Der IT-Beauftragte
der Bayerischen Staatsregierung

Leitfaden zur Informationssicherheit

in kleinen und mittleren Unternehmen

IHK Industrie- und Handelskammern in Bayern

Aufbruch Bayern

Rund 600.000 kleine und mittlere Unternehmen in Bayern sind das Rückgrat und der Motor unserer Wirtschaft. Sie schaffen 3,2 Millionen Arbeitsplätze und setzen jährlich 900 Milliarden Euro um. Mit ihrer Produktivität leisten sie damit einen entscheidenden Beitrag für Wohlstand und Wachstum. Dank der heimischen Standortvorteile meistern sie erfolgreich die Herausforderungen des Wettbewerbs in einem durch Globalisierung geprägten Umfeld. Es ist die Innovationskraft der kleinen und mittelständischen Unternehmen, die wesentlich dazu beträgt, dass Bayern weltweit als Markenzeichen für höchste Qualität und Zuverlässigkeit gilt.

Im globalen Wettbewerb um innovative Produkte und Dienstleistungen kommt es in einer zunehmend vernetzen Welt immer mehr auf den Schutz und die vertrauliche Übermittlung von Unternehmensdaten an. Jedes fünfte Unternehmen in Deutschland wurde bereits Opfer von Industriespionage. Der Mittelstand ist hier besonders betroffen. Die weltweite IT-Vernetzung und die steigende Bedrohungslage im Internet erfordern deshalb auch in kleinen und mittleren Unternehmen ein klares Bewusstsein für die Abhängigkeit des Unternehmens von der Sicherheit moderner Informations- und Kommunikationstechnik. Der Schutz der betrieblichen IT-Systeme vor unberechtigten Zugriffen und Cyber-Angriffen ist eine wichtige Aufgabe des Mittelstands.

Der vorliegende Leitfaden für Informationssicherheit wurde vom IT-Beauftragten der Bayerischen Staatsregierung in Kooperation mit den bayerischen Industrie- und Handelskammern erarbeitet. Er soll kleine und mittlere Unternehmen für die Gefahren, denen betriebliche IT-Systeme heute ausgesetzt sind, sensibilisieren. Gleichzeitig zeigt dieser Leitfaden pragmatische Wege auf, wie diesen Gefahren begegnet werden kann. Die Umsetzung des Leitfadens erhöht die Sicherheit betrieblicher IT-Systeme und damit auch den Schutz der wertvollen Daten bayerischer Unternehmen. Dieser Leitfaden leistet damit einen Beitrag zur weiteren Sicherung der Standortvorteile Bayerns und zur Zukunft unseres Freistaats.

Dr. Markus Söder, MdL
Staatsminister

Franz Josef Pschierer, MdL
IT-Beauftragter der Bayerischen Staatsregierung

In Zeiten der weltweiten Vernetzung ist die Nutzung moderner Informationstechnologien in der Wirtschaft selbstverständlich geworden. Aber nicht immer hält der Ausbau des Sicherheitsstandards mit dieser Entwicklung Schritt. In einer Studie des Bundesamtes für Sicherheit in der Informations-technik (BSI) gaben über 95 Prozent der kleinen und mittleren Unternehmen an, dass ihnen das Thema IT-Sicherheit wichtig oder sehr wichtig ist. Die meisten Unternehmen legen dabei den Schwerpunkt auf die Datensicherung und die Netzwerkabsicherung. Aber allzu oft vernachlässigen sie die Vorsorge für Sicherheitsvorfälle oder das Notfallmanagement. Nur etwa 50 Prozent der Unternehmen haben hier Vorkehrungen getroffen.

Diese Strategie ist gefährlich, denn viele Unternehmen wähnen sich in Sicherheit und werden dann von Angriffen überrascht. Besonders tückisch ist, dass man unter Umständen gar nicht merkt, dass man ausspioniert wurde. Daraus entsteht oft erheblicher finanzieller Schaden und mit dem Verlust von Geschäftsgeheimnissen steht auch die Wettbewerbsfähigkeit des Unternehmens auf dem Spiel.

Komplett ausschließen kann man IT-Sicherheitsprobleme nie. Aber mit überschaubarem und angemessenem Aufwand kann man das Risiko deutlich verringern. Gerade für kleinere und mittlere Unternehmen mit beschränkten Ressourcen ist es deshalb wichtig, eine passende und angemessene IT-Sicherheitsstrategie zu finden.

Genau hier setzt dieser Leitfaden an: Er gibt praktische Ratschläge zur Verbesserung der IT-Sicherheit in Unternehmen. In Zusammenarbeit mit dem Bayerischen Staatsministerium der Finanzen helfen Ihnen die bayerischen IHKs gerne, diese Herausforderung zu meistern.

Peter Driessen
Bayerischer Industrie- und Handelskammertag e.V.
Hauptgeschäftsführer

Inhalt

1. Einleitung

Die Innovationskraft und Leistungsfähigkeit der kleinen und mittleren Unternehmen (KMU) ist nach wie vor das Rückgrat der bayerischen Wirtschaft. In einem von Globalisierung und weltweiter IT-Vernetzung geprägten Umfeld hängt die Wettbewerbsfähigkeit der KMU zunehmend von einem sicheren und zuverlässigen Betrieb ihrer Unternehmens-IT ab. Der Schutz sensibler Daten spielt dabei vor dem Hintergrund der sich verschärfenden Bedrohungslage durch Internetkriminalität und Wirtschaftsspionage sowie dem Trend zu gezielten Cyber-Attacken mit hocheffizienten „IT-Präzisionswaffen“ eine besondere Rolle.

Länderübergreifend haben das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) deshalb eine „Allianz für Cyber-Sicherheit“ initiiert, die mit weiteren Partnern auf strategischer Ebene die Informationssicherheit in Deutschland weiter verbessern soll.

Um Informationssicherheit in KMU operativ zu unterstützen, zeigt der vorliegende Leitfaden zur Informationssicherheit in KMU auf, wie, wo und mit welchen Mitteln mehr Informationssicherheit in KMU wirtschaftlich und pragmatisch erreicht werden kann.

KMU sollen für die Gefahren unsicherer Informationssysteme sensibilisiert werden. In einem sog. „Best Practice Ansatz“ sollen ihnen Wege beschrieben werden, wie sie mit vertretbarem Aufwand ein Mindestmaß an Informationssicherheit in ihren Unternehmen umsetzen können.

Grundlage für die Erstellung des Leitfadens war der IT-Grundschutz des BSI. Der IT-Grundschutz ist sehr umfangreich und erscheint manchen KMU auf den ersten Blick nur schwer umsetzbar. Er ist jedoch gut strukturiert und beschreibt detailliert eine Vielzahl an sinnvollen Sicherheitsmaßnahmen. Daher orientiert sich der Leitfaden am IT-Grundschutz und gibt praxisnahe und kompakte Anregungen über Verfahren zur Aufrechterhaltung eines angemessenen Sicherheitsniveaus und stellt beispielhafte Maßnahmen für die Umsetzung heraus, die typisch für KMU sind und ein meist hinreichendes Maß an messbarer Informationssicherheit erzeugen sollen.

2. Beispiele für Schäden

Kleine und mittlere Unternehmen zeichnen sich in der Regel durch ein stark fokussiertes Geschäftsfeld mit sehr hohen Spezialkenntnissen und -fähigkeiten aus, die durch aufwändige Entwicklungsarbeit erworben wurden. Die Entwicklungsergebnisse stellen als Alleinstellungsmerkmal das Kapital des Unternehmens dar und sind vor dem Zugriff der Konkurrenz zu schützen. Gelangen Firmengeheimnisse in falsche Hände, kann das die Existenz des Unternehmens gefährden.

Ein anderes Merkmal vieler KMU ist das Fehlen von Redundanzen. Ausfälle oder Verluste in verschiedensten Bereichen (Personal, Anlagen, IT-Systeme, Daten) können kaum kompensiert werden und ebenfalls schwerwiegende Folgen haben.

Die folgenden Szenarien beschäftigen sich exemplarisch mit diesen beiden Problemfeldern. Sie zeigen, welche Folgen Versäumnisse bei der Informationssicherheit haben können, wenn bestimmte Ereignisse eintreten bzw. Angriffe durchgeführt werden. Es wird dabei deutlich, dass es oft nicht nur „die eine“ Ursache gibt, sondern Angriffe mehrschichtig sind und Sicherheitsvorkehrungen auf mehreren Ebenen notwendig sind bzw. eben versagen können.

2.1 Schadensszenario 1: Diebstahl von Firmengeheimnissen

Eine mittelständische Firma X hat drei Jahre intensiv zu neuen Technologien zur Stromspeicherung geforscht und sich dabei hoch verschuldet. Die Forschung hat zur Entwicklungsreife einer effizienten Technologie geführt, welche nun in Produkte verbaut wird, die in dieser Qualität einzigartig sind und über Jahre hinweg eine marktbeherrschende Stellung haben sollten. Die Entwicklungsdokumente machen mehrere Gigabyte aus und befinden sich verschlüsselt gespeichert auf mehreren Servern im Unternehmensnetzwerk. Das Unternehmensnetzwerk ist durch eine mehrstufige Firewall abgeschottet.

Während Vertragsverhandlungen mit potenziellen Großkunden springen diese ab und erwerben die Produkte eines Konkurrenten, welche dieser zu einem Viertel des Preises anbietet. Bei genauerer Betrachtung von dessen Produkten stellt sich heraus, dass diese zwar nicht ganz den eigenen Qualitätsansprüchen genügen, aber bereits auf der aufwändig entwickelten, vermeintlich geheim gehaltenen Technologie beruhen.

Die Firmengeheimnisse müssen in fremde Hände gefallen sein. Wie könnte sich das Ganze abgespielt haben?

Der Administrator von X bewegt sich gerne in sozialen Netzwerken und gibt dort auch seine berufliche Stellung preis. Ihm wird von einem Angreifer gezielt eine mit einem Trojaner verseuchte Software (z.B. als neues Spiel) für sein Privat-Notebook untergeschoben. Dadurch, dass der Administrator sein Notebook auch geschäftlich nutzt, kann sich der Trojaner in das Firmennetz übertragen und dort weiter verbreiten. Er ist – als maßgefertigte Auftragsarbeit – so programmiert, dass er die geheimen Schlüssel zur Verschlüsselung der Entwicklungsdaten auslesen kann. Die eigene Firewall von X hat eine hocheffiziente und komplexe Architektur, welche durch das Personal von X nicht administriert werden kann. Daher wird eine Fremdfirma mit der Wartung beauftragt; aus Kostengründen wird ein (vermeintlich) sehr preiswerter Dienstleister gewählt, nähere Informationen über ihn werden nicht eingeholt. Der Dienstleister – exakt dafür von einem Dritten instruiert und bezahlt – manipuliert die Filterregeln und Proxyeinstellungen für eine bestimmte Zeit so, dass ein Angreifer von außen Zugriff auf die (verschlüsselten) Entwicklungsdaten und auf die vom Trojaner abgegriffenen Schlüssel bekommt. Der Angreifer kopiert die Daten und gelangt somit an die Ergebnisse der jahrelangen Entwicklungsarbeit.

Was war falsch gelaufen? Das Unternehmen hat doch hinsichtlich Informationssicherheit viel investiert und vieles richtig gemacht. Verschlüsselung wurde eingesetzt und eine Firewall betrieben, auch ein stets aktuell gehaltener Virenscanner war im Einsatz.

Dennoch wurden einige – im IT-Grundschutz des BSI empfohlene – Sicherheitsaspekte nicht beachtet bzw. Maßnahmen nicht umgesetzt. Dies in Kombination mit einem motivierten und potenten Angreifer konnte zur Katastrophe führen. Die einzelnen Defizite waren:

- Der Administrator war entweder nicht sensibilisiert über Gefahren in sozialen Netzwerken oder (wahrscheinlicher) ihm wurde nicht rigoros untersagt, Details über seine Stellung preis zu geben und private Systeme dienstlich zu nutzen.
- Es war keine wirksame Kontrolle zur Anbindung mobiler Geräte oder Verwendung externer Datenträger vorhanden.

- Bei der Auswahl des externen Dienstleisters gab es massive Versäumnisse. Hier wären Informationsbeschaffung vorab, Sicherheitsüberprüfung und Zertifikate sinnvoll gewesen.
- Bei der Firewall-Administration wurde kein 4-Augen-Prinzip umgesetzt. (Dieses ist eine sehr harte Forderung, aber im Hochsicherheitsbereich durchaus angemessen.)

Dem Virenschutz kann übrigens kein Vorwurf gemacht werden. Bei dem Trojaner handelte es sich um eine individuell erstellte Software, für die noch keine Erkennungsmuster (sog. Signaturen) vorhanden sein konnten.

2.2 Schadensszenario 2: Datenverlust

Ein großes Ingenieurbüro mit 75 Mitarbeitern bearbeitet zeitgