MITARBEITER

Bei der Einstellung von Mitarbeiterinnen und Mitarbeitern sind diese zur Einhaltung einschlägiger Gesetze, Vorschriften und interner Regelungen zu verpflichten.

Es empfiehlt sich, Regelungen zu folgenden Bereichen zu treffen, die in Form einer Verpflichtungserklärung zu unterzeichnen sind:

- Einhaltung der **PC-Benutzungsregeln**
- Einhaltung der **Regeln für die Benutzung von Internet und E-Mail**
- Einhaltung der **Verpflichtungserklärung auf das Datengeheimnis** (§ 15 DSG 2000, Artikel 32 Abs. 4 DSGVO und § 6 DSG)

Neue Mitarbeiterinnen und Mitarbeiter müssen unbedingt auf interne Regelungen, Gepflogenheiten und Verfahrensweisen im IT-Einsatz hingewiesen werden. Ohne entsprechende Einweisung kennen sie ihre Ansprechpersonen in Sicherheitsfragen nicht und wissen nicht, welche IT-Sicherheitsmaßnahmen einzuhalten sind.

In die Stellenbeschreibungen müssen alle sicherheitsrelevanten Aufgaben und Verantwortlichkeiten explizit aufgenommen werden. Dies gilt besonders für Mitarbeiterinnen und Mitarbeiter mit speziellen Sicherheitsaufgaben (Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, Applikations- und Projektverantwortliche, ...).

Bei der Einstellung von IT-Administratorinnen und Administratoren ist besondere Sorgfalt nötig: Sie haben weitgehende und umfassende Befugnisse, insbesondere sind sie in der Lage, auf alle Daten zuzugreifen, sie zu verändern und Berechtigungen so zu vergeben, dass erheblicher Missbrauch möglich ist. Das hierfür eingesetzte Personal muss sorgfältig ausgewählt werden und absolut vertrauenswürdig sein.

VERFAHREN BEI PERSONELLEN VERÄNDERUNGEN

Bei personellen Veränderungen, insbesondere beim Ausscheiden von Mitarbeiterinnen und Mitarbeitern aus dem Unternehmen, sollten folgende grundlegende Punkte beachtet werden:

- Sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (z.B. Mobilgeräte, Speichermedien, Dokumentationen) sind zurückzufordern.
- Sämtliche Zugangsberechtigungen und Zugriffsrechte müssen angepasst, entzogen oder gelöscht werden. Dies betrifft unter anderem auch Berechtigungen für eventuelle Telearbeitszugänge sowie Daten auf privaten Smartphones oder Notebooks.
- Wenn eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt wurde (z.B. mittels eines gemeinsamen Passwortes), muss nach Ausscheiden einer der Personen die Zugangsberechtigung sofort geändert werden. Wenn Administratorinnen und Administratoren oder andere Schlüsselpersonen ausscheiden, müssen auch alle anderen Passwörter geändert werden, die ihnen bekannt waren.
- Die Neuvergabe eines bestehenden Benutzerkontos an neue Mitarbeiterinnen oder Mitarbeiter sollte möglichst vermieden werden.

REGELUNGEN FÜR DEN EINSATZ VON FREMDPERSONAL

Betriebsfremde Personen wie z.B. Personal von Reinigungsfirmen oder IT-Dienstleistern können leicht Zugang zu vertraulichen Unternehmensdaten erhalten und stellen unter Umständen eine erhebliche Bedrohung dar.

Einige einfache Regeln sollten beachtet werden, um vertrauliche Informationen zu schützen:

- Externe Mitarbeiterinnen und Mitarbeiter, die über einen längeren Zeitraum in einem Unternehmen tätig sind und Zugang zu vertraulichen Unterlagen und Daten erhalten könnten, müssen schriftlich (im Rahmen von **Geheimhaltungsverpflichtungen**) auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen verpflichtet werden.
- Für Fremdpersonal, das nur kurzfristig oder einmalig zum Einsatz kommt, gelten die gleichen Regeln wie für Besucherinnen und Besucher, d.h. dass etwa der Aufenthalt in sicherheitsrelevanten Bereichen **nur in Begleitung** von unternehmenseigenem Personal erlaubt ist.
- Ist es nicht möglich, betriebsfremde Personen ständig zu begleiten oder zu beaufsichtigen, sollten zumindest die **persönlichen Arbeitsbereiche abgeschlossen** werden (Schreibtisch, Schrank; Abmeldung/Sperre am PC).

SICHERHEITSSENSIBILISIERUNG UND -SCHULUNG

Um die IT-Sicherheit zu verbessern, sollten alle Mitarbeiterinnen und Mitarbeiter über angemessene Kenntnisse im Umgang mit IT-Systemen und den Gefahren und Gegenmaßnahmen in ihrem eigenen Arbeitsgebiet verfügen. Es liegt in der Verantwortung der Geschäftsführung, durch geeignete Schulungsmaßnahmen die nötigen Voraussetzungen zu schaffen. Darüber hinaus sollten alle Benutzerinnen und Benutzer dazu motiviert werden, sich auch in Eigeninitiative Kenntnisse anzueignen.

Die überwiegende Zahl von Schäden im IT-Bereich entsteht durch Nachlässigkeit oder Bequemlichkeit. Das Aufzeigen der Abhängigkeit des Unternehmens von Informationen und vom reibungslosen Funktionieren der IT-Systeme ist ein geeigneter Einstieg in die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für Sicherheitsanliegen.

Weitere mögliche Inhalte einer Benutzerschulung sind:

- Der richtige Umgang mit Passwörtern
- Richtiges Verhalten beim Auftreten von Sicherheitsproblemen
- Der Umgang mit personenbezogenen Daten
- Wirkungsweise und Arten von Schadprogrammen
- Erkennen eines Befalls mit Schadprogrammen
- Sofortmaßnahmen im Verdachtsfall und Maßnahmen zur Entfernung von Schadprogrammen
- Das richtige Verhalten im Internet
- Das richtige Verhalten bei unzulässigen Anfragen
- Risiken bei der Verwendung mobiler IT-Geräte und Datenträger
- Die Bedeutung der Datensicherung und ihrer Durchführung

TIPP:

Verwenden Sie für Benutzerschulungen und zum Selbststudium das „IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter“ aus der it-safe-Reihe (kostenlos unter www.it-safe.at erhältlich).

ABWEHR VON SOCIAL ENGINEERING-ANGRIFFEN

Als Social Engineering bezeichnet man das Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten.

Social Engineering-Angriffe werden meistens über das Telefon, gelegentlich aber auch über soziale Netzwerke oder durch persönliches Auftreten des „Social Engineers" geführt: Angreifer geben sich als Mitarbeiter, Kunden oder IT-Fachkräfte aus und überzeugen ihre Gesprächspartner durch geschickte Täuschung von ihrer vorgetäuschten Identität. Bei geeigneter Gelegenheit – oft erst nach mehrmaligen Telefonaten – gelangen sie so an Informationen, die die Opfer üblicherweise nie herausgeben würden. Gute Social Engineers können unvorbereitete Mitarbeiterinnen und Mitarbeiter zu verschiedensten unerlaubten Handlungen, insbesondere zu Verstößen gegen Sicherheitsauflagen und -richtlinien bewegen.

Social Engineering-Angriffe sind häufig erfolgreich, weil sie menschliche Eigenschaften und Schwächen gezielt ausnützen: Hilfsbereitschaft und Höflichkeit, Kundenfreundlichkeit, aber auch Autoritätshörigkeit und Angst. Einige Maßnahmen können aber helfen, das Risiko zu verringern:

- **Schulungen** über Social Engineering-Strategien und -Methoden helfen den Mitarbeiterinnen und Mitarbeitern, sich auf Angriffe dieser Art vorzubereiten.
- Alle Mitarbeiterinnen und Mitarbeiter müssen sich regelmäßig den **Wert der** von ihnen **bearbeiteten Daten** bewusstmachen, insbesondere hinsichtlich des Schadens, der entstehen kann, wenn sie in falsche Hände geraten.
- **Schriftliche Festlegungen,** welche Informationen vertraulich behandelt werden müssen und welche auch an Unbekannte weitergegeben werden dürfen, können Benutzerinnen und Benutzern zur Orientierung dienen und dem Unternehmen außerdem als Argumentationshilfe nach Sicherheitsvorfällen nützlich werden.
- Festlegungen zur **Anfragenform** sind empfehlenswert: Das Anfordern einer Rückrufnummer oder einer schriftlichen Anfrage kann den Social Engineer unter Umständen bereits abschrecken und gibt den betroffenen Mitarbeiterinnen und Mitarbeitern Gelegenheit zur Nachfrage. Auskünfte zu sensiblen Daten sollten generell nur bei persönlichem Erscheinen erteilt werden.
- Besonders neuen Mitarbeiterinnen und Mitarbeitern sollte empfohlen werden, **Anfragen**, bei denen sie unsicher sind, ob deren Beantwortung zulässig ist, an Vorgesetzte oder andere erfahrene Personen **weiterzuleiten**.
- **Mitarbeiterkommunikation** ist wichtig: Bei „verdächtigen" Anfragen sollten auch die anderen Mitarbeiterinnen und Mitarbeiter informiert werden, um zu verhindern, dass ein abgewiesener Angreifer sein Glück bei anderen, zugänglicheren Kolleginnen und Kollegen versucht.

CLEAR DESK/CLEAR SCREEN-POLICY

In ungesicherten Arbeitsumgebungen hilft eine Clear Desk-Policy beim Schutz vertraulicher Dokumente und Daten vor unbefugten Zugriffen.

Alle Mitarbeiterinnen und Mitarbeiter sollten bei Abwesenheit vertrauliche Unterlagen verschließen. Dies gilt insbesondere für Großraumbüros, aber auch in anderen Fällen ist dafür Sorge zu tragen, dass keine unberechtigten Personen (Kundinnen und Kunden, Besucherinnen und Besucher, Reinigungspersonal, unbefugte Mitarbeiterinnen und Mitarbeiter, etc.) Zugriff auf Schriftstücke oder Datenträger mit sensiblen Inhalten haben. Ähnliches gilt auch für die Computer: Beim Verlassen des Arbeitsplatzes muss sich jede Benutzerin und jeder Benutzer vom PC abmelden. Wenn nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann der Computer stattdessen gesperrt werden. Zusätzlich sollte auch eine automatische Sperre bei Nicht-Nutzung, z.B. durch einen passwortgeschützten Bildschirmschoner, vorgesehen werden.
Es sollte darauf geachtet werden, dass den Mitarbeiterinnen und Mitarbeitern ausreichende Möglichkeiten zum Versperren der sensiblen Arbeitsunterlagen zur Verfügung stehen. Alle Benutzerinnen und Benutzer müssen außerdem über die Tastenkombinationen (z.B. „Windows-Taste + L“) zum schnellen Sperren des PCs informiert werden. Falls möglich, sollten besonders in der ersten Zeit auch Kontrollen und wiederholte Aufforderungen erfolgen, um die Durchsetzung dieser Anweisungen zu sichern.

ENTSORGUNG VON DATENTRÄGERN UND PAPIERDOKUMENTEN

Datenträger und Dokumente mit vertraulichen Inhalten müssen auf sichere Art entsorgt werden.

In vielen Unternehmen stellt der Umgang mit Dokumenten ein Sicherheitsrisiko dar. Dokumente mit vertraulichen oder personenbezogenen Inhalten werden mit dem Altpapier entsorgt, ohne vorher unlesbar gemacht zu werden. Ähnliches gilt für nicht mehr gebrauchte Datenträger wie z.B. defekte Festplatten, Sicherungsbänder oder USB-Sticks.

Unbefugte Personen können auf einfache Art an sensible Daten gelangen, indem sie Altpapiercontainer durchsuchen und entsorgte Datenträger wieder lesbar machen. Daher müssen entsprechende Sicherheitsmaßnahmen befolgt werden:

- Die Mitarbeiterinnen und Mitarbeiter müssen über das Entsorgungskonzept informiert und insbesondere darüber in Kenntnis gesetzt werden, welche Dokumente nicht über das Altpapier entsorgt werden dürfen.

- Papierdokumente müssen mit einem handelsüblichen Shredder oder über ein Entsorgungsunternehmen vernichtet werden.
- Eine ausreichende Anzahl von Entsorgungsmöglichkeiten in erreichbarer Nähe der Mitarbeiterinnen und Mitarbeiter sowie Ansprechpartner für Rückfragen im Zweifelsfall sollten vorgesehen werden.
- Datenträger müssen auf sichere Art vernichtet werden: Sicherungsbänder werden geshreddert, Festplatten müssen physisch zerstört werden (durch Aufschrauben und Zertrümmern der einzelnen Plattenscheiben).
- Bei Festplatten und Wechseldatenträgern ist zudem der Einsatz von Löschprogrammen ratsam, die ein sicheres Löschen der Daten gewährleisten.
- Die Vernichtung der Datenträger kann auch durch ein entsprechendes Entsorgungsunternehmen erfolgen, wobei jedenfalls eine Bestätigung der Vernichtung zu verlangen ist.

TELEARBEIT

Unter Telearbeit versteht man Tätigkeiten, die räumlich entfernt vom Standort des Arbeitgebers durchgeführt werden und deren Erledigung durch eine kommunikationstechnische Anbindung an die IT-Infrastruktur des Arbeitgebers unterstützt wird.

Bestimmte Anforderungen sollten möglichst noch vor der Einrichtung und Vergabe von Telearbeitszugängen überlegt und definiert werden. Z.B. sollte ein Telearbeitsplatz immer in einem eigenen, von der übrigen Wohnung getrennten Zimmer eingerichtet werden, Versperrmöglichkeiten für Datenträger und Dokumente müssen zur Verfügung stehen, etc.

Für die verwendeten Computer müssen ebenfalls bestimmte Auflagen erteilt werden: Aktuelle Virenschutzsoftware ist unbedingt nötig, ebenso der Einsatz eines Zugriffsschutzes durch Benutzeranmeldung und Passworteingabe. Soweit das umsetzbar ist, sollte eine Liste von Software erstellt werden, die auf dem Telearbeit-PC aus Sicherheitsgründen nicht betrieben werden darf. Werden diese Auflagen nicht eingehalten, darf der Telearbeitszugang nicht vergeben oder muss wieder entzogen werden.

Oft ist es günstiger, den für die Telearbeit verwendeten PC vom Unternehmen bereitzustellen. In diesem Fall sollte schriftlich festgelegt werden, dass der Rechner ausschließlich für die berufliche Nutzung verwendet werden darf und dass andere Personen keinen Zugang erhalten dürfen. Auch die Festlegung der Softwareausstattung des Telearbeit-PCs und die Vereinbarung zusätzlicher Kontrollrechte des Arbeitgebers sind in solchen Fällen einfacher möglich. Ähnliches gilt natürlich auch für Mobilgeräte wie Smartphones oder Tablets, wenn diese für Telearbeit verwendet werden. Falls für

diesen Zweck eigene Geräte der Mitarbeiterinnen und Mitarbeiter verwendet werden, müssen die Überlegungen in Kapitel 3 zu BYOD berücksichtigt werden: Sofern nicht eine eigene Mobile Device Management-Software eingesetzt wird, um die IT-Sicherheit des Mobilgeräts zu steuern, müssen die Mitarbeiterinnen und Mitarbeiter entsprechende Vorgaben des Unternehmens zu allen sicherheitsrelevanten Einstellungen einhalten. Weitere Regelungen, z.B. zur Durchführung regelmäßiger Datensicherungen, zu Sicherheitsmaßnahmen bei sensiblen Daten oder zum Vorgehen bei Problemen, sollten zu einer schriftlichen Richtlinie zusammengefasst werden, die allen Telearbeiterinnen und Telearbeitern übergeben wird.

KONTROLLFRAGEN

- Haben alle Mitarbeiterinnen und Mitarbeiter PC-Benutzungsregeln, Regeln für die Benutzung von Internet und E-Mail und eine Verpflichtungserklärung auf das Datengeheimnis unterzeichnet? Werden neue Mitarbeiterinnen und Mitarbeiter mit den Sicherheitsbestimmungen im Unternehmen vertraut gemacht?

- Wurden Regeln hinsichtlich der Sicherung der Arbeitsumgebung (z.B. Verschließen vertraulicher Unterlagen) und der Nutzung und Aufbewahrung mobiler IT-Geräte (z.B. Verschließen, Verschlüsseln) festgelegt und den Mitarbeiterinnen und Mitarbeitern kommuniziert?

- Gibt es ausreichend dimensionierte Dokumentenshredder oder Sammelcontainer von Entsorgungsunternehmen im Unternehmen? Sind sie für alle betroffenen Mitarbeiterinnen und Mitarbeiter leicht erreichbar und werden sie zur Entsorgung aller sensiblen Dokumente und Datenträger genutzt?

- Ist ein dokumentiertes Verfahren beim Ausscheiden von Mitarbeiterinnen und Mitarbeitern hinsichtlich sicherheitsrelevanter Maßnahmen, wie etwa dem Löschen von Zugangsberechtigungen und Zugriffsrechten vorgesehen?

- Werden Mitarbeiterinnen und Mitarbeiter über Social-Engineering Attacken und die Sensibilität der von Ihnen bearbeiteten Daten geschult? Gibt es eine schriftliche Festlegung der vertraulich zu behandelnden Datenarten und kennen alle Mitarbeiterinnen und Mitarbeiter eine Ansprechperson für Rückfragen im Zweifelsfall?

- Wurden Regeln über die Verpflichtungen von Fremdpersonal und den Umgang der Mitarbeiterinnen und Mitarbeiter mit diesen Personen festgelegt und kommuniziert?

5. Computersicherheit und Virenschutz

Die folgenden Punkte behandeln wesentliche Maßnahmen der Computersicherheit. Sie sollten unbedingt umgesetzt werden, um den grundlegenden Schutz der IT-Systeme zu gewährleisten.

AUSWAHL VON PASSWÖRTERN

Passwörter haben grundlegende Bedeutung beim Schutz der IT-Systeme und Daten. Die richtige Auswahl und der richtige Umgang mit Passwörtern können über die Sicherheit vor unbefugten Zugriffen und Manipulationen entscheiden.

Passwörter müssen ausreichend komplex sein, um nicht erraten werden zu können.
Einige Grundregeln sollten dabei unbedingt beachtet werden:

- **Namen,** Vornamen, Geburtsdaten, tel. Durchwahlen, KFZ-Kennzeichen etc. dürfen **nicht** verwendet werden. Sie sind leicht ausfindig zu machen und werden bei Versuchen, ein Passwort zu erraten, mit Sicherheit getestet.
- Passwörter sollten **nicht** aus Begriffen bestehen, die in einem **Wörterbuch** (auch einer anderen Sprache) aufzufinden sein könnten. Programme, die zum Auffinden von Passwörtern verwendet werden, nützen Wortlisten mit mehreren tausend Begriffen, um Passwörter dieser Art innerhalb kürzester Zeit zu entschlüsseln. Auch Eigennamen, geografische Begriffe, etc. sollten möglichst vermieden werden.
- **Trivialpasswörter** (aaaaaa, qwertz, asdf, 123456, 08/15, 4711, ...) dürfen nicht verwendet werden. Abgesehen davon, dass solche Passwörter in jeder Wortliste vorkommen, können sie durch Beobachten der Passworteingabe leicht erraten werden.
- Das Passwort muss **ausreichend lang** sein. Für die Konten normaler Benutzerinnen und Benutzer muss es mindestens zehn Zeichen lang sein, für Benutzerkonten mit besonderen Rechten (Administrator, root, Dienstkonten etc.) sollte ein Passwort mit zumindest zwölf Zeichen gewählt werden.
- Ein Passwort muss aus **verschiedenen Arten von Zeichen** zusammengesetzt sein. Großbuchstaben, Kleinbuchstaben, Ziffern und/oder Sonderzeichen (Satzzeichen, Währungssymbole etc.) müssen miteinander kombiniert werden, um ausreichende Sicherheit zu erhalten. Nur ein oder zwei Zeichenarten zu verwenden, reduziert die Sicherheit des Passworts erheblich!
- Passwörter – insbesondere das Passwort bei der Anmeldung am Computer – dürfen **nicht an andere Personen** weitergegeben werden. Auch Kolleginnen und Kollegen oder Vorgesetzten dürfen Passwörter nur in absoluten Notfällen mitgeteilt werden; anschließend sollten sie sofort geändert werden.

- Für **verschiedene Anmeldungen** müssen **verschiedene Passwörter** eingesetzt werden. Auf keinen Fall darf z.B. für die Anmeldung am PC und das E-Mail-Konto beim Internet-Provider das gleiche Passwort verwendet werden. Auch für verschiedene Cloud- und Webdienste (Dropbox, Facebook, E-Banking, ...) müssen unterschiedliche Passwörter gewählt werden. Bei geringem Sicherheitsbedarf kann es ausreichen, kleine Variationen einzufügen, z.B. einige Buchstaben zu ändern.

Passwörter sollten **in regelmäßigen Abständen geändert** werden (z.B. alle 90 Tage). Sie sollten aber auf jeden Fall immer dann geändert werden, wenn der Verdacht besteht, dass sie Unbefugten bekannt sind. Alle Mitarbeiterinnen und Mitarbeiter müssen wissen, auf welche Weise sie ihr Passwort ändern können.

Wenn viele unterschiedliche Passwörter eingesetzt werden, können diese auch mit Hilfe eines **Passwort-Managers** verwaltet werden. Solche Programme verwenden ein **Master-Passwort**, um gespeicherte Passwörter zu schützen. Dieses Master-Passwort muss selbstverständlich besonders sorgsam ausgesucht werden und den oben angeführten Kriterien entsprechen. Sofern Ihre IT-Systeme durch einen externen Servicepartner gewartet werden, sollten alle eingesetzten Administratorpasswörter an einem sicheren Ort hinterlegt werden (verschlossenes Kuvert im Firmensafe). Diese müssen selbstverständlich aktuell gehalten werden.

ZWEI-FAKTOR-AUTHENTIFIZIERUNG

Für besonders sensible oder gefährdete Einsatzzwecke, z.B. dem Fernzugriff auf Unternehmensdaten, kann Zwei-Faktor-Authentifizierung den Schutz vor unbefugten Zugriffen deutlich erhöhen.

Bei einer Zwei-Faktor-Authentifizierung muss ein Benutzer bei der Anmeldung über zwei getrennte Erkennungsmerkmale verfügen, um seine Identität nachzuweisen. Ein typisches Beispiel dafür ist die Bankomat-Anmeldung, für die sowohl die Chipkarte als auch ein PIN-Code benötigt werden.

Meistens handelt es sich bei diesen zwei Erkennungsmerkmalen um eine Zeichenfolge, die nur der richtige Benutzer kennt (Passwort, PIN-Code etc.) sowie ein Gerät (Chipkarte, Hardware-Token etc.), das nur dieser Benutzer besitzt. Durch diese Kombination sind unbefugte Zugriffe selbst dann unmöglich, wenn der Angreifer das Passwort kennt. Nur durch den Nachweis beider Komponenten kann die Benutzeranmeldung erfolgen.

Eine weitere Möglichkeit besteht darin, dem Benutzer ähnlich wie beim E-Banking via SMS-Nachricht einen zufällig generierten Code zuzusenden. Dieser muss noch mit einer kurzen Zeichenfolge, die nur dieser Benutzer kennt, kombiniert werden, um ein Einmal-Passwort zu bilden. Der Vorteil dieser Variante ist, dass auf teure oder verlustträchtige Zusatzhardware verzichtet werden kann.

Für den alltäglichen Betrieb bzw. den Einsatz am Unternehmensgelände ist Zwei-Faktor-Authentifizierung meistens zu umständlich oder zu teuer. Für den Fernzugriff auf das Unternehmen, d.h. für Telearbeit oder im mobilen Einsatz, ist dieser Aufwand dagegen angemessen, wenn geheime oder sensible Daten verarbeitet werden. In solchen Fällen ist eine Absicherung über einfache Passwörter oft nicht sicher genug. Mit Zwei-Faktor-Authentifizierung kann der Schutz deutlich verbessert werden, ohne die Mitarbeiterinnen und Mitarbeiter nennenswert zu belasten.

RECHTESTRUKTUR AUF ARBEITSPLATZRECHNERN

Zum besseren Schutz gegen Malware und Rechnerausfälle sollte darauf geachtet werden, dass administrative Rechte auf PCs nur dann genützt werden, wenn es tatsächlich nötig ist.

Moderne Betriebssysteme sehen Benutzerkonten mit unterschiedlichen Berechtigungen vor:

- Konten mit **Superuser- bzw. Administrator-Rechten** dienen zur Administration des Computers, zur Softwareinstallation, zum Ändern grundlegender Einstellungen, zum Anlegen neuer Benutzerinnen und Benutzer etc.
- Konten mit **einfachen Benutzerrechten** werden für alltägliche Tätigkeiten, d.h. für die eigentliche Arbeitstätigkeit, verwendet.

Ein häufiger Fehler besteht darin, an alle Mitarbeiterinnen und Mitarbeiter Konten mit Administrator-Rechten zu vergeben. Durch diese Konfiguration entstehen aber verschiedene Probleme:

- Das Einschleppen und die Ausbreitung von **Schadsoftware** wird stark erleichtert;
- die Wahrscheinlichkeit von **Rechnerausfällen** ist deutlich erhöht, da Schutzmaßnahmen gegen das versehentliche Löschen von Systemdaten wegfallen;
- die Benutzerinnen und Benutzer haben volle Rechte zur **unbefugten Installation** von Software;
- verschiedenste **Schutz- und Kontrollmaßnahmen des Betriebssystems** werden wirkungslos oder können von den Benutzerinnen und Benutzern umgangen werden.

Für die tägliche Arbeit dürfen daher ausschließlich Konten mit einfachen Benutzerrechten verwendet werden. Superuser-Rechte müssen einigen wenigen IT-Administratorinnen und -Administratoren vorbehalten bleiben und dürfen auch von diesen nur dann genützt werden, wenn es für die betreffende Tätigkeit unbedingt nötig ist. Auch für diese Personen müssen daher zusätzliche, einfach berechtigte Benutzerkonten eingerichtet werden.

GEFAHRENQUELLE WECHSELMEDIEN

Wechselmedien, wie z.B. USB-Sticks, externe Festplatten, Speicherkarten oder CDs, ermöglichen den raschen und einfachen Transfer von Daten und Programmen, bringen aber auch eine Reihe von Risiken mit sich.

Derartige Risiken sind unter anderem:

- das **Starten fremder Betriebssysteme**, durch die Schutzmechanismen umgangen werden können;
- die **unbefugte Installation** unerwünschter Software oder Schadsoftware;
- das **unberechtigte Kopieren** von Unternehmensdaten auf Wechselmedien (Datendiebstahl, Verlust der Vertraulichkeit).

In vielen Fällen ist eine völlige Sperre der Wechselmedien entweder technisch nicht möglich oder aus betrieblichen Gründen nicht durchsetzbar. Hier sind zusätzliche personelle (Dienstanweisungen, Verbote) und organisatorische Maßnahmen (Kontrollen) erforderlich.

VERSCHLÜSSELUNG VON ARBEITSPLATZSYSTEMEN

Wenn auf einem Computer, der in einer ungeschützten Umgebung betrieben oder aufbewahrt wird, schutzwürdige Daten gespeichert werden, muss Verschlüsselungssoftware eingesetzt werden.

Der typische Anwendungsfall für ein derartiges Verschlüsselungsprodukt sind Notebooks, auf denen wichtige Unternehmensdokumente gespeichert sind. Angesichts der hohen Diebstahls- und Verlustgefahr bei derartigen Geräten müssen diese Firmendaten immer verschlüsselt werden, um sicherzustellen, dass sie nur von ihrem rechtmäßigen Eigentümer gelesen werden können. Auch bei gewöhnlichen Arbeitsplatzrechnern kann Verschlüsselung sinnvoll sein, z.B. wenn sensible Personendaten oder Dokumente der Geschäftsführung geschützt werden sollen. Dabei sind drei Möglichkeiten zu unterscheiden:

- **Transparente Verschlüsselung:** Bei dieser wird die gesamte Festplatte des Rechners verschlüsselt, alle Dateien sind geschützt. Für die Benutzerinnen und Benutzer ist das bei ihrer Arbeit nicht zu bemerken, sie müssen aber beim Rechnerstart ein Verschlüsselungspasswort eingeben.
- **Online-Verschlüsselung:** Auf der Festplatte wird ein virtuelles Dateisystem erstellt, das nur nach Eingabe eines Verschlüsselungspasswords geöffnet werden kann. Anschließend dürfen sensible Daten nur in diesem Dateisystem abgespeichert werden. Die Benutzerinnen und Benutzer müssen selbst darauf achten, wichtige Daten nicht in unsicheren Bereichen abzulegen.
- **Offline-Verschlüsselung:** Einzelne Dateien werden verschlüsselt auf dem unverschlüsselten Datenträger gespeichert. Benutzerinnen und Benutzer müssen bei jeder einzelnen Datei entscheiden, ob sie verschlüsselt werden muss und gegebenenfalls beim Aufruf jeder einzelnen Datei ein Passwort eingeben.

Im Allgemeinen ist die transparente Verschlüsselung die benutzerfreundlichste und am wenigsten fehleranfällige Variante. Der einzige Nachteil besteht darin, dass bei jedem Neustart das Verschlüsselungspasswort eingegeben werden muss. Daher können automatische Rechnerneustarts, wie sie z.B. nach Betriebssystem-Updates nötig sind, nicht mehr unbemerkt in der Nacht erfolgen. Verschlüsselungssoftware kann aus dem Internet geladen werden; es gibt auch gute kostenlose Produkte. Aktuelle Betriebssysteme bieten teilweise ebenfalls Verschlüsselungslösungen, die für übliche Einsatzfälle oft ausreichen.

Auch Daten auf Smartphones und Tablets können verschlüsselt werden. In den meisten Fällen kann das durch das Betriebssystem erfolgen, die Verschlüsselung muss nur noch aktiviert werden. Es gibt aber auch eigene Apps für diesen Zweck, die zusätzlichen Schutz bieten. Wenn Mobile Device Management-Software eingesetzt wird, ist Datenverschlüsselung ohnehin obligatorisch.

Um zu vermeiden, dass auf wichtige Daten nicht mehr zugegriffen werden kann, weil das Passwort zu ihrer Entschlüsselung verloren gegangen ist, sollte festgelegt werden, dass Verschlüsselungspasswörter an sicherer Stelle hinterlegt werden. Das kann z.B. geschehen, indem sie in verschlossenen Kuverts im Firmensafe deponiert werden, die nur in Notfällen geöffnet werden dürfen.

REGELMÄSSIGE SOFTWARE-AKTUALISIERUNGEN

Durch Software-Updates können Schwachstellen beseitigt oder Funktionen erweitert werden.

Updates sind vor allem dann erforderlich, wenn Schwachstellen bekannt werden, die Auswirkungen auf die Sicherheit der Systeme haben oder wenn Fehlfunktionen wiederholt auftauchen. Vor ihrem Einspielen sollte die Zuverlässigkeit der neuen Komponenten und das Zusammenwirken mit bestehenden Programmen geprüft werden. Im Idealfall geschieht das auf einem eigenen Testsystem, alternativ dazu kann das Update auch auf einem einzelnen Rechner getestet werden, bevor es auf allen betroffenen Systemen eingespielt wird.

Aus sicherheitstechnischer Sicht besonders wichtig ist das regelmäßige Einspielen von Updates zu Betriebssystemkomponenten und Internet-Browsern, wie sie von den Herstellern regelmäßig angeboten werden. Solche Aktualisierungen dienen fast immer der Behebung von aktuellen Sicherheitslücken. Werden sie nicht durchgeführt, ist kein Schutz gegen neuere Bedrohungen gegeben.

Auch verschiedene andere Programme (z.B. Adobe Flash, Adobe Reader, Java…) können als Einfallstore für Schadsoftware dienen, wenn sie nicht rechtzeitig aktualisiert werden. Sie müssen regelmäßig überprüft werden, um sicherzustellen, dass ausschließlich Versionen eingesetzt werden, bei denen alle bekannten Schwachstellen behoben sind.

Meistens werden dazu auch Mechanismen angeboten („automatische Updates“), die für die automatische Durchführung sicherheitskritischer Updates sorgen und gleichzeitig sicherstellen, dass dabei ausschließlich vertrauenswürdige Quellen verwendet werden. Diese Einrichtungen ermöglichen es, bei geringem Administrationsaufwand die IT-Systeme auf dem aktuellen Sicherheitsstand zu halten und sollten unbedingt genutzt werden.

NUTZUNGSVERBOT NICHT-BETRIEBLICHER SOFTWARE

Um sicherzustellen, dass keine unerwünschten Programme installiert werden und das System nicht über den vorgesehenen Funktionsumfang hinaus unkontrolliert genutzt wird, muss das Einspielen bzw. die Nutzung nicht-betrieblicher Software verboten und, soweit technisch möglich, verhindert werden.

Im Allgemeinen sollte auch die Nutzung privater Software (Programme, Daten) und Hardware (Notebooks, USB-Sticks, externe Festplatten, Speicherkarten etc.) untersagt werden. Der Einsatz jeder Hard- und Software, die nicht für den eigentlichen Betriebszweck benötigt wird, erhöht die Gefahr des „Einschleusens" von Schadprogrammen und verringert die Stabilität der Systeme.

Weitere Probleme können durch unlizenzierte Software entstehen, die von Benutzerinnen und Benutzern auf Firmenrechnern installiert wurde. Derartige Lizenzrechtsverletzungen können unter Umständen auch zu finanziellen Belastungen für das Unternehmen führen.

Folgenden Maßnahmen sollten umgesetzt werden:

- Ein **Nutzungsverbot nicht-betrieblicher Software** sollte schriftlich fixiert und allen Mitarbeiterinnen und Mitarbeitern mitgeteilt werden.
- Das **unautorisierte Einspielen** und/oder Nutzen von Software ist, soweit möglich, mit **technischen Mitteln** zu verhindern.
- In unregelmäßigen Abständen sollten die Rechner im Unternehmen **auf unzulässige Software überprüft** werden; wenn derartige Software gefunden wird, muss sie umgehend deinstalliert werden.
- Falls nötig, kann eine **Liste von Programmen, deren Nutzung explizit untersagt ist**, erstellt und an die Mitarbeiterinnen und Mitarbeiter ausgegeben werden. Beispiele dafür sind z.B. Skype, Instant Messaging-Clients, Filesharing-Software, Spiele oder Hacker-Tools.

MOBILE IT-GERÄTE

Smartphones, Tablets und Notebooks sind heute weit verbreitet und werden in Unternehmen eingesetzt. Für den sicheren Betrieb müssen aber typische Gefährdungen beachtet und Gegenmaßnahmen umgesetzt werden.

Risiken, die beim Einsatz derartiger Geräte unbedingt beachtet werden müssen, sind:

- Mobile Geräte gehen leicht verloren und sind ein beliebtes Ziel für Diebstähle. Dadurch können gespeicherte Firmendaten in falsche Hände geraten und eventuell vorhandene Passwörter zu einer Kompromittierung der Firmen-IT führen.
- Über unzureichend abgesicherte Schnittstellen von Mobilgeräten (Bluetooth, WLAN, USB) können unter Umständen Daten ausgelesen oder Schadprogramme eingeschleppt werden.
- Schadsoftware, die auf mobilen IT-Geräten ausgeführt wird, kann Dateninhalte auslesen oder Passworteingaben aufzeichnen und versenden. Auch der Versand von Werbe-SMS an Dritte oder die automatische Anwahl kostenpflichtiger Telefonnummern ist möglich.
- Manipulierte Mobilgeräte können dazu genützt werden, vertrauliche Gespräche aufzuzeichnen und abzuhören.
- Über Internetaufrufe oder infizierte E-Mails eingeschleppte Schadsoftware kann in das Firmennetzwerk gelangen, z.B. wenn sich Mobilgeräte über WLAN mit dem Firmennetz verbinden.
- GPS-Empfänger und Daten des WLAN-Empfängers können dazu verwendet werden, um Bewegungsprofile zu erstellen und automatisch zu versenden.

Da der Großteil dieser Geräte für den privaten Einsatz gedacht ist, ist eine zentrale Kontrolle von Sicherheitseinstellungen nur schwer möglich. Die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für den sicheren Umgang mit mobilen IT-Geräten ist daher besonders wichtig. Falls sensible oder geheime Daten verarbeitet werden sollen, ist außerdem der Einsatz von Mobile Device Management-Software notwendig.

Folgende Maßnahmen sollten schriftlich festgelegt und umgesetzt werden:

- Mobile IT-Geräte dürfen nicht unbeaufsichtigt (etwa im Hotel oder im Auto) liegen gelassen oder anderen Personen überlassen werden. Abgesehen von der möglichen Diebstahlgefahr besteht immer die Möglichkeit, dass darauf gespeicherte Daten eingesehen werden oder Schadsoftware installiert wird.
- Mobilgeräte müssen ebenso wie PCs durch Passwörter oder PINs vor unbefugter Inbetriebnahme geschützt werden. Das Aufheben der automatischen Sperre nach Nichtbenutzung muss ebenfalls durch ein Passwort geschützt sein.
- Auch auf mobilen IT-Geräten müssen Virenschutzprogramme betrieben und regelmäßig aktualisiert werden.
- Der Zugriff auf Firmendaten (E-Mails oder Dateien) darf nur über verschlüsselte Kanäle (z.B. SSL-Verbindungen) erfolgen.
- Alle auf dem Mobilgerät gespeicherten Firmendaten müssen verschlüsselt gespeichert werden. Für die Verschlüsselung können Betriebssystemfunktionen oder spezielle Apps genutzt werden.
- Alle Schnittstellen, die nicht aktuell benötigt werden, müssen deaktiviert werden. Auch der GPS-Empfänger muss inaktiv bleiben, solange er nicht benötigt wird.
- Auf allen Mobilgeräten müssen Apps eingesetzt werden, die sämtliche Daten löschen, wenn das Gerät verloren oder gestohlen wird.
- Der Verlust oder Diebstahl eines mobilen IT-Geräts muss den zuständigen Verantwortlichen sofort gemeldet werden, damit rechtzeitig die Fernlöschung oder andere Sicherheitsmaßnahmen ausgelöst werden können.
- Im Idealfall sollten nur vorher geprüfte und als sicher eingestufte Apps installiert werden. In jedem Fall müssen die Benutzerinnen und Benutzer aber auf ihre Auswahl achten und dürfen nur vertrauenswürdige Programme installieren.
- Auf manchen Systemen kann bei der Installation von Apps gewählt werden, auf welche Datenbestände das neue Programm zugreifen darf. Dabei sollten nur Zugriffe erlaubt werden, die unkritische Daten oder Funktionen umfassen.
- Das sogenannte „Jailbreaking“, d.h. das Aushebeln der vom Hersteller vorgesehenen Sicherheitsmaßnahmen, darf auf beruflich verwendeten Mobilgeräten keinesfalls ausgeführt werden. Es setzt die Geräte besonderen, zusätzlichen Sicherheitsgefährdungen aus.
- Wenn mobile IT-Geräte weitergegeben oder entsorgt werden, müssen alle darauf gespeicherten Daten und Einstellungen gelöscht werden. Dazu eignet sich am besten ein „Factory Reset“, d.h. das Zurücksetzen des Geräts in den Auslieferungszustand. Danach sollte noch manuell nachgeprüft werden, ob noch Informationen auf den Speichern verblieben sind.

NUTZUNG VON CLOUD-SPEICHERDIENSTEN

Cloud-Speicherdienste wie z.B. Dropbox, iCloud oder Google Drive ermöglichen den einfachen Datenaustausch beim Einsatz mehrerer IT-Geräte und sind auch für Online-Backups geeignet. Wenn sie von den Mitarbeiterinnen und Mitarbeitern eigenmächtig eingesetzt werden, besteht aber die Gefahr, dass Daten unbemerkt aus dem Unternehmen abfließen.

Als Nebeneffekt des Mobile Computing-Trends ist die Verwendung von Online-Speicher wesentlich einfacher und billiger geworden. Für die Beschäftigten liegt es nahe, ihren privaten Cloud-Speicher auch für berufliche Zwecke zu nutzen. Das kann dazu führen, dass Firmendaten dem Zugriff des Unternehmens entzogen und in unsicheren Umgebungen gespeichert werden.Auch der Diebstahl von Daten – unter Umständen durch eigene Mitarbeiterinnen und Mitarbeiter – wird damit erleichtert.

Beim ungeregelten Einsatz von Cloud-Speicherdiensten können unter anderem folgende Probleme auftreten:

- Der Zugang zu privatem Online-Speicher ist oft nur durch ein schwaches Passwort abgesichert. Für private Zwecke mag das ausreichen, betriebliche Sicherheitsvorgaben werden damit aber unterschritten.
- Daten, die Mitarbeiterinnen und Mitarbeiter im mobilen Einsatz erstellen und über den eigenen Cloud-Speicher sichern, können nur von ihnen selbst abgerufen werden. Scheiden sie aus, gehen die Daten dem Unternehmen verloren.
- Über Online-Speicher können mit geringem Aufwand große Mengen von Unternehmensdaten außer Haus transferiert werden, selbst wenn die Verwendung von USB-Speichergeräten auf Firmen-PCs unterbunden wurde.
- Alle Überlegungen, die vor dem Einsatz von Cloud Computing durch das Unternehmen zu treffen sind – z.B. zu Fragen des Zugriffsschutzes oder der Übertragung personenbezogener Daten in Staaten außerhalb der EU –, gelten selbstverständlich auch für Online-Speicherdienste. Der ungeprüfte Einsatz von Cloud-Speicher führt damit zu sicherheitstechnischen und oft auch rechtlichen Problemen.

Die Nutzung von Online-Speicherdiensten im Unternehmen muss daher unbedingt geregelt werden. Die wichtigsten Maßnahmen dazu:

- Der eigenmächtige Einsatz dieser Dienste muss entweder vollständig verboten oder auf bestimmte, unkritische Daten beschränkt werden.
- Der Transfer von Firmendaten aus dem Unternehmen kann durch Sperren der Cloudspeicher-Anbieter auf der Firewall unterbunden werden.
- Falls Cloud-Speicher aus strategischen Gründen zugelassen werden soll, müssen die Anbieter zuvor eingehend geprüft werden. Dazu sollten die Empfehlungen des Kapitels „Outsourcing und Cloud Computing“ herangezogen werden.
- Die Mitarbeiterinnen und Mitarbeiter dürfen anschließend nur die zugelassenen Anbieter verwenden. Um Datenverlust nach dem Ausscheiden von Mitarbeiterinnen oder Mitarbeitern aus dem Unternehmen zu vermeiden, muss das Unternehmen (IT-Abteilung, Vorgesetzte) eine Möglichkeit besitzen, eigenständig auf die gespeicherten Inhalte zuzugreifen.

Virenschutz

Computer-Viren (in weiterer Folge einfach als Viren bezeichnet) gehören zu den „Schadprogrammen" („Malware"). Dies sind Programme, die verdeckte Funktionen enthalten und damit durch Löschen, Überschreiben oder sonstige Veränderungen unkontrollierbare Schäden an Programmen und Daten bewirken können. Sie verursachen zusätzliche Arbeit und Kosten und beeinträchtigen die Sicherheit von Daten oder Programmen.

Während früher Viren meist durch den Austausch verseuchter Datenträger verbreitet wurden, ist heute zunehmend die Verbreitung über Internet bzw. E-Mail das Problem. Bei den meisten über E-Mail verbreiteten „Viren" handelt es sich eigentlich um Würmer, die – unabhängig von der eigentlichen Schadensfunktion – schon durch ihr massenhaftes Auftreten und ihre rasante Verbreitung großes Aufsehen erregen und zu hohen Schäden führen.

Das nachfolgende Kapitel beschäftigt sich vorwiegend mit dem Schutz gegen Viren und Würmer. Die angeführten Maßnahmen sind großteils auch gegen andere Arten von Software mit Schadensfunktion, wie z.B. Trojanische Pferde, anwendbar.

TECHNISCHE VIRENSCHUTZMASSNAHMEN

Zur Abwehr von Vireninfektionen müssen alle Computer des Unternehmens mit Antivirus-Software ausgestattet werden. Zusätzlich müssen noch andere Einstellungen gesetzt werden, um Gefahren zu reduzieren, die aus noch unbekannter oder vom Virenschutz „übersehener" Schadsoftware entstehen können.

Der Betrieb von Antivirus-Programmen ist aus heutiger Sicht unerlässlich. Das gilt zumindest für alle Client- und Serversysteme, die unter Microsoft-Betriebssystemen betrieben werden, ist aber auch bei Linux- oder MacOS-Systemen anzuraten.

Bei der Auswahl der Virenschutzsoftware sind einige grundlegende Anforderungen zu beachten, die aber von allen modernen Lösungen erfüllt werden: Die Virensignaturdateien müssen laufend automatisch aktualisiert werden, alle infizierbaren Dateien müssen beim Dateizugriff (Zugriffs-, On-Access-Scan) geprüft werden, beim Auffinden von Viren müssen die Betroffenen verständigt und die infizierte Datei entweder gelöscht oder an eine sichere Stelle (Quarantäne) verschoben werden. Zusätzlich sollten noch automatisch gestartete Virensuchläufe über alle Datenträger des Computers eingestellt werden können, um regelmäßig eine genaue Prüfung des gesamten Datenbestandes durchzuführen.

Auch die beste Virenschutzsoftware erzielt nie eine hundertprozentige Trefferquote. Moderne Virentypen setzen verschiedene Methoden der Tarnung ein; gelegentlich kommt es auch vor, dass Viren sich schneller verändern, als die Hersteller von Antivirus-Software passende Signaturupdates erarbeiten können. Eine weitere Gefahrenquelle sind sogenannte Zero-Day-Attacken, bei denen bisher unbekannte Sicherheitslücken für Angriffe genützt werden, bevor noch Abwehrmaßnahmen verfügbar sind.

Einige Maßnahmen können helfen, das Risiko einer Infektion weiter zu verringern:

- Die **Anzeige der Dateiendungen** (.docx, .exe, .scr, ...) sollte aktiviert werden, um Schadprogramme, die als E-Mail-Attachment geschickt werden, leichter erkennen zu können.
- In bestimmten Anwendungsprogrammen (MS Word, Excel, Powerpoint) sollte der **Makro-Virenschutz** aktiviert und auf entsprechende Warnmeldungen geachtet werden.
- In den **Sicherheitseinstellungen von Internet-Browsern** können aktive Inhalte (ActiveX, Java, JavaScript) und Skript-Sprachen (z.B. Visual Basic Script) deaktiviert werden. Dafür werden auch entsprechende Plug-ins angeboten.
- Das **Ausführen von aktiven Inhalten** in E-Mail-Programmen muss durch entsprechende Sicherheitseinstellungen **unterbunden** werden.
- In verschiedenen E-Mail-Programmen gibt es die Option, Anlagen mit bestimmten Datei-Endungen nicht anzuzeigen. Sie sollte so gesetzt werden, dass **ausführbare Programme und Skripte unterdrückt** werden. Falls eine derartige Datei dennoch erwünscht ist, muss sie an die IT-Zuständigen zur Prüfung weitergeleitet werden.
- E-Mail-Clients müssen so eingestellt sein, dass **Attachments nicht automatisch geöffnet** werden. Als E-Mail-Editor dürfen keine Programme, die Makro-Sprachen (z.B. MS Word) oder Scripts unterstützen, eingesetzt werden. Auch beim Empfang von HTML-Mails ist Vorsicht geboten.
- Durch den Einsatz einer **Personal Firewall**, die Verbindungsversuche unbekannter Programme zum Internet blockiert, kann Angriffen gezielt entgegengewirkt werden. Eine zentrale Firewall kann durch derartige Software wirkungsvoll ergänzt werden.

VERMEIDUNG BZW. ERKENNUNG VON VIREN DURCH BENUTZERINNEN UND BENUTZER

Die Sensibilisierung der Anwenderinnen und Anwender für die Virenproblematik ist eine wichtige Komponente aller Virenschutzmaßnahmen. Daher sollte in Schulungen regelmäßig auf die Gefahr von Viren, die Möglichkeiten zu ihrer Erkennung und Vermeidung sowie das richtige Vorgehen im Falle eines (vermuteten) Virenbefalls hingewiesen werden. Auch die laufende Information der Betroffenen über aktuelle Bedrohungen ist empfehlenswert.

Alle Benutzerinnen und Benutzer sollten folgende Verhaltensregeln beachten:

- Auch bei E-Mails von vermeintlich bekannten bzw. vertrauenswürdigen Absendern muss geprüft werden, ob der **Inhalt der Nachricht** zum Absender passt und ob das Mail bzw. das Attachment auch erwartet wurde. Englischsprachige Mails von deutschsprachigen Partnern sind ein klares Alarmsignal, aber auch unerwartete Inhalte oder der fehlende Bezug zu aktuellen Vorgängen sollten Vorsichtsmaßnahmen auslösen.
- Als Attachment gesendete **Programme oder Skripts** (d.h. Dateien mit den Endungen .com, .exe, .bat, .vbs etc.) dürfen nur ausgeführt werden, wenn sie von der Empfängerin oder dem Empfänger erwartet wurden und ihre Rechtmäßigkeit klar feststeht. Besondere Vorsicht ist bei doppelten, „merkwürdigen“ Dateinamen-Endungen („.jpg.vbs“ oder „gif.exe“) geboten. Sie sollen Empfängern eine harmlose Datei vortäuschen, sind aber ausführbare Schadprogramme.
- Auch E-Mails im **HTML-Format** oder **Office-Dokumente** (.docx, .xlsx, .pptx etc.) sowie Bildschirmschoner (.scr) können Schadfunktionen enthalten. Sie dürfen ebenfalls nur dann geöffnet werden, wenn sie von vertrauenswürdigen Absendern stammen oder die Datei erwartet wurde.
- Mehrere **E-Mails mit gleichem Betreff** sind verdächtig, vor allem, wenn sie von verschiedenen Absendern stammen.

- **Phishing-Mails,** d.h. Mails, in denen zur Übermittlung von persönlichen Daten oder Passwörtern (z.B. PIN oder TAN) aufgefordert wird, dürfen auf keinen Fall beantwortet werden. Auch darin angegebene Webseiten dürfen nicht geöffnet werden. Bei Erhalt einer derartigen E-Mail müssen auch die anderen Mitarbeiterinnen und Mitarbeiter darauf hingewiesen werden, dass es sich dabei um einen Betrugsversuch handelt.
- **Internet-Links in E-Mails** dürfen nur dann aufgerufen werden, wenn es sich um vertrauenswürdige Nachrichten handelt, und müssen mit großer Vorsicht behandelt werden: Beim Anklicken kann Schadsoftware wie z.B. ein Verschlüsselungstrojaner installiert oder eine Phishing-Website aufgerufen werden. Die im Link angezeigte Website täuscht oft über die tatsächlich aufgerufene URL hinweg.
- Abgefangene Phishing- oder Virus-E-Mails können in entschärfter Form (d.h. ohne ausführbare Anhänge oder irreführende Links) zur Ansicht an die Mitarbeiterinnen und Mitarbeiter weitergeleitet werden. Damit wird ihr Problembewusstsein verbessert und sie erhalten die Gelegenheit, gefährliche E-Mails **selbst erkennen zu lernen**.
- **Spam-Mails,** Werbemails und andere unaufgefordert erhaltene Zusendungen dürfen **nicht beantwortet** werden. Die Aufforderung an den Absender, weitere Zusendungen zu unterlassen, ist kontraproduktiv: Diese Rückmeldung bestätigt nur die Gültigkeit der Empfänger-Adresse und erhöht damit das Risiko, weitere Zusendungen zu erhalten. Das Abbestellen von E-Mails ist nur bei seriösen Zustellern sinnvoll.
- **Weitere Hinweise** zur Erkennung von Viren oder Phishing-Versuchen finden Sie im „IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter".

NOTFALLMASSNAHMEN IM FALL VON VIRENINFEKTIONEN

Für Notfälle, die in Folge einer Virusinfektion auftreten können, sollten Vorkehrungen getroffen werden, um die weitere Ausbreitung der Viren zu verhindern und möglichst rasch die Rückkehr zum Normalbetrieb einleiten zu können.

Wie bei allen Notfällen sollte auch für den Fall einer massiven Vireninfektion rechtzeitig Vorsorge getroffen werden. Bei entsprechender Planung können Stillstände und Produktionsausfälle verhindert oder wenigstens eingeschränkt werden. Dabei sollten die folgenden Punkte behandelt werden:

- Den Benutzerinnen und Benutzern sollte eine **Ansprechperson** bekannt sein, die sie in Notfällen erreichen können, um die weiteren Maßnahmen einzuleiten und zu koordinieren.

- Ein Programm an **Erstmaßnahmen**, die eine Weiterverbreitung von Viren verhindern, muss ausgearbeitet werden. Mögliche Inhalte sind z.B. das Herunterfahren des Mail-Servers und der betroffenen Clients oder das Trennen der Internetverbindung. Zu berücksichtigen ist dabei auch, wie vorgegangen werden soll, wenn keine IT-Administratorinnen oder -Administratoren oder sonstige technisch Sachkundige erreichbar sind.
- Es muss sichergestellt sein, dass bei Vorliegen eines neuen Virus die **Updates der Virenschutzprogramme** möglichst rasch auf allen Rechnern eingespielt werden. Entsprechende Maßnahmen müssen vorbereitet und getestet werden.
- Falls infizierte E-Mails an **andere Unternehmen** (Kunden, Partner) versandt wurden, müssen diese Unternehmen umgehend darüber informiert werden, um die weitere Ausbreitung der Schadsoftware zu verhindern.
- **Wiederherstellungsstrategien** müssen erarbeitet werden, die festlegen, welche Rechner in welcher Reihenfolge in betriebsbereiten Zustand zu bringen sind, damit in kürzester Zeit zumindest eine eingeschränkte Funktionsfähigkeit hergestellt werden kann.
- Sollte der Virus Daten gelöscht oder verändert haben, so muss versucht werden, die Daten aus den **Datensicherungen** und die Programme aus den **Sicherungskopien** der Programme zu rekonstruieren.

RANSOMWARE UND VERSCHLÜSSELUNGSTROJANER

Eine der größten Bedrohungen für Unternehmen im Bereich Internetkriminalität ist die Ransomware. Dabei handelt es sich um Schadsoftware, bei der Benutzerinnen und Benutzer erpresst werden, ein „Lösegeld“ (eng. Ransom) zu zahlen, um ihren Computer weiter benutzen oder ihre Dateien öffnen zu können.

In einfachen Fällen wird durch Ransomware der Computer blockiert, z.B. indem ein Hinweis erscheint, die Benutzung wäre wegen ungesetzlicher Nutzung durch die Bundespolizei oder andere Institutionen gesperrt. Angriffe dieser Art können mit Hilfe von Virenschutzsoftware leicht und ohne Datenverlust repariert werden.

Wesentlich schwerwiegender sind Attacken mit Verschlüsselungs- oder Kryptotrojanern. Dabei werden Dateien, die von den Benutzerinnen und Benutzern erstellt wurden, verschlüsselt und dadurch unbenutzbar gemacht. Z.B. werden sämtliche Office-Dokumente und PDF-Dateien, die auf dem Computer gespeichert sind, verschlüsselt, häufig zusätzlich auch Bild- und Musikdateien.

Wenn auf dem befallenen PC Netzlaufwerke verbunden sind, sind auch die Dateien auf diesen Laufwerken betroffen. Der Angriff kann daher weit über den einzelnen Computer hinausreichen und den gesamten Datenbestand des Unternehmens beschädigen. Verschlüsselungstrojaner können auf diese Weise zu massivem, vielleicht auch existenzbedrohendem Datenverlust führen.

Um das Passwort für die Entschlüsselung zu erhalten, werden die Betroffenen aufgefordert, einen bestimmten Betrag über anonyme Zahlungsmethoden (z.B. mittels Bitcoin) zu überweisen. Bei manchen Angriffen ist es tatsächlich möglich, die Daten auf diese Weise „freizukaufen". Häufig ist die Schadsoftware aber so programmiert, dass eine Entschlüsselung gar nicht mehr möglich ist. Es sollten daher in jedem Fall Sicherheitsexperten oder Behörden befragt werden, bevor eine Zahlung des „Lösegelds" erfolgt.

Die folgenden Maßnahmen können helfen, Schäden durch Ransomware zu vermeiden:

- Das wichtigste Mittel gegen Datenverluste durch Verschlüsselungstrojaner sind regelmäßige und vollständige Datensicherungen. Wenn diese zur Verfügung stehen, besteht der entstandene Schaden nur in der Arbeitszeit bis zum Entfernen der Schadsoftware und der Wiederherstellung der Daten.
- Datensicherungen dürfen auf keinen Fall durch Schadsoftware unbrauchbar gemacht, d.h. verschlüsselt oder überschrieben werden. Die Sicherungsmedien (z.B. USB-Festplatten) sollten daher außerhalb der Sicherungszeiten immer offline sein.

Die Einfallswege für Ransomware sind nicht anders als bei anderer Schadsoftware. Die Benutzerinnen und Benutzer müssen daher geschult werden, Angriffe zu erkennen und Vorsichtsmaßnahmen einzuhalten (siehe dazu auch den Abschnitt Vermeidung und Erkennung von Viren durch Benutzerinnen und Benutzer):

- Seien Sie vorsichtig beim Erhalt von E-Mails, deren Absender Sie nicht kennen oder wenn Sie keine entsprechenden Mitteilungen erwarten.
- Kontrollieren Sie nach Möglichkeit die tatsächliche Absenderadresse, achten Sie auf Ungereimtheiten. Bei angeführten Weblinks legen Sie den Mauszeiger über den entsprechenden Link, ohne diesen anzuklicken. Sollte die Weblink-Adresse aufscheinen, kontrollieren Sie, ob diese tatsächlich zum Absender gehört.
- Achten Sie auf die Schreibweise und Rechtschreibung solcher Nachrichten, Angreifer verwenden hier gerne Übersetzungsprogramme, wodurch der Betrug oft leicht erkennbar ist.

- Öffnen Sie keinesfalls Ihnen unbekannte Dateianhänge, ohne sich vorher von deren „Echtheit“ zu überzeugen. Werden Ihnen Rechnungen oder Bewerbungsunterlagen zum Download „angeboten“, tun Sie dies bitte nicht! Wenn Sie dennoch der Ansicht sind, dass es sich um echte und notwendige Dokumente handelt, laden Sie die Datei nur in einer gesicherten Umgebung (Sandbox, virtuelle Systeme mit Option auf Rücksetzung) und auf nicht produktiven Geräten herunter und öffnen diese dann auch dort. Oder bedienen Sie sich unterstützender Seiten im Internet (z.B. Virustotal.com).
- Beschränken Sie die Benutzerrechte der jeweiligen User so weit als möglich und arbeiten Sie nur unter dem Administrator-Account, wenn dies unbedingt notwendig ist.
- Auch nach Bezahlung des geforderten Betrags gibt es keine Sicherheit, dass eine Wiederherstellung der Daten erfolgt oder überhaupt möglich ist. Das Überweisen des „Lösegelds“ sollte daher das letzte Mittel sein und nur dann versucht werden, wenn unentbehrliche Daten ansonsten unrettbar verloren sind.

KONTROLLFRAGEN

- Haben Sie ein schriftliches Nutzungskonzeptverbot für nicht-betriebliche Software und ist in Ihrem Unternehmen durch ein angemessenes Berechtigungssystem sichergestellt, dass die Installation von Programmen nur von befugten und fachkundigen IT-Administratorinnen und -Administratoren vorgenommen werden kann?
- Wurde sichergestellt, dass in Ihrem Unternehmen die Betriebssystemkomponenten, Internetbrowser und andere Software auf allen Computern laufend und systematisch aktualisiert werden?
- Wurden Ihre Mitarbeiterinnen und Mitarbeiter über die fachgerechte Auswahl und den richtigen Umgang mit Passwörtern geschult?
- Werden Daten auf Ihren Firmennotebooks verschlüsselt und werden die Verschlüsselungspasswörter an zentraler, gesicherter Stelle hinterlegt?
- Ist die Benutzung von Wechselmedien, wie z.B. USB-Sticks, in Ihrem Unternehmen reguliert und wurden die Vorschriften allen Mitarbeiterinnen und Mitarbeitern zur Kenntnis gebracht? Wird die Einhaltung der Vorschriften regelmäßig kontrolliert?
- Wurden Ihre Mitarbeiterinnen und Mitarbeiter über die Risiken von mobilen IT-Geräten informiert und wurden entsprechende Sicherheitsmaßnahmen festgelegt?
- Haben Sie auf allen Ihren Computern Virenschutzprogramme installiert und werden diese laufend (täglich oder öfter) aktualisiert?
- Sind Sie sicher, dass die Sicherheitsoptionen aller Internetbrowser und aller E-Mail-Clients in Ihrem Unternehmen korrekt eingestellt wurden?
- Werden Ihre Mitarbeiterinnen und Mitarbeiter regelmäßig über die Gefahren von Viren und Möglichkeiten zu deren Vermeidung geschult?
- Werden Ihre Mitarbeiterinnen und Mitarbeiter regelmäßig über die Gefahren von Ransomware und Möglichkeiten zu deren Vermeidung geschult?
- Haben Sie ein schriftliches Notfallkonzept, das bei akutem Virenbefall eine Ansprechperson, ein Programm an Erstmaßnahmen sowie Wiederherstellungsstrategien unter Berücksichtigung Ihres Datensicherungskonzepts vorsieht? Sind alle Mitarbeiterinnen und Mitarbeiter über Ansprechpersonen, Erstmaßnahmen und Verhaltensweisen bei einem Virenbefall informiert?

6. Netzwerksicherheit

Durch eine Netzwerkverbindung zum Internet entstehen Gefahren: Werden keine zusätzlichen Schutzmaßnahmen eingerichtet, ist die Verbindung in beiden Richtungen offen, d.h. es kann nicht nur vom Firmenrechner auf das Internet, sondern auch von einem beliebigen Rechner im Internet auf das Firmennetz und die Firmendaten zugegriffen werden.

Auch der Zugriff auf das WWW ist nicht immer unproblematisch: Aktive Inhalte auf Webseiten gefährden die Sicherheit der lokalen Rechner und dadurch auch die Vertraulichkeit der Firmendaten. Weitere Gefahren gehen von Schadprogrammen (Viren, Würmer, Spyware, Adware etc.) aus.

FIREWALLS

IT-Systeme im Firmennetzwerk dürfen nur unter Verwendung ausreichender Sicherheitseinrichtungen mit dem Internet verbunden werden. Solche Einrichtungen werden als „Firewalls" bezeichnet.

Eine Firewall kontrolliert die Netzwerkverbindungen zwischen Firmennetzwerk und Internet und blockiert alle jene Verbindungen, die nicht explizit als „erlaubt" deklariert wurden. Firewalls sind in unterschiedlichsten Ausführungen und Preisklassen erhältlich, die Palette reicht von Breitband-Routern mit integrierter Paketfilter-Firewall bis zu hochleistungsfähigen Firewall-Appliances mit verschiedenen Schutzzonen. Sie unterscheiden sich stark in ihrer Leistungsfähigkeit und Schutzwirkung:

- In WLAN-Router und ähnliche für den Privatgebrauch gedachte Geräte sind einfache Firewalls eingebaut, die oft nur eingeschränkte Betriebsstabilität und gelegentlich massive Sicherheitslücken aufweisen. Für den betrieblichen Einsatz sind sie ungeeignet.
- Multifunktions-Firewalls, oft auch Sicherheits-Appliances o.ä. genannt, bieten zusätzlich zur Firewall-Funktion noch weitere Dienste an. Viele können den Netzwerkverkehr auf Viren absuchen oder Spam-Mails ausfiltern, auch die gezielte Sperre bestimmter Websites oder Downloads ist oft möglich. Sie sind für kleine und mittlere Betriebsgrößen meistens gut geeignet.
- Als Next Generation-Firewall werden Geräte bezeichnet, die den Datenverkehr im Detail prüfen und auf Applikationsebene „verstehen". Sie erlauben gezielte Eingriffe in den Internetzugriff, indem z.B. einzelne Anwendungen gesperrt oder nur für bestimmte Benutzer freigegeben werden, benötigen aber ausreichendes Know-How und Planung.

- Komplexe Firewallsysteme kommen dagegen vor allem dann zum Einsatz, wenn es nötig ist, wichtige Unternehmensanwendungen – z.B. öffentlich zugängliche Web- und Datenbankserver – abzusichern, wenn eine große Anzahl von Benutzerinnen und Benutzern auf hochleistungsfähige Internetverbindungen zugreifen muss oder wenn durch eine doppelte Auslegung der Firewall höchstmögliche Ausfallsicherheit erreicht werden soll.

Häufig bieten auch Internet-Provider unter dem Schlagwort „Managed Security" Firewall-Dienste an. Dabei stellt der Provider die Firewall zur Verfügung und übernimmt auch deren Einrichtung und Wartung. Insbesondere in kleineren Unternehmen oder wenn kein ausreichendes Fachwissen vorliegt, sollte diese Variante in Betracht gezogen werden.

Weiters muss zwischen Firewalls im eigentlichen Sinn und Personal Firewalls unterschieden werden. Bei ersteren handelt es sich um Hardware-Geräte, die zwischen Internet und Firmennetz installiert werden und das gesamte Netzwerk (d.h. mehrere Rechner) schützen. Eine Personal Firewall ist dagegen ein Programm auf einem einzelnen Rechner, das den Datenverkehr dieses PCs kontrolliert und unerlaubte Verbindungen blockiert.

Jede Firewall muss richtig installiert und konfiguriert werden, um wirksam Schutz zu bieten. Sie muss außerdem laufend administriert werden. Folgende grundlegende Regeln müssen erfüllt sein:

- Jede **Kommunikation** zwischen Firmennetz und Internet muss **ausnahmslos über die Firewall** geführt werden. Die Firewall darf nicht durch Modem-, WLAN- oder Mobile Internet-Verbindungen umgangen werden.
- **Sicherheitsrelevante Updates** der Firewall-Software müssen regelmäßig eingespielt werden, um zu verhindern, dass durch eine Schwachstelle der Firewall das gesamte Firmennetzwerk gefährdet wird.
- Die **Konfiguration und Administration** der Firewall darf nur über eine **sichere Verbindung** möglich sein. Angreifern aus dem Internet darf es nicht möglich sein, die Konfiguration der Firewall zu verändern oder auszulesen. Auch aus dem Firmennetzwerk darf der Zugang nur befugten Personen möglich sein.
- Die Konfiguration der Firewall muss in einer **Dokumentation** festgehalten werden, die nach jeder Änderung aktualisiert wird. Bei Konfigurationsänderungen sollten Grund, Zeitpunkt und der Name des oder der Durchführenden vermerkt werden.
- Eine richtig konfigurierte Firewall gestattet **nur die unbedingt notwendigen und tatsächlich gebrauchten Verbindungen**, alle anderen Verbindungen werden blockiert.

Die richtige Planung und Konfiguration einer Firewall ist komplex. Sie ist von höchster Wichtigkeit für die Sicherheit des Firmennetzwerkes und der verwendeten Daten und sollte in jedem Fall durch qualifiziertes Fachpersonal durchgeführt werden. Wenn im Unternehmen kein ausreichendes Fachwissen vorliegt, ist es am sichersten, die Grundkonfiguration durch einen spezialisierten externen Dienstleister vornehmen zu lassen. Nachträgliche Änderungen können dann eventuell durch die eigenen Mitarbeiterinnen und Mitarbeiter erfolgen, sobald diese sich das nötige Fachwissen erarbeitet haben.

PERSONAL FIREWALLS

In Fällen, in denen der Einsatz einer klassischen Firewall nicht möglich ist, vor allem beim Internetzugang unterwegs, über WLAN oder Mobile Internet, bieten Personal Firewalls einen grundlegenden Schutz gegen Fremdzugriffe. Bei korrekter Konfiguration können sie aber auch in Firmennetzen, die durch eine Hardware-Firewall geschützt sind, eingesetzt werden, um den Schutz vor unzulässigen Verbindungen zu verbessern.

Typischerweise funktioniert eine Personal Firewall so, dass nur Programme mit dem Internet kommunizieren dürfen, die dazu eigens autorisiert wurden. Oft „erlernt" sie zulässige Verbindungen aufgrund von Benutzereingaben: Beim ersten Verbindungsversuch eines Programms (z.B. des Internet-Browsers) mit dem Netzwerk wird die Benutzerin oder der Benutzer gefragt, ob diese Verbindung gestattet sein soll. Wenn die Verbindung erlaubt wird, wird sie in Zukunft ohne weitere Nachfrage zugelassen.

Bildschirmdialog einer Personal Firewall: Erst nach Erlaubnis des Benutzers darf das Programm (ein WWW-Browser) auf die Webseite im Internet zugreifen

Eine Personal Firewall kann den Schutz einzelner mit dem Internet verbundener PCs verbessern. Es gibt allerdings auch einige Bedenken:

- Die Abfrage, welchen Programmen die Verbindung zum Internet gestattet werden soll, kann die **Anwenderinnen und Anwender überfordern**. Einigen Programmen (insbes. jenen, die selbsttätig nach Produktaktualisierungen und Updates suchen, wie z.B. Virenschutzprogramme) muss diese Verbindung erlaubt werden, bei anderen Programmen (Schadprogramme wie Trojaner oder Spyware) ist der Verbindungsversuch als

Alarmsignal zu werten. Diese Unterscheidung kann selbst gut ausgebildeten Administratorinnen und Administratoren manchmal schwer fallen.

- **Schadprogramme,** die den Computer befallen haben, können auch die Personal Firewall manipulieren oder sogar ausschalten. In diesem Fall ist der vermeintlich geschützte Rechner problemlos aus dem Internet angreifbar.

Personal Firewalls sind in verschiedenster Form erhältlich: Manche erfordern keine oder nur wenig Benutzereingriffe, andere können ohne ausgeprägtes Fachwissen kaum bedient werden. Der Schutz, den diese Programme bieten, ist ebenfalls sehr unterschiedlich. Im Allgemeinen sollte eine Personal Firewall nur zum Schutz von Einzelplatzrechnern eingesetzt werden. Wenn mehrere Rechner geschützt werden müssen, muss sie durch eine Hardware-Firewall ergänzt werden.

WIRELESS LAN (WLAN)

Drahtlose Netzwerke, sogenannte WLAN-Lösungen, ergänzen zunehmend traditionelle LANs, bei denen der Netzwerkanschluss über Kabelverbindungen realisiert wird. Zum einen bieten sie Flexibilität bei der Arbeitsplatzgestaltung, zum anderen sind für ihren Aufbau keine aufwändigen Verkabelungsarbeiten notwendig. Die steigende Zahl von mobilen Geräten (Notebooks, Smartphones, etc.) fördert die Verbreitung von WLAN zusätzlich. Sicherheitstechnisch entstehen durch WLANs neue Gefährdungen und es sind einige Maßnahmen zu beachten, um nicht durch ihre Einführung die Sicherheit des gesamten Netzwerks zu gefährden.

Sicherheitsmängel in WLAN-Netzwerken waren schon häufig die Ursache für erfolgreiche Attacken. Zum Teil lag das an Konfigurationsmängeln, zum Teil aber auch an Schwächen in den zugrundeliegenden Sicherheitstechnologien. Diese Schwachstellen sind bereits seit langem behoben; sie können aber bei älteren Geräten noch vorhanden sein oder durch fehlerhafte Konfigurationen bestehen bleiben.

An einem zufällig gewählten Standort verfügbare WLANs. Ungesicherte Netzwerke können jederzeit missbraucht werden.

Die Bedrohung durch WLAN-Angriffe darf nicht unterschätzt werden; das Aufspüren und der unbefugte Gebrauch von Drahtlosnetzen kann für Angreifer sehr einfach sein. Die Nutzung eines solchen ungeschützten Netzes als kostenloser drahtloser Internetzugang ist noch die harmloseste Art des Missbrauchs, das Ausspionieren von Firmendaten die weitaus bedenklichere Variante. Es besteht auch die Gefahr, dass Eindringlinge illegale Aktivitäten über das offene WLAN durchführen, für die dann der Betreiber verantwortlich gemacht wird. Ein ungesichertes WLAN kann daher auch zu rechtlichen Problemen führen.

Vor der Planung und Installation einer neuen WLAN-Lösung oder Absicherung bereits bestehender Anlagen sollten daher unbedingt die letzten Entwicklungen und Sicherheitshinweise recherchiert werden. An dieser Stelle sind nur Hinweise auf einige Maßnahmen möglich, die unbedingt beachtet werden sollten:

- **Geeignete Positionierung** und Ausrichtung der Zugriffspunkte und Antennen – außerhalb des Firmengeländes sollte der WLAN-Empfang möglichst verhindert werden;
- **Verschlüsselungsoptionen** aktivieren; ausschließlich WPA oder WPA2 dürfen eingesetzt werden;
- Wird ein **Pre-Shared-Key** eingesetzt (WPA-PSK), sollte dieser **möglichst lang** sein (mindestens 20 Zeichen) und aus einer Folge zufälliger Zeichen bestehen;
- Ändern der **Standardeinstellungen** (insbes. der Passwörter) am WLAN-Access-Point;
- Aktivieren der **MAC-Adressfilterung** am WLAN-Access-Point;
- **Deaktivieren des DHCP-Servers** am WLAN-Access-Point;
- Verwendung von aktuellen, derzeit als sicher geltenden **EAP-Authentifizierungsmethoden**.

GÄSTE-WLAN

Viele Unternehmen haben als Kundenservice oder für die privaten Mobilgeräte ihrer Mitarbeiter ein Gäste-WLAN eingerichtet. Für einen sicheren Betrieb müssen verschiedene Maßnahmen umgesetzt werden.

Unbedingt erforderlich ist die strikte netzwerktechnische Trennung von Firmennetzwerk und Gäste-WLAN: Jeder Verkehr zwischen den beiden Netzabschnitten muss blockiert werden. Aus dem Besuchernetzwerk ist ausschließlich die Verbindung zum Internet zulässig; aus dem Firmen-LAN dürfen Geräte der Gäste nicht erreichbar sein.

Im Allgemeinen ist es besser, den Zugang zum Gäste-WLAN mit einem Passwort zu schützen. Dadurch wird verhindert, dass es von Fremden als kostenloser Internetzugang missbraucht wird. Außerdem lässt sich damit eine grundlegende Kontrolle der Benutzung erzielen. Ein wesentlicher Vorteil besteht außerdem darin, dass der Datenverkehr innerhalb des WLAN verschlüsselt wird und von Außenstehenden nicht einfach abgehört werden kann.

Neben der technischen Absicherung sind auch rechtliche Aspekte zu berücksichtigen: Gästen muss eine Benutzerordnung zur Verfügung gestellt werden, die Auflagen für die korrekte Verwendung des WLAN enthält. Unter anderem sollten darin die Nutzung zu rechtswidrigen Zwecken (illegale Downloads, Angriffe, verbotene Inhalte…) untersagt und Schutzmaßnahmen (Virenschutz, Firewall, verschlüsselte Datenübertragung) empfohlen werden.

Das Zugangspasswort zum Gäste-WLAN kann in Verbindung mit dieser Benutzerordnung übergeben werden. Es können aber auch technische Lösungen eingesetzt werden, die den Zugang erst herstellen, nachdem der Gast die Benutzerordnung mit einem Mausklick akzeptiert hat.

FESTLEGUNG EINER INTERNET-SICHERHEITSSTRATEGIE

Eine WWW-Sicherheitsstrategie dient zur Klärung grundlegender sicherheitsrelevanter Fragestellungen, die noch vor Freigabe der Internetnutzung für die Mitarbeiterinnen und Mitarbeiter geklärt werden sollten.

Insbesondere folgende Fragen sollten behandelt werden:

- Wer erhält WWW-Zugang?
- Welche Bedingungen sind bei der WWW-Nutzung zu beachten?
- Wie werden die Benutzerinnen und Benutzer geschult?
- Wie wird technische Hilfestellung für die Benutzerinnen und Benutzer gewährleistet?

Das richtige Benutzerverhalten hat wesentlichen Anteil bei der Abwehr der Gefahren, die aus der Internet-Nutzung entstehen. Jede Benutzerin und jeder Benutzer sollte daher bereits vor der Nutzung von Internet-Diensten durch entsprechende Anweisungen verpflichtet werden, die einschlägigen Sicherheitsrichtlinien des Unternehmens einzuhalten. Empfehlenswert ist eine betriebsweite schriftliche Richtlinie, die den Umgang der Mitarbeiterinnen und Mitarbeiter mit Internet und E-Mail festlegt.

GEFAHREN BEIM INTERNET-ZUGRIFF

Einige typische Bedrohungen müssen bei der Planung der Sicherheitsmaßnahmen für den Internet-Zugriff berücksichtigt werden.

Beim Herunterladen von Dateien und/oder Programmen kann eine Vielzahl von Sicherheitsproblemen auftreten. Die bekanntesten sind Viren, Makro-Viren, Würmer und trojanische Pferde (Trojaner). Die Benutzerinnen und Benutzer sollten immer die Möglichkeit in Betracht ziehen, dass heruntergeladene Dateien oder Programme Schadsoftware enthalten. Insbesondere das Installieren verschiedener Zusatzprogramme (Bildschirmschoner, Spiele, ...) aus dem Internet sollte unterlassen werden, da diese oft Schadprogramme (insbes. Spyware) enthalten.

Firmendaten werden vor allem durch Programmfunktionen gefährdet, die ohne weitere Nachfrage auf dem lokalen Rechner ausgeführt werden. So können in heruntergeladenen Dokumenten oder Bildern Befehle enthalten sein, die automatisch beim Betrachten ausgeführt werden und Schäden

verursachen können (z.B. Makro-Viren in Word- oder Excel-Dokumenten). Auf allen Rechnern mit Internetzugang müssen daher aktuelle Virenschutzprogramme installiert sein, die diese Dateien bereits beim Download oder beim Zugriff prüfen.

Eine weitere Gefahr besteht in Phishing-Angriffen, bei denen ein Angreifer die Webseite einer Bank oder eines Webshops imitiert, um seine Opfer damit zur Herausgabe von Passwörtern oder geheimen Daten zu bewegen. Solche Angriffe werden üblicherweise durch E-Mail-Aussendungen eingeleitet und sind weit verbreitet. In diesem Zusammenhang ist besonders die Schulung der Benutzerinnen und Benutzer wichtig: Als Grundregel muss dabei gelten, dass kein seriöses Unternehmen via E-Mail zur Eingabe von Passwörtern, PINs oder TANs auffordert. Aussendungen dieser Art müssen daher von den Mitarbeiterinnen und Mitarbeitern als Betrugsversuch erkannt und gemeldet werden. Im Zweifelsfall sollte die Bank oder der Web-Anbieter telefonisch kontaktiert werden.

SICHERHEIT VON WEB-BROWSERN

Verschiedene Sicherheitsprobleme beim WWW-Zugriff entstehen durch Schwachstellen in den eingesetzten Internet-Browsern.

Übliche Ursachen dafür sind:

- Fehlbedienungen und falsches Verhalten der Benutzerinnen und Benutzer
- Unzureichende Konfiguration der benutzten Browser
- Sicherheitslücken in den Browsern

Sicherheit bei WWW-Zugriffen lässt sich nur dann erzielen, wenn jede dieser Problemquellen behandelt wird: Richtiges Verhalten ist mit Sicherheit der wichtigste Punkt; auch die bestgeschulten Benutzerinnen und Benutzer sind aber überfordert, bei den heute möglichen Angriffen immer richtig zu reagieren. Aktuelle Browser können durch Konfigurationsmaßnahmen weitgehend abgesichert werden, allerdings werden die Benutzerinnen und Benutzer dann durch die umständliche Bedienung leicht überfordert und eine Reihe von Webseiten lässt sich nur sehr eingeschränkt oder gar nicht nutzen. Auch die Auswahl eines „sicheren“ Browsers ist nicht möglich, da alle derzeit existierenden Programme gegen spezifische Angriffe anfällig sind und immer wieder neue erfolgreiche Angriffsmethoden gefunden werden.

Eine Abwehrstrategie gegen Sicherheitsprobleme beim WWW-Zugriff muss daher drei Elemente enthalten:

- **Mitarbeiterinnen und Mitarbeiter** müssen **geschult** werden, um Fehlbedienungen zu vermeiden und Gefahren erkennen zu können. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen aus dem Internet und einzuhaltender Sicherheitsmaßnahmen sensibilisiert werden; sie sollten beispielsweise richtig auf Sicherheitsabfragen reagieren oder selbständig gesicherte Verbindungen erkennen können (SSL-Verschlüsselungen). Regelungen und Bedienungshinweise zur sicheren Internet-Nutzung sollten schriftlich fixiert werden.
- Die **Browser** müssen so **konfiguriert** werden, dass ohne weiteres Zutun der Benutzerinnen und Benutzer maximale Sicherheit erreicht werden kann. Dazu sollten die sicherheitsrelevanten Einstellmöglichkeiten genutzt werden, die moderne Browser bieten: Im Internet Explorer sind das insbesondere die Einstellungen des Zonenmodells, in Mozilla Firefox die verschiedenen sicherheitsrelevanten Add-Ons (NoScript, Adblock, Ghostery, ...). Alle aktuellen Browser beinhalten zudem Schutzvorkehrungen gegen Phishing-Angriffe, die unbedingt eingesetzt werden sollten.

Eine SSL-gesicherte Verbindung erkennt man am Schloss-Symbol in der rechten unteren Ecke Ihres Browsers. Durch Doppelklick öffnet sich ein Fenster mit Detailangaben zum Sicherheits-Zertifikat

- **Internet-Browser** müssen immer **auf dem neuesten Stand** gehalten werden; häufig enthalten die Aktualisierungen Maßnahmen gegen neu gefundene Sicherheitslücken. Auch Zusatzprogramme und Plug-Ins (Java, Adobe Flash, …) müssen regelmäßig aktualisiert werden. Dazu muss u.a. auch überlegt werden, wie diese Updates im gesamten Unternehmen durchgeführt werden können, ob dazu der Eingriff einer Administratorin oder eines Administrators nötig ist etc.

Nicht unerwähnt bleiben sollte außerdem die **Tracking- und Datenschutzproblematik:** Sehr viele Websites verfolgen die Internetzugriffe ihrer Besucher mittels Tracking-Cookies, die von großen Werbeanbietern für gezielte Werbung genutzt werden. Diese Anbieter können die erhobenen Daten verwenden, um Bewegungsprofile der Benutzerinnen und Benutzer zu erstellen und ihr Surfverhalten zu verfolgen.

Nach geltendem Recht ist dieses Tracking nur dann zulässig, wenn die Besucher zuvor ihre Zustimmung erteilt haben. In der Praxis lässt es sich aber nur durch entsprechende **Einstellungen im Browser** (Löschen von Cookies beim Beenden der Browsersitzung, „Do Not Track"-Einstellungen) oder durch den Einsatz spezieller **Plug-Ins** (Ghostery, uBlock …) unterbinden.

Die Mitarbeiterinnen und Mitarbeiter sollten auf diese Thematik jedenfalls hingewiesen werden. Ob sie der Nachverfolgung ihrer Internet-Aktivitäten zustimmen, muss ihnen freigestellt werden. Bei Bedarf sollten ihnen entsprechende Informationsmöglichkeiten und Support zur Verfügung gestellt werden.

SOZIALE NETZWERKE

Soziale Netzwerke (Facebook, Xing, Twitter, ...) erfreuen sich weiterhin hoher Beliebtheit und werden immer häufiger auch für geschäftliche Ziele genutzt.

Die Portale ermöglichen es ihren Benutzerinnen und Benutzern, soziale Kontakte zu pflegen und Informationen geschäftlicher oder privater Art auszutauschen. Meist wird dafür ein persönliches Profil mit mehr oder weniger detaillierten Auskünften über die eigene Person, Vorlieben und Überzeugungen erstellt. Mittlerweile nutzen auch viele Unternehmen und deren Mitarbeiterinnen und Mitarbeiter diese sozialen Netzwerke.

Die Nutzung von sozialen Netzwerken durch Unternehmen wird vor allem für Marketing-Zwecke wie zum Beispiel

- Steigerung des Bekanntheitsgrads des Unternehmens oder einer Firmenmarke
- Verbesserung des Firmenimages
- Steigerung der Besucherzahlen auf der Website des Unternehmens
- Akquise neuer oder stärkere Bindung bestehender Kundinnen und Kunden
- Verbesserung von Verkaufszahlen
- Gewinnung neuer Mitarbeiterinnen und Mitarbeiter
- Bessere Kommunikation und Interaktion mit Kundinnen und Kunden

vorangetrieben.

Neben den Vorteilen einer solchen Nutzung durch ein Unternehmen müssen aber auch die potenziellen Risiken bedacht werden:

- Datenabflüsse, bewusstes oder unbewusstes Preisgeben von geschäftlich sensiblen Daten
- Erleichterung von Social Engineering Attacken durch Preisgabe geschäftlicher Informationen
- Einschleusen und Verbreitung von Schadsoftware über soziale Netzwerke
- Kontrollverlust über die transportierten Inhalte
- Offenlegung vertraulicher firmeninterner sowie privater Informationen
- Cyber-Mobbing, d.h. öffentliches Bloßstellen und Herabwürdigen von Personen
- Produktivitätsverlust aufgrund intensiver privater Nutzung durch Mitarbeiterinnen und Mitarbeiter

Die Entscheidung, ob soziale Medien im Rahmen der Unternehmenstätigkeit eingesetzt oder sogar für private Zwecke erlaubt werden, sollte erst nach Abwägen der Vor- und Nachteile im Rahmen einer Risikoanalyse erfolgen:

- Ist der Einsatz sozialer Medien mit der **Unternehmensstrategie** und **-kultur** vereinbar?
  Der Einsatz von sozialen Medien führt zu einem Kommunikationswandel im Unternehmen. Unternehmen, die soziale Medien einsetzen, müssen eine offene Kommunikationskultur pflegen und fördern, um erfolgreich zu sein. Dies kann mit einem Verlust der Kontrolle über publizierte Inhalte einhergehen.

- Können **Sicherheitsrisiken**, die durch Nutzung von sozialen Medien auftreten, ausreichend minimiert werden?
  Über soziale Netzwerke können neue Sicherheitsbedrohungen durch spezifische Schadsoftware oder Betrugsversuche entstehen. Social Engineering-Angriffe stellen eine der am häufigsten angewendeten und erfolgversprechendsten Methoden dar, um an vertrauliche Informationen zu kommen. Vor dem Einsatz von sozialen Medien sollten daher Nutzungsregeln und Richtlinien erarbeitet und den Mitarbeiterinnen und Mitarbeitern kommuniziert werden. Empfohlen werden in diesem Zusammenhang die von der WKÖ entwickelten „Social Media-Guidelines für KMU“, abrufbar unter www.it-safe.at, die unverändert übernommen oder an die Unternehmenserfordernisse angepasst werden können. Zudem muss dafür gesorgt werden, dass die Unternehmensgeräte durch technische Maßnahmen abgesichert werden, sodass keine Schadsoftware von infizierten Webseiten in das Unternehmensnetzwerk gelangen kann.

- Kann der **hohe Verwaltungs- und Betreuungsaufwand** bewältigt werden?
  Soziale Netzwerke leben von der Interaktion mit Kundinnen und Kunden, die ständig neue Inhalte generieren können. Dies birgt aber auch das Risiko, dass Unpassendes, Unsinniges, aber auch Rechtswidriges auf der Unternehmensseite veröffentlicht und der Website-Betreiber dafür verantwortlich gemacht wird. Es ist daher ein laufender Betreuungsaufwand der Website vorzusehen, der nicht unterschätzt werden darf.

KONTROLLFRAGEN

- Haben Sie auf allen Computern Virenschutzprogramme installiert und werden diese laufend (täglich oder öfter) aktualisiert?
- Haben Sie ein fachmännisch installiertes und laufend gewartetes Firewallsystem im Einsatz, dessen Protokolle (Logfiles) regelmäßig überprüft und ausgewertet werden?
- Ist sichergestellt, dass in Ihrem Unternehmen die Betriebssystemkomponenten, Web-Browser und andere Software auf allen Computern laufend und systematisch aktualisiert werden?
- Wurde WLAN in Ihrem Unternehmen fachmännisch installiert und konfiguriert? Erfolgt die Verschlüsselung mittels WPA2? Sind sämtliche WLAN-Passwörter sicher?
- Betreiben Sie ein eigenes Gäste-WLAN für Kunden und Besucher? Gibt es eine Benutzerordnung, in der die wichtigsten Verhaltensregeln festgehalten sind?
- Haben Sie eine schriftliche Internet-Sicherheitsstrategie, mit der Berechtigungen und Bedingungen für den Internet-Zugang festgelegt werden? Wurden die Benutzerinnen und Benutzer entsprechend geschult und existiert eine klar definierte Ansprechperson bei Problemen mit der Internet-Nutzung?
- Haben Sie eine Social Media-Strategie in Ihrem Unternehmen eingeführt, welche die Nutzung sozialer Netzwerke regelt?

7. Datensicherung und Notfallvorsorge

Datensicherung und Notfallwiederherstellungsmaßnahmen helfen bei der Schadensbegrenzung nach Systemausfällen, dem Verlust einzelner Dateien oder im schlimmsten Fall der Zerstörung der gesamten IT-Infrastruktur. Verschiedene, miteinander verknüpfte Maßnahmen sind nötig, um sicherzustellen, dass die IT-Systeme innerhalb eines definierten Zeitraums wieder funktionsfähig sind.

TIPP:

Sie sind nicht sicher, ob Sie Ihre Daten ausreichend gesichert haben? Testen Sie jetzt Ihr Datensicherungskonzept unter www-it-safe.at → „Online-Ratgeber Datensicherung“

Datensicherung

Voraussetzung für jede Notfallvorsorge sind die Planung und Durchführung regelmäßiger Datensicherungen. In vielen Fällen müssen auch die Mitarbeiterinnen und Mitarbeiter zur Einhaltung und Unterstützung der Datensicherungsmaßnahmen verpflichtet werden.

Heute werden oft Technologien eingesetzt, die bestimmte typische Einsatzzwecke von Datensicherungen abdecken: RAID-Laufwerke bieten Schutz vor dem mechanischen Ausfall einzelner Festplatten, Snapshot-Technologien ermöglichen das Wiederherstellen versehentlich gelöschter Dateien. Der Nutzen von Datensicherungen geht aber weit über diese begrenzten Einsatzbereiche hinaus: Sie können bestimmte Datenstände zu Beweisführungszwecken wiederherstellen (Jahres-, Monatssicherungen) oder Daten retten, die von Schadsoftware verfälscht oder zerstört wurden. Vor allem aber ermöglichen sie, die Daten nach schwerwiegenden Vorfällen, wie z.B. einem Brand im Serverraum oder dem Diebstahl von Rechnern, wiederherzustellen. Durch die geringe Größe der Sicherungsmedien ist auch die Auslagerung an einen sicheren Ort ohne großen Aufwand möglich.

DATENSICHERUNGSKONZEPT UND -PLANUNG

*Zunächst sollte in **schriftlicher Form** festgelegt werden, **welche Daten** von **wem** zu **welchem Zeitpunkt** gesichert werden.*

Folgende Punkte müssen dabei in jedem Fall behandelt werden:

- Umfang und Klassifizierung der zu sichernden Daten (Geschäfts- und Produktionsdaten, Systemdateien, Datenbanken, Laufwerke, ...)
- Sicherungstechnologie und -medien (Sicherungsbänder, Wechselfestplatten, Cloud-Speicher, USB-Sticks, CD/DVD, ...)

- Zeitintervall und Zeitpunkt der Sicherungen (täglich, wöchentlich, an Werktagen, ...)
- Anzahl der aufzubewahrenden Sicherungen aus der Vergangenheit
- Zuständigkeit für Durchführung, Überwachung und Dokumentation der Sicherungen
- Aufbewahrung der Backup-Datenträger
- Überprüfung der Datensicherungen, Wiederherstellungstests und -übungen

Voraussetzung regelmäßiger Datensicherungen ist die zentrale Speicherung aller wichtigen Daten, die auch hinsichtlich der Datensicherheit zu empfehlen ist. Benutzerinnen und Benutzer müssen dazu angehalten werden, ihre Daten auf den Servern (und nicht den Festplatten ihrer Arbeitsplatzrechner) abzuspeichern. Vorrangig müssen Geschäfts- und Produktionsdaten (selbst erstellte Daten wie z.B. Dokumente, Kundendatei, Buchhaltung, E-Mail) gesichert werden, außerdem noch eventuelle Konfigurationsdateien der eingesetzten Software. Wichtige Computer, die nach einem Ausfall schnell wieder zur Verfügung stehen müssen, sollten dagegen (z.B. mittels Image-Sicherung) vollständig gesichert werden. Grundsätzlich sind alle Arten von Wechseldatenträgern als Sicherungsmedien geeignet. Im einfachsten Fall kann es ausreichen, die Produktionsdaten wöchentlich auf eine CD-ROM oder DVD zu brennen. Auch externe USB-Festplatten und Cloud-Speicher, eventuell auch USB-Sticks, können verwendet werden.

Allerdings erfordert dieses Vorgehen hohen Arbeits- und Zeitaufwand und lässt sich schlecht automatisieren. Ab einer bestimmten Datenmenge ist es daher sinnvoller, geeignete Sicherungssoftware und spezielle Sicherungslaufwerke einzusetzen. Server-Betriebssystemen liegen einfache Versionen von Backup-Software bei, die bereits ausreichen können. Im Handel erhältliche Sicherungssoftware ist dagegen für komplexe Sicherungsaufgaben (z.B. dem Sichern eines Datenbank- oder Mailservers) besser geeignet und kann mit einer größeren Auswahl verschiedener Sicherungsmedien (z.B. Bandsicherungen) umgehen.

Als Sicherungshardware können **USB-Festplatten** oder **Bandlaufwerke** eingesetzt werden. Die Daten können auch auf einen eigenen Storage-Server (NAS – Network Attached Storage) gesichert werden. Dies ist aber nur dann sinnvoll, wenn dieser räumlich und vor allem brandschutztechnisch von den gesicherten Computern getrennt ist.

Für kleine bis mittlere Datenmengen lässt sich die Möglichkeit der **Online-Datensicherung** nützen. Dabei werden Daten über das Internet zu Anbietern von Cloud-Speicher übertragen, von denen sie im Notfall wieder abgerufen werden können. Der Vorteil dieser Methode ist, dass die Daten außer Haus gespeichert werden und dadurch eine räumliche Trennung der Sicherungen von den Originaldaten gegeben ist. Bei einer Online-Sicherung ist aber großes Augenmerk auf die Seriosität und Sicherheit des Anbieters zu legen: Die Zuverlässigkeit und Verfügbarkeit muss wie bei jedem Cloud-Dienst genau geprüft werden. Wenn sensible Daten auch vor Zugriffen des An-

bieters sicher sein sollen, müssen sie bereits vor der Übertragung verschlüsselt werden. Zu bedenken ist auch, dass der Datentransport über das Internet sehr lange dauern kann, vor allem, wenn nach einem Totalausfall der gesamte Datenbestand wiederhergestellt werden soll.
Verschiedene Datensicherungsmethoden sind möglich:

- **Volldatensicherung:** Bei dieser Methode werden sämtliche zur Sicherung vorgesehenen Dateien einzeln gesichert. Volldatensicherungen sind einfach durchzuführen, und auch die Wiederherstellung der Daten ist einfach. Allerdings verbrauchen sie viel Speicherplatz auf den Sicherungsdatenträgern und dauern lange. Sie sind ideal für unbeaufsichtigte, in der Nacht oder am Wochenende durchgeführte Sicherungsläufe.
- **Inkrementelle Sicherung:** Bei inkrementellen Sicherungen werden nur jene Dateien gesichert, die sich seit der letzten Vollsicherung geändert haben. Da üblicherweise der Großteil der Daten unverändert bleibt, ist der Umfang dieser Datensicherung deutlich geringer. Für die Wiederherstellung werden aber die letzte Volldatensicherung sowie alle darauffolgenden inkrementellen Sicherungen benötigt. Da eine einzige fehlgeschlagene Sicherung ausreicht, um alle darauffolgenden Sicherungen unbrauchbar zu machen, müssen in größeren Abständen (z.B. wöchentlich) zusätzliche Volldatensicherungen durchgeführt werden.
- **Differenzielle Sicherung:** Bei der differenziellen Methode wird zunächst eine Volldatensicherung gemacht. Bei den nächsten Sicherungen werden nur die Dateien, die seit dieser geändert wurden, gesichert. Der Sicherungsumfang ist dadurch höher als bei der inkrementellen, aber niedriger als bei einer Volldatensicherung. Zur Wiederherstellung werden nur mehr zwei Sicherungsmedien benötigt: Das der letzten Volldatensicherung sowie das der letzten differentiellen Datensicherung.
- **Image-Sicherung:** Bei Image-Sicherungen wird ein „Image“ (Speicherabbild) der Festplatte eines Rechners erstellt und auf einen Datenträger gespeichert. Im Bedarfsfall kann der Rechner damit in kurzer Zeit wieder in den exakten Zustand zum Zeitpunkt der Imageerstellung versetzt werden. Diese Methode ist auch für Backups gut geeignet, verbraucht aber ähnlich viel Platz wie eine Volldatensicherung.

Um sicherzustellen, dass die Datensicherung richtig eingerichtet wurde, muss **unbedingt** die Wiederherstellung der gesicherten Daten **getestet** werden. Besonders gilt dies für die Wiederherstellung komplexer Server (Datenbank-, Mailserver, Domänencontroller): Die Notfallwiederherstellung solcher Server, von der neuen Hardware bis zur produktionsreifen Maschine, muss mindestens einmal durchgeführt und dokumentiert werden.

Ohne einen derartigen Test ist es sehr wahrscheinlich, dass im Ernstfall Probleme auftreten, die eine erfolgreiche Wiederherstellung verhindern.

GEEIGNETE AUFBEWAHRUNG DER BACKUP-DATENTRÄGER

Bei der Aufbewahrung der Backup-Datenträger ist aus zwei Gründen besondere Sorgfalt angebracht: Die Entwendung eines Sicherungsmediums würde einem Angreifer den einfachen Zugriff auf die wichtigsten Unternehmensdaten ermöglichen. Und im Katastrophenfall, etwa nach der Zerstörung der IT-Systeme durch einen Brand, sind die Sicherungen die einzige Chance, den elektronisch gespeicherten Datenbestand zu retten.

Folgende Anforderungen sollten erfüllt sein:

- Der **Zugriff** auf Backup-Datenträger darf **nur befugten Personen** möglich sein. Sie sollten idealerweise in einem Safe, jedenfalls aber geschützt gelagert werden. Auch die Sicherungslaufwerke sollten nur den zuständigen Mitarbeitern zugänglich sein, um zu verhindern, dass Medien unbemerkt ausgetauscht werden können.
- Die **Backup-Datenträger** müssen von den gesicherten Rechnern **räumlich getrennt** aufbewahrt werden, um zu vermeiden, dass bei einem Brand, Wasserschaden, Einbruch etc. Computer und Datensicherungen gleichzeitig zerstört werden.
- In regelmäßigen Abständen – z.B. einmal wöchentlich – sollte ein vollständiger **Sicherungssatz** an einen anderen Ort (ein Nebenstandort des Unternehmens, ein Bankschließfach, evtl. auch der Wohnsitz einer Mitarbeiterin oder eines Mitarbeiters) **ausgelagert** werden.
- Im **Notfall** muss es möglich sein, auf die benötigten Sicherungsmedien **ohne größere Verzögerung** zugreifen zu können.

SCHRIFTLICHE AUFZEICHNUNGEN VON KONFIGURATIONSDATEN

Zusätzlich zur eigentlichen Datensicherung sollten verschiedene Konfigurationsdaten ausgedruckt und an sicherer Stelle aufbewahrt werden.

Selbst wenn sämtliche Konfigurationseinstellungen in elektronischer Form gespeichert werden können, ist es von Vorteil, in Notfällen auf Ausdrucke der wichtigsten Einstellungen zurückgreifen zu können. Z.B. sollten die Zugangsdaten zum Internet-Provider, einschließlich der Konfigurationsdetails für den Netzwerkzugang und der Passwörter (z.B. für evtl. Mail-Accounts), gesondert zugreifbar sein. Auch für Konfigurationseinstellungen der Netzwerkrouter und Switches sind schriftliche Aufzeichnungen oder Bildschirmausdrucke bei der Wiederherstellung wichtig.

SICHERUNGSVARIANTEN IM ÜBERBLICK

	Pro	Kontra	Fazit
SICHERUNG AUF EXTERNE FESTPLATTEN, WECHSELFEST-PLATTEN ODER USB-STICKS	Kostengünstig, einfache Bedienung, für annähernd alle Datenarten möglich	Versionsmanagement und räumliche Trennung problematisch, hoher Bedienungsaufwand, teilweise störanfällig	Günstige Einsteigerlösung mit Abstrichen bei der Sicherheit und Bedienungsfreundlichkeit
BANDSICHERUNG	Archivierung sehr einfach, räumliche Trennung leicht möglich, große Datenmengen, gut automatisierbar	Einrichtungs- und Bedienungsaufwand, Anschaffungskosten, teilweise störanfällig	Sehr gut für Volldatensicherungen und Datenarchivierung geeignet
ONLINE-SICHERUNG	Räumliche Trennung, Sicherheit (bei seriösen Anbietern)	Laufende Kosten, eher für kleine Datenmengen geeignet, abhängig von der Qualität der Internetverbindung	Vor allem für einzelne Daten geeignet, kaum für Komplettsicherungen
IMAGESICHERUNG	Sehr schnell, gut für Sicherung kompletter Systeme geeignet, schnelle Wiederherstellung, gut automatisierbar	Wiederherstellung einzelner Dateien teilweise kompliziert, Einrichtungs- und Bedienungsaufwand, Anschaffungskosten	Sehr gut zur Wiederherstellung vollständiger Systeme und Konfigurationen sowie für Volldatensicherungen einzelner Rechner geeignet

Diese Aufzeichnungen müssen an sicherer Stelle, d.h. vor Zerstörung und unbefugten Zugriffen geschützt, gelagert werden. Bei Änderungen an den Einstellungen oder Passwörtern müssen sie umgehend aktualisiert werden.

DATENSICHERUNG BEI MOBILEN IT-SYSTEMEN (NOTEBOOKS, SMARTPHONES ETC.)

Wenn Notebooks oder Smartphones verwendet werden, um wichtige Daten „unterwegs" zu erfassen oder zu bearbeiten, muss dafür gesorgt werden, dass auch die auf diesen Geräten abgelegten Daten gesichert werden.

Dazu bieten sich folgende Verfahren an:

- **Datensicherung auf externen Datenträgern (externe Festplatten, USB-Sticks, DVD-ROMs etc.)**
  Die Datenträger müssen getrennt von den zugehörigen Computern aufbewahrt werden, um den gleichzeitigen Verlust, etwa bei einem Diebstahl, zu verhindern. Die Sicherungsdaten müssen verschlüsselt sein, um Missbrauch beim Verlust eines Sicherungsdatenträgers ausschließen zu können.
- **Datensicherung über Fernverbindung zum Firmennetzwerk**
  Dabei werden die Daten vom Standort der Mitarbeiterin oder des Mitarbeiters zu einem zentralen Firmenserver übertragen. Ausreichende Übertragungsgeschwindigkeit sowie die verschlüsselte Übertragung der Daten sind dafür unbedingte Voraussetzungen. Diese Methode ist daher nur dann einsetzbar, wenn auf der Firewall des Unternehmens verschlüsselte Fernzugänge z.B. für Telearbeit eingerichtet wurden.
- **Datensicherung auf Cloud-Speicher**
  Sicherungsdaten von Mobilgeräten können in der Cloud gespeichert werden, wenn das Unternehmen über eigenen Online-Speicher verfügt. Cloud-Speicher für Privatkunden (iCloud, Google Drive …) ist aber ungeeignet und darf nicht verwendet werden, da Datenverlust auftreten könnte (z.B. bei einem Personalwechsel). Die Mitarbeiterinnen und Mitarbeiter müssen darauf entsprechend hingewiesen werden.
- **Datensicherung bei der Rückkehr ins Firmennetzwerk**
  Dieses Verfahren ist nur dann empfehlenswert, wenn die Mitarbeiterin oder der Mitarbeiter regelmäßig (z.B. wöchentlich) in das Unternehmen zurückkehrt und der mögliche Verlust der zwischenzeitlich geänderten Daten tragbar erscheint.

Die ersten drei Verfahren bringen zusätzlichen Aufwand und Verantwortung für die Benutzerinnen und Benutzer mit sich. Durch den Einsatz geeigneter Software-Tools ist es möglich, den nötigen Arbeitsaufwand zu verringern. Mitarbeiterinnen und Mitarbeiter mit mobilen IT-Systemen müssen aber besonders auf die Wichtigkeit regelmäßiger Datensicherungen und ihre Eigenverantwortung beim Schutz der Daten hingewiesen werden.

Notfallvorsorge und -wiederherstellung

Vor allem in Betrieben, in denen ein großer Teil der Wertschöpfung auf dem Funktionieren der IT-Infrastruktur beruht, ist es wichtig, rechtzeitig Überlegungen zum Abwenden und Bewältigen von Notfällen anzustellen. Notfälle sind kostspielig; ihre Kosten entstehen nicht nur durch Maßnahmen zu ihrer Behebung, sondern vor allem auch durch den Verlust an produktiver Arbeitszeit. Ein Notfallkonzept hilft, diese Ausfallszeiten zu minimieren und möglichst rasch zum normalen Produktionsbetrieb zurückzukehren.

ERHEBUNG DER WICHTIGSTEN ANWENDUNGEN

Erster Schritt jeder Notfallvorsorge ist das Festlegen von Prioritäten für die einzelnen Anwendungen.

Für die Notfallvorsorge ist es unerlässlich, zuerst die Anwendungen mit den höchsten Verfügbarkeitsanforderungen ausfindig zu machen, d.h. jene, bei denen ein längerer Ausfall am wenigsten akzeptabel ist. Im nächsten Schritt müssen jene Teile der IT-Systeme (wie z.B. Server, Daten, Datenleitungen), die für den Betrieb dieser Anwendungen nötig sind, identifiziert werden. Die Notfallplanung sollte sich vorwiegend auf diese zentralen Komponenten konzentrieren.

NOTFALLVORSORGE UND EINGESCHRÄNKTER ERSATZBETRIEB

Bei entsprechender Planung ist es oft möglich, mit relativ kleinem Aufwand Notfälle drastisch zu verkürzen: Ein einziger Ersatzrechner, z.B. ein Firmennotebook, das auch für andere Zwecke genützt werden kann, kann ausreichen, um den Ausfall einzelner PCs vollständig zu überbrücken.

Ersatzrechner müssen nicht den gleichen technischen Leistungsstandards entsprechen wie die Systeme, die sie ersetzen sollen.

Daher können unter Umständen auch alte Rechner, die bereits durch neue Systeme ersetzt wurden, oder auch weniger leistungsstarke und dadurch kostengünstigere Neu-Systeme für solche Aufgaben herangezogen werden. Auch für zentrale Netzwerkkomponenten können Altgeräte zurückbehalten werden.

Ist der Aufwand für die Notfallvorsorge im eigenen Unternehmen zu hoch, sollte eine Auslagerung an externe Dienstleister überlegt werden. So werden etwa für bestimmte Serversysteme (z.B. Web-Shops) Standardlösungen angeboten, die eine hohe Ausfallssicherheit garantieren. Bei der Auslagerung muss besonders auf die vertragliche Gestaltung geachtet werden. Fragen wie Verfügbarkeit, Wiederherstellungszeit, etc. müssen unbedingt in einem sogenannten „Service Level Agreement“ definiert werden.

Häufige Ursache für Notfälle sind Hardwareprobleme, wie z.B. Defekte an Netzteilen oder Festplatten. Für zentrale, wichtige Systeme sollten daher Wartungsverträge abgeschlossen werden, die den Ersatz defekter Komponenten innerhalb einer vereinbarten Zeitspanne sicherstellen. Oft sind derartige Wartungsverträge nur zum Zeitpunkt der Anschaffung der Komponenten günstig erhältlich. Diese Gelegenheit sollte daher möglichst genützt werden.

NOTFALLWIEDERHERSTELLUNG

Für die Rückkehr zum Normalbetrieb ist es notwendig, die ausgefallenen Systemkomponenten wiederherzustellen. Durch das Planen und Testen von Wiederherstellungsverfahren lässt sich dieser Prozess verkürzen und kalkulierbar machen. Vor allem kann dadurch aber vermieden werden, dass sich verschiedene Datenbestände erst beim Wiederherstellungsversuch als nicht mehr rekonstruierbar herausstellen.

Verschiedene Methoden der Notfallwiederherstellung sind möglich: Als erster Schritt werden üblicherweise Betriebssystem und Sicherungssoftware installiert; das kann manuell, skriptgesteuert oder mit Hilfe einer Image-Sicherung erfolgen. Danach werden die Daten aus den letzten Datensicherungen eingespielt, um den Rechner auf aktuellen Stand zu bringen.

Wenn die Datensicherung ausschließlich über Image-Sicherungen erfolgte, ist die Wiederherstellung deutlich einfacher. In diesem Fall wird lediglich die letzte Sicherung aufgespielt; der Zeit- und Manipulationsaufwand ist deutlich geringer. Noch einfacher kann sich – bei entsprechender Grundanlage und Infrastruktur – die Wiederherstellung virtueller Maschinen gestalten. Wesentlich ist, dass die eingesetzten Sicherungs- und Wiederherstellungstechnologien dem tatsächlichen Bedarf entsprechen: Es ist sinnlos, für die selten auftretenden Ausfälle hochwertige und teure Technologie vorzusehen, wenn kein großer Schaden zu erwarten ist. Es gibt aber auch Fälle (z.B. Webshops), wo jede einzelne Minute Ausfallsdauer erhebliche Umsatzeinbußen nach sich zieht oder rechtliche Probleme wie z.B. Haftungsfragen entstehen können. Vor der Entscheidung für eine bestimmte Lösung muss daher eine Risikoabwägung zwischen den möglichen Folgen eines Ausfalls und den Kosten der Sicherungslösung vorgenommen werden.

Um Verzögerungen zu vermeiden, muss dafür gesorgt sein, dass alle benötigte Software im Notfall greifbar und funktionsfähig ist. Eine gute Methode besteht darin, von den Installationsdatenträgern Kopien zu erstellen, die an gleicher Stelle wie die Sicherungsmedien gelagert werden. Auch an dem Ort, an den die Datensicherungsmedien ausgelagert werden (Bankschließfach o.ä.), sollten Kopien deponiert werden.

Häufig zeigen erst praxisnahe Tests der Wiederherstellung, dass die eingesetzte Methode nicht allen Anforderungen entspricht, z.B. nicht für die vollständige Wiederherstellung ausreicht. Die Wiederherstellung hat also oft auch Rückwirkungen auf die Einstellungen der Datensicherung. Um im Notfall sicher und rasch reagieren zu können, müssen die Backup/Restore-Methoden unbedingt detailliert und ausführlich dokumentiert werden. Die ausführliche Dokumentation des Wiederherstellungsverfahrens hilft u.a. in Fällen, in denen die oder der Verantwortliche nicht greifbar ist. Sie sollte ausreichend detailliert sein, um auch anderen technisch versierten Personen die Wiederherstellung zu ermöglichen.

KONTROLLFRAGEN

- Haben Sie einen präzisen Überblick über die Art Ihrer Daten, deren Speicherort sowie die Art, Häufigkeit und den Ort ihrer Sicherung? Werden z.B. auch die Daten Ihrer Office-Anwendung und Ihre E-Mails ausreichend gesichert?

- Haben Sie berücksichtigt, wie schnell sich die zu sichernden Daten verändern? Wissen Sie zum Beispiel, für welche Daten eine regelmäßige Sicherung (z.B. einmal pro Tag) und für welche eine bedarfsweise Sicherung ausreicht?

- Haben Sie eine sinnvolle Auslagerungsstrategie für die Sicherungsdatenträger, um zu verhindern, dass bei einem Vorfall im Serverraum auch die Sicherungen vernichtet werden?

- Haben Sie ein schriftliches Datensicherungskonzept, das festlegt, welche Daten von wem zu welchem Zeitpunkt gesichert werden? Berücksichtigt das Konzept auch allfällige mobile IT-Systeme? Sind Ihre Mitarbeiterinnen und Mitarbeiter über dieses Konzept ausreichend informiert?

- Haben Sie ein schriftliches Notfallkonzept, das festlegt, wer im Notfall informiert werden muss, wie und innerhalb welcher Zeiträume die Datenwiederherstellung abläuft und wer welche Verantwortung trägt? Wird das Notfallkonzept inklusive der Datenwiederherstellung in regelmäßigen Abständen (mindestens einmal jährlich) einem Test unterzogen?

8. Bauliche und infrastrukturelle Maßnahmen

Die in diesem Abschnitt beschriebenen Maßnahmen dienen dem Schutz von IT-Systemen mittels baulicher und infrastruktureller Vorkehrungen.

Baulich-organisatorische Maßnahmen

SCHÜTZENSWERTE GEBÄUDETEILE

Besonders schützenswerte Räume (Serverräume, Datenträgerarchive etc.) sollten nicht in exponierten oder gefährdeten Bereichen untergebracht sein.

Insbesondere ist zu beachten:

- Kellerräume sind durch Wasser gefährdet;
- Räume im Erdgeschoß – zu öffentlichen Verkehrsflächen hin – sind durch Vandalismus und höhere Gewalt (Verkehrsunfälle in Gebäudenähe) gefährdet;
- Räume im Erdgeschoß mit schlecht einsehbaren Höfen sind durch Einbruch und Sabotage gefährdet;
- Räume unterhalb von Flachdächern sind durch eindringendes Regenwasser gefährdet.

Im Allgemeinen sind schutzbedürftige Räume im Zentrum eines Gebäudes besser untergebracht als in dessen Außenbereichen; das ist bei der Planung neuer Räume für sensible oder betriebswichtige Komponenten zu berücksichtigen. Wenn die zentrale Anlage solcher Schutzbereiche aufgrund der bestehenden Bausubstanz oder Leitungsführung nicht möglich sein sollte, müssen zusätzliche Schutzmaßnahmen zur Abwehr der oben angeführten Gefährdungen eingerichtet werden (Wassermelder, Alarmanlagen, Fenstergitter etc.).

ZUTRITTSKONTROLLE

Die Überwachung des Zutritts zum Gebäude bzw. zu sensiblen Bereichen zählt zu den wichtigsten Schutzmaßnahmen. Ein Zutrittskontrollsystem vereinigt verschiedene bauliche, organisatorische und personelle Vorkehrungen.

In einem Zutrittskontrollkonzept sollten u.a. folgende Inhalte festgehalten werden:

- **Welche** Bereiche sind besonders **schützenswert** (Serverräume, Archive, Räume für Kommunikationseinrichtungen oder Haustechnik etc.)? Die einzelnen Bereiche können unterschiedliche Sicherheitsstufen aufweisen.
- **Welche internen und externen Personengruppen** haben Zutritt zu welchen Bereichen?
- **Welche Daten** müssen bei Betreten und Verlassen eines geschützten Bereichs **protokolliert** werden?

Aus diesen Festlegungen lassen sich Anforderungen für Zutrittskontrollmaßnahmen ableiten, die z.B. bei der Auswahl einer Schließlösung, der Schlüsselvergabe, der Planung von Alarmanlagen oder der Führung von Zutrittslogbüchern beachtet werden müssen.

SCHLÜSSELVERWALTUNG

Alle Maßnahmen und Informationen, die in Zusammenhang mit der Schlüsselvergabe stehen, sollten in einem Schließplan dokumentiert werden.

Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln muss zentral geregelt werden. Reserveschlüssel sind vorzuhalten und gesichert aufzubewahren. Schlüssel dürfen nur an berechtigte Personen ausgegeben werden; es ist also ein ausgearbeitetes Zutrittskontrollkonzept nötig.

Über die Aus- und Rückgabe aller Schlüssel müssen schriftliche Aufzeichnungen geführt werden. Anhand dieser Listen sollte es jederzeit möglich sein, nachzuvollziehen, wer zu welchem Zeitpunkt Zutritt zu welchen Unternehmensbereichen hatte. Aus diesem Grund sollte es auch den Mitarbeiterinnen und Mitarbeitern verboten sein, ihre Schlüssel anderen zu überlassen; jede Schlüsselausgabe muss über die zentrale Ausgabestelle erfolgen.

Für den Verlust von Schlüsseln sollte ebenfalls vorgesorgt werden: Jeder Mitarbeiterin und jedem Mitarbeiter muss bekannt sein, wer in diesem Fall zu verständigen ist. Eine Reihe von Maßnahmen – vom Ersatz des Schlüssels bis zum Austausch des Schlosses oder ganzer Schließgruppen – sollte von den zuständigen Verantwortlichen durchgeplant werden.

Das Gleiche gilt sinngemäß auch für alle anderen Zutrittskontrollmedien wie Magnetstreifen oder Chipkarten bzw. so genannte Multifunktionschipkarten.

EMPFANG

Die Einrichtung eines Empfangsdienstes (Portier, Front-Sekretariat etc.) hat weit reichende positive Auswirkungen gegen eine ganze Reihe von Gefährdungen.

Voraussetzung ist allerdings, dass bei der Umsetzung des Empfangsdienstes einige Grundprinzipien beachtet werden, die auch für vermeintlich vertrauenswürdige Personen (z.B. ehemalige Mitarbeiterinnen und Mitarbeiter) gelten müssen.

- Die Mitarbeiterinnen und Mitarbeiter am Empfang beobachten und kontrollieren den Eingang zum Gebäude/Büro bzw. zu sicherheitsrelevanten Bereichen.
- Unbekannte Personen müssen sich beim Empfang anmelden und ausweisen.
- Der Empfangsdienst hält vor Einlass fremder Personen bei der oder dem Besuchten Rückfrage.
- Besucherinnen und Besucher werden am Eingang abgeholt und nach dem Besuch wieder hinausbegleitet.

GEEIGNETE AUFSTELLUNG UND AUFBEWAHRUNG VON SERVERN UND ANDEREN BESONDERS SCHÜTZENSWERTEN IT-KOMPONENTEN

Aufgrund ihrer zentralen Funktion für das Unternehmen müssen Server besonders geschützt werden. Ähnliches gilt auch für zentrale Netzwerk- und Telekommunikationskomponenten (Router, Switches, Firewalls, Telefonanlage).

Um den Schutz solcher besonders betriebswichtigen IT-Komponenten sicherzustellen, ist es zwingend erforderlich, diese in einer gesicherten Umgebung aufzustellen. Diese kann realisiert werden als:

- **Serverraum:** Raum zur Unterbringung von Servern, serverspezifischen Unterlagen, Datenträgern in kleinem Umfang sowie weiterer Hardware (etwa Drucker oder Netzwerkkomponenten). Im Serverraum ist im Allgemeinen kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten. Ein Serverraum muss Schutz vor unbefugtem Betreten bieten, spezielle Vorrichtungen wie z.B. Brandschutztüren können darüber hinaus im Fall eines Brandes die Sicherheit der Geräte und Daten erhöhen.
- **Serverschrank:** Versperrbare Serverschränke (Racks) dienen zur Unterbringung von IT-Geräten und schützen sie gegen unbefugten Zugriff. Der Schutz vor Schäden durch Feuer und Rauchgasen ist bei den meisten Serverschränken dagegen nicht gegeben.

Generell ist zu beachten:

- Der Zugang zu Servern und anderen schützenswerten Komponenten darf ausschließlich wenigen, befugten Personen möglich sein.
- Eine Vertretungsregelung muss sicherstellen, dass der Zugriff auch im Vertretungsfall geregelt möglich ist und nicht autorisierte Zugriffe auch in Ausnahmesituationen nicht vorkommen können.
- Für die sichere Verwahrung der Zugangsschlüssel muss gesorgt sein. Außerdem muss darauf geachtet werden, dass die entsprechenden Räume bzw. Schränke tatsächlich immer versperrt werden.

Brandschutz

Brandschutz stellt die Gesamtheit aller Maßnahmen dar, die die Entstehung und Ausbreitung von Bränden verhindern und die Bekämpfung von Bränden gewährleisten.

Bei systemkritischen Räumen (Serverräume, Verteilerräume) ist der Einsatz von Brandschutztüren zur Bildung eines eigenen Brandabschnitts sowie von Sicherheitstüren, die einen höheren Schutz gegen Einbruch bieten, vorzusehen.

Brandmeldeanlagen ermöglichen die Überwachung bestimmter, besonders gefährdeter Bereiche oder des gesamten Gebäudes. Brandmelder dienen zur Früherkennung von Brandgefahren und werden in automatische und nichtautomatische Melder unterschieden, welche an einer Brandmeldeanlage hängen oder als Einzelmelder fungieren.

In Räumen mit Computern oder Datenträgern, in denen Brände oder Verschmutzungen hohe Schäden verursachen können, sollte ein Rauchverbot erlassen werden. Dieses Rauchverbot dient gleichermaßen dem vorbeugenden Brandschutz wie der Betriebssicherheit. Die Einhaltung des Rauchverbotes ist zu kontrollieren.

Papier und andere leicht brennbare Materialien müssen unbedingt außerhalb der systemkritischen Räume (Serverraum, Verteilerraum) gelagert werden, um die Brandlast möglichst gering zu halten.

HANDFEUERLÖSCHER (MITTEL DER ERSTEN UND ERWEITERTEN LÖSCHHILFE)

Die meisten Brände entstehen aus kleinen, anfangs noch gut beherrschbaren Brandherden. Besonders in Büros findet das Feuer reichlich Nahrung und kann sich sehr schnell ausbreiten. Der Sofortbekämpfung von Bränden kommt also sehr hoher Stellenwert zu.

Eine Sofortbekämpfung ist nur möglich, wenn entsprechende Handfeuerlöscher in ausreichender Zahl und Größe im Gebäude – möglichst in räumlicher Nähe zu besonders schützenswerten Bereichen und Räumen – zur Verfügung stehen.

Dabei ist zu beachten:

- Die Feuerlöscher müssen **regelmäßig geprüft und gewartet** werden.
- Die Feuerlöscher müssen so angebracht werden, dass sie im Brandfall leicht erreichbar sind.
- Zur Brandbekämpfung bei IT-Geräten dürfen ausschließlich **CO_2-Löscher** eingesetzt werden; dabei muss auf die Gefahr der Sauerstoffverdrängung geachtet werden.
- Die Beschäftigten müssen über die Standorte der nächsten Feuerlöscher **informiert** und in deren Handhabung **unterwiesen** sein.

Im Brandfall geht von der damit verbundenen Rauchentwicklung sowohl für Mensch als auch für IT-Geräte eine erhebliche Gefahr aus. Ein umfassender Rauchschutz, z.B. durch rauchdichte Brandschutztüren, ist daher ebenfalls vorzusehen.

Stromversorgung und Klimatechnik

ANGEPASSTE AUFTEILUNG DER STROMKREISE

Eine unterdimensionierte Stromversorgung kann zu Computer-Abstürzen führen, die Datenverlust verursachen können.

Die Dimensionierung, für die eine Elektroinstallation ausgelegt wurde, stimmt erfahrungsgemäß nach einiger Zeit nicht mehr mit den tatsächlichen Gegebenheiten überein. Vor der Anschaffung neuer IT-Komponenten sollte daher die Elektroinstallation geprüft und gegebenenfalls angepasst werden. Dabei müssen auch eventuell erforderliche Änderungen der Klimatisierung berücksichtigt werden.

LOKALE UNTERBRECHUNGSFREIE STROMVERSORGUNG (USV)

Die Überbrückung von Stromausfällen durch eine USV sowie das geordnete Herunterfahren der angeschlossenen Geräte beugt Datenverlusten vor, die in Folge von plötzlichem „Ausschalten" (Stromverlust) entstehen können.

USV-Anlagen können neben der Überbrückung von Totalausfällen der Stromversorgung und Unterspannungen auch dazu dienen, Überspannungen (z.B. durch Blitzschlag) zu glätten. Zumindest alle betriebswichtigen Server sowie die Sicherheits- und Alarmsysteme sollten an einer USV betrieben werden.

Empfehlenswert ist auch der Anschluss eines Monitors für die betreffenden Server, um während eines Stromausfalls noch manuell eingreifen zu können.

Bei der Dimensionierung einer USV sollte man von einer Überbrückungszeit von mindestens 10 bis 15 Minuten ausgehen. In dieser Zeit kann die angeschlossene IT ohne externe Stromquelle betrieben oder geordnet heruntergefahren werden. Das Herunterfahren muss dabei von einer Softwarelösung automatisch ausgelöst werden. In regelmäßigen Abständen sollten Tests durchgeführt werden, bei denen die Funktion der USV-Anlage und der automatischen Serverabschaltung überprüft wird. Dies kann z.B. im Rahmen der regelmäßigen Prüfung der Stromversorgungsanlage erfolgen.

KLIMATISIERUNG

Insbesondere in kleinen Serverräumen muss für die ausreichende Abfuhr der Rechnerabwärme gesorgt werden.

Server sind für den Betrieb innerhalb eines engen Temperaturbereichs ausgelegt. Oberhalb ihrer maximalen Betriebstemperatur (meistens 30-35 °C) besteht die Gefahr des Rechnerausfalls. Diese Temperatur kann gerade in kleinen, durch Brand- oder Zutrittsschutzmaßnahmen zusätzlich abgeschotteten Serverräumen, leicht überschritten werden. In solchen Fällen ist der Einbau einer Klimaanlage zwingend erforderlich.

Bei der Auswahl des Klimageräts muss auf die ausreichende Kälteleistung geachtet werden. Dabei sollte auch die Möglichkeit der Anschaffung zusätzlicher Server mit bedacht werden, die zusätzliche Kühlung nötig machen. Oft ist eine Überdimensionierung empfehlenswert, um nicht bei zukünftigen Anschaffungen gleich auch die Klimaanlage wechseln zu müssen.

Zum Schutz der Serversysteme sollte außerdem eine Raumtemperaturüberwachung überlegt werden, die bei Überschreiten einer bestimmten Grenztemperatur per E-Mail oder SMS Alarmmeldungen aussendet.

KONTROLLFRAGEN

- Haben Sie beim Aufstellen Ihres Servers oder für Ihre Datenträgerarchive bauliche Risiken (z.B. Wassereinbruch, Brandgefahr, Diebstahlgefahr) berücksichtigt? Ist der Zutritt zu kritischen IT-Komponenten gesichert und geregelt?

- Haben Sie ein schriftliches Zutrittskontrollkonzept und eine entsprechende Schlüsselverwaltung? Sind Sie sicher, dass das Zutrittskontrollkonzept in der Praxis berücksichtigt wird und werden Kontrollen durchgeführt?

- Wenn Sie einen Empfangsdienst haben, wurden die dort tätigen Mitarbeiter über ihre Kontrollfunktion geschult und gibt es definierte Verfahren zum Umgang mit Besuchern?

- Haben Sie angemessene Brandschutzmaßnahmen wie etwa Brandmelder und Handfeuerlöscher für systemkritische Räume vorgesehen? Gibt es ein Verbot des Hantierens mit leicht brennbaren Materialien in kritischen Räumen und wird es auch kontrolliert?

- Ist die Stromversorgung Ihrer IT-Komponenten angemessen und betreiben Sie gegebenenfalls eine Anlage zur unterbrechungsfreien Stromversorgung? Ist die ausreichende Klimatisierung des Serverraums sichergestellt?

9. Suchen Sie einen Sicherheits-Experten? WKO IT Security ExpertsGroup

Die IT-Security ExpertsGroup WKÖ ist eine ehrenamtliche Arbeitsgruppe mit über 180 aktiven Mitgliedern, gehört zur Fachgruppe UBIT und führt jene IT-Dienstleister zusammen, die sich dem Thema der Informationssicherheit in all ihren Formen verschrieben haben.

Neben dem Networking- und Kooperationsgedanken findet auch ein reger Know-How-Transfer sowie Erfahrungsaustausch innerhalb der Gruppe statt. Darüber hinaus ist die ExpertsGroup bemüht, aktuelle Themen aufzubereiten und weiterzuentwickeln. Beispielsweise wird der Umgang mit der DSGVO, der NIS-Richtlinie uvm. behandelt.

Die IT-Security ExpertsGroup WKÖ veranstaltet mehrmals im Jahr Konferenzen, Seminare sowie regelmäßige Mitgliedertreffen. Die Aktivitäten sind auch überregional bemerkbar, indem Sitzungen und Veranstaltungen bewusst in den Bundesländern veranstaltet werden. Ein Beispiel für nachhaltige Projekte ist die **Cyber-Security-Hotline** der Wirtschaftskammern Steiermark, Kärnten, Burgenland, Vorarlberg, Oberösterreich und Tirol.

Wenn Ihr Unternehmen Opfer einer Cyberattacke, eines Cybercrime Angriffs, von Ransomware und Verschlüsselungstrojanern wurde, bekommen Sie unter 0800 888 133 eine telefonische, kostenlose Notfallhilfe.

Der Expertenpool wird von der IT-Security ExpertsGroup gestellt.

Ziele:

- Schaffung von Awareness
- Schnittstelle für Sicherheitsprobleme
- Aufbereitung branchenrelevanter Themengebiete
- Plattform für Sicherheitsaktivitäten
- Anlaufstelle für Security-Herausforderungen

Themenschwerpunkte:

- Risikomanagement & Einhaltung rechtlicher Vorgaben
- IT-strategische Überlegungen
- Sicherer Umgang mit Computern und Informationen
- Computerhardware- und Netzwerksicherheit

- Personelle Maßnahmen
- Bauliche und infrastrukturelle Sicherheit
- Sicherheit für Jugendliche und Erwachsene im Internet
- E-Mailverschlüsselung und Kryptografie
- DSGVO
- Internet of Things
- Gefährliche Schadprogramme
- Datensicherung und Notfallvorsorge
- NIS-Richtlinie

FINDEN SIE EINEN IT-SECURITY EXPERT IN IHRER NÄHE: HTTPS://FIRMEN.WKO.AT/WEB/UBIT

Im UBIT Firmen A-Z können Sie gezielt mit Hilfe der erweiterten Auswahlkriterien nach Fachleuten der IT-Security ExpertsGroup suchen.

KONTAKTDATEN:

© Foto Fischer

Leitung der IT Security ExpertsGroup WKÖ auf Bundesebene:
DI Gerald Kortschak, BSc. CMC
Sprecher IT Security ExpertsGroup WKÖ

© Wenisch

Landesprecher IT Security ExpertsGroup WK Steiermark
Harald Wenisch
Sachverständiger für IT und Sicherheitsfragen
stv. Sprecher IT Security ExpertsGroup WKÖ
Landesprecher IT Security ExpertsGroup WK Wien

Hier finden Sie die jeweiligen Landessprecher mit Ihren Kontaktdaten. In den Bundesländern sind regionale Arbeitskreise der IT-Security Experts Group aktiv, um die regionalen Interessen der Mitglieder direkt vertreten zu können.

Wien	Harald Wenisch E-Mail: harald.wenisch@wenisch-consulting.com
Niederösterreich	Christopher Leder MSc E-Mail: uplink@satellite-telecom.net
Oberösterreich	Erik Rusek E-Mail: erik.rusek@awarity.at
Salzburg	Martin Schober E-Mail: ms@martinschober.com
Burgenland	Norbert Freissmuth E-Mail: office@inoha.com
Steiermark	Gerald Kortschak E-Mail: office@itsecurityexperts.at
Kärnten	Thorsten Jost E-Mail: thorsten.jost@secriso.com
Vorarlberg	Wolfgang Hödl E-Mail: office@profit-management.at
Tirol	Alfred Gunsch E-Mail: alfred.gunsch@siplan.at

10. Glossar

AKTIVE INHALTE:

Als aktive Inhalte werden von einem Webserver an den Internet-Browser übermittelte Programme/ Skripte bezeichnet, die anschließend auf dem PC lokal ausgeführt werden. Bekannte Vertreter sind ActiveX, Javascript und Java. Üblicherweise dienen sie zur Erleichterung der Webseitenbedienung oder steigern die Attraktivität durch spezielle Effekte. Sie können aber auch eingesetzt werden, um Schadroutinen auszuführen und sind als Sicherheitsrisiko anzusehen.

BYOD:

BYOD (Bring Your Own Device, d.h. „Bring dein eigenes Gerät“) ist eine Strategie, Kosten einzusparen und die Mitarbeitermotivation anzuheben, indem die Verwendung privater IT-Geräte wie Smartphones oder Notebooks für berufliche Zwecke zugelassen wird. Dabei entstehen allerdings verschiedene Probleme in rechtlicher und sicherheitstechnischer Hinsicht, die vor dem Einsatz unbedingt geklärt werden müssen.

DDOS-ATTACKE:

Unter DDoS- (Distributed Denial of Service = Verweigerung des Dienstes)Attacke versteht man einen Angriff einer Vielzahl von Rechnern auf einen Computer mit dem Ziel, dessen Verfügbarkeit durch Überlastung außer Kraft zu setzen.

KRYPTOTROJANER:

Krypto- oder Verschlüsselungstrojaner verschlüsseln auf befallenen PCs verschiedenste Arten von Dateien wie z.B. Office-Dokumente, PDF-Dateien, Bild- und Musikdateien, Dateiarchive etc. Eine Möglichkeit zur Entschlüsselung wird gegen Zahlung an den Angreifer angeboten, häufig funktioniert diese aber nicht und ist technisch gar nicht vorgesehen. Hinsichtlich der Einfallswege unterscheiden sich Kryptotrojaner nicht von anderer Schadsoftware.

NEXT GENERATION-FIREWALL:

Als Next Generation-Firewalls werden Geräte bezeichnet, die zusätzlich zur Schutzwirkung einer traditionellen Firewall vertiefte Prüf- und Eingriffsmöglichkeiten auf Applikationsebene bieten. Damit können z.B. einzelne Anwendungen blockiert oder nur für bestimmte Benutzer freigegeben werden, weiters kann auch bei verschlüsselten Verbindungen der Download von Schadsoftware blockiert werden.

PDA:

Ein Personal Digital Assistant (PDA) *(englisch für persönlicher digitaler Assistent)* ist ein kleiner tragbarer Computer, der neben vielen anderen Programmen hauptsächlich für die persönliche Kalender-, Adress- und Aufgabenverwaltung benutzt wird.

PHISHING:

Phishing ist ein Kunstwort aus den beiden Begriffen „Password“ und „Fishing“ und bezeichnet den Versuch, mittels gefälschter E-Mails an fremde Nutzerdaten (Login, Passwort, TAN etc.) zu gelangen. Üblicherweise wird die Empfängerin oder der Empfänger eines solchen Mails unter Vorspiegelung falscher Tatsachen (Userdaten gingen verloren, Neuidentifikation ist notwendig …) aufgefordert, die Webseite einer Bank (Online Shop, Kreditkarteninstitut, Auktionshaus etc.) aufzusuchen und dort Zugangsberechtigungen einzugeben. Diese Webseiten sind ebenfalls gefälscht und sehen den Originalen zum Verwechseln ähnlich. Die eingegebenen Daten landen auf den Servern von Betrügern, die mit den Nutzerdaten Transaktionen zum Schaden der User durchführen.

QUARANTÄNE:

In Analogie zum medizinischen Begriff bezeichnet man damit jenen „Ort“, wo mit Schadprogrammen infizierte Daten aufbewahrt werden. Anti-Virenprogramme verlagern Dateien in die Quarantäne, um die Schadroutine eventuell zu einem späteren Zeitpunkt zu entfernen.

RAID:

Ein RAID-System dient zur Organisation mehrerer physischer Festplatten eines Computers zu einem logischen Laufwerk, das eine größere Speicherkapazität, eine höhere Datensicherheit bei Ausfall einzelner Festplatten und/oder einen größeren Datendurchsatz erlaubt als eine physische Platte. Bei RAID-Systemen werden gezielt redundante Informationen erzeugt, damit beim Ausfall einzelner Komponenten das RAID als Ganzes seine Funktionalität und somit auch die gespeicherten Daten behält.

RANSOMWARE:

Als RANSOMWARE (ransom, eng.: Lösegeld) bezeichnet man Schadsoftware, die entweder die Benutzung des Computers oder den Zugriff auf wichtige Dateien verhindert und erst nach Zahlung an den Angreifer wieder freigibt. Typische Vertreter dieser Kategorie sind Verschlüsselungstrojaner, die wichtige Dateien verschlüsseln und damit unbrauchbar machen. Eine Entschlüsselung ist erst nach Durchführung einer anonymen Geldanweisung an den Angreifer, z.B. via Bitcoin, möglich. Es ist aber keineswegs sicher, dass sie wirklich funktioniert.

ROOTKITS:

Rootkits sind Schadprogramme, die in der Lage sind, sich auf einem Rechner vollständig unsichtbar zu machen. Sie verbergen sich vor Antivirusprogrammen und Benutzereinblicken und werden oft erst durch den entstandenen Schaden auffällig, z.B. wenn der Provider den Internetzugang sperrt, weil Spam-Mails verschickt wurden. Häufig dienen sie auch zum Verstecken von „Hintertüren“, mit deren Hilfe das Fernsteuern des Rechners möglich ist, um ihn für Hack-Angriffe auf

andere Rechner zu missbrauchen. Rootkits werden durch Computerviren oder durch die Installation zweifelhafter Software eingeschleppt. Ihre Entdeckung und Entfernung ist schwierig; im Internet findet man aber verschiedene (häufig kostenlose) Anti-Rootkit-Programme, die dazu in der Lage sind.

SMARTPHONE:

Als Smartphones bezeichnet man Mobiltelefone, die zusätzlich Computerfunktionalität aufweisen. Aktuelle Smartphones verfügen über hochauflösende Touchscreens und können mittels Programmen von Drittanbietern (Apps aus geschützten Quellen) in ihrem Funktionsumfang erweitert werden. Häufig besitzen sie zusätzliche Sensoren (insbes. GPS-Empfänger) und eine eingebaute Digitalkamera. Aufgrund ihrer hohen Flexibilität und Leistungsfähigkeit sind sie für den betrieblichen Einsatz attraktiv, wobei allerdings ähnliche Sicherheitsvorkehrungen wie bei anderen tragbaren Computern getroffen werden sollten.

SOZIALE NETZWERKE:

Soziale Netzwerke sind Netzgemeinschaften, die meist über Internetportale zugänglich sind. Über das Portal können Benutzerinnen und Benutzer eigene Inhalte erstellen und austauschen. Typische soziale Netzwerke bieten die Möglichkeit, Profile über die eigene Person, Vorlieben und Interessen anzulegen, sowie Kontakte zu anderen Benutzerinnen und Benutzern herzustellen und mit diesen zu kommunizieren.

SNAPSHOT:

Snapshot-Technologien dienen zur Aufbewahrung älterer Versionen eines Datenbestands, mit deren Hilfe eine versehentlich überschriebene Datei ohne großen Aufwand wieder hergestellt werden kann. Snapshots können aber auch von ganzen Datenträgern gemacht werden. Insbesondere größere Speichersysteme (Storage Area Networks) nutzen diese Möglichkeit, um Datensicherungen zu beschleunigen.

SPAM:

Als Spam werden unerwünschte Werbemails bezeichnet, die mittlerweile einen Großteil des weltweiten E-Mail-Verkehrs ausmachen. Auch bei kleineren Unternehmen ist es durchaus möglich, mehrere hundert Spam-Mails pro Tag zu erhalten. Gefährlich ist Spam grundsätzlich nicht, er kostet allerdings Arbeitszeit und Internet-Bandbreite. Mittels eigener Spam-Filter können bereits auf Provider/Mailserver-Ebene oder auch erst am lokalen Rechner unerwünschte Mails gefiltert und gelöscht werden.

SPYWARE:

Programme, die unbemerkt das Surfverhalten ausspionieren. Diese Daten werden an den Hersteller der Software oder auch an Dritte, meist mit dem Zweck, personalisierte Werbung und Pop-ups einzublenden, weitergeleitet. Mittels Spyware können aber auch sensible persönliche Daten an Unbefugte übertragen werden.

SSL/HTTPS:

HTTPS ist die Abkürzung für HyperText Transfer Protocol Secure, das durch die Verwendung des Verschlüsselungsverfahrens SSL ausreichende Sicherheit für die Übertragung sensibler Daten bietet. Mit Hilfe dieses Verfahrens werden einerseits die übertragenen Daten verschlüsselt und abhörsicher gemacht, andererseits wird durch die Verwendung von digitalen Zertifikaten die Identität des Webservers gesichert. Einem Angreifer sollte es – richtige Handhabung vorausgesetzt – nicht möglich sein, sich z.B. als E-Banking-Server auszugeben, um Benutzerinnen und Benutzern ihre Passwörter, PINs oder TANs zu entlocken.

TABLET:

Tablet-Computer sind tragbare Computer, die mittels Finger oder Stift über einen Touchscreen bedient werden. Sie entsprechen in weiten Teilen modernen Smartphones, so können z.B. aus geschützten Quellen Apps installiert werden. Durch die im Vergleich zu Smartphones größere Bildschirmoberfläche ist aber die Verwendung als Eingabegerät (mit Hilfe einer virtuellen Bildschirmtastatur) deutlich einfacher. Für Tablet-Computer gelten im Wesentlichen die gleichen Sicherheitshinweise wie für Smartphones.

TROJANISCHE PFERDE:

Selbständige Programme mit verdeckter Schadensfunktion, ohne Selbstreproduktion. Trojaner tarnen sich als nützliche, gutartige Programme: Ein Programm, das zum Zweck der Viren-Entfernung aus dem Internet heruntergeladen wird, kann so unter Umständen genau das Gegenteil bewirken. Daher sollte immer die Seriosität der Quelle, von der ein Programm bezogen wird, überprüft werden.

VERSCHLÜSSELUNGSTROJANER:

Verschlüsselungs- oder Kryptotrojaner verschlüsseln auf befallenen PCs verschiedenste Arten von Dateien wie z.B. Office-Dokumente, PDF-Dateien, Bild- und Musikdateien, Dateiarchive etc. Die Entschlüsselung ist erst nach Zahlung an den Angreifer möglich, häufig funktioniert sie aber nicht und ist technisch auch gar nicht vorgesehen. Verschlüsselungstrojaner unterscheiden sich ansonsten nicht von anderer Schadsoftware. Es gelten auch dieselben Vorsichtsmaßnahmen zur Abwehr.

VIREN:

Nicht-selbständige, in andere Programme oder Dateien eingebettete Programmroutinen, die sich selbst reproduzieren und dadurch Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornehmen.

VIRTUALISIERUNG:

Mit Virtualisierung wird die Erstellung von „künstlichen“ (virtuellen) Ressourcen bezeichnet. So können insbesondere auf einem einzelnen physischen Servers (des „Hosts“) mehrere virtuelle Server (manchmal als „Guests“ bezeichnet), die voneinander weitestgehend unabhängig sind, eingerichtet werden. Dadurch können Energie- und Hardwarekosten reduziert und ausfallsichere Serverlösungen eingerichtet werden.

WEP:

WEP (Wired Equivalent Privacy) ist ein veraltetes Verschlüsselungsprotokoll für Drahtlosnetzwerke. Es weist verschiedene Schwachstellen auf, die genützt werden können, um unbefugt in das Netzwerk einzudringen. Es sollte daher nicht mehr eingesetzt werden.

WPA UND WPA2:

WPA und WPA2 sind Sicherheitsstandards für Drahtlosnetzwerke, die zusichern sollen, dass sich ausschließlich zugelassene Geräte und Personen mit dem Netzwerk verbinden können. Beide gelten derzeit als sicher, sofern ein ausreichend langes, komplexes und nicht erratbares Passwort als Pre-Shared-Key (PSK) eingesetzt wird. WPA2 bietet als Nachfolger von WPA etwas bessere Sicherheit und sollte im Zweifelsfall vorgezogen werden.

WÜRMER:

Selbständige, selbst reproduzierende Programme, die sich in einem System (vor allem in Netzen) ausbreiten. Zu diesem Zweck verwenden viele Würmer das Adressbuch des infizierten Rechners und versenden Mails mit gefälschten Absenderadressen. Das Öffnen solcher Mails kann bei einem ungeschützten System zu einer Infizierung führen.

it-safe.at

IST IHR BETRIEB IT-SAFE?

Jetzt kostenlos herausfinden:
Mit den Online-Ratgebern auf www.it-safe.at

IT-Sicherheit ist für jedes Unternehmen überlebenswichtig!

Mit der Initiative „it-safe.at“ bietet die WKÖ vor allem kleinen und mittleren Unternehmen (KMU) sowie Ein-Personen-Unternehmen (EPU) Hilfestellung:

- Online-Ratgeber it-safe
- Online-Ratgeber Datensicherung
- EPU-Checkliste
- Sicherheits-Handbücher
- News und Tipps im it-safe Blog

Gemeinsam gehen wir’s an und machen auch Ihr Unternehmen IT-sicher: **www.it-safe.at**

bmwfw
Bundesministerium für Wissenschaft, Forschung und Wirtschaft

Der Online-Ratgeber it-safe ist ein gemeinsames Service von BMWFW und WKÖ.

WKO
WIRTSCHAFTSKAMMER ÖSTERREICH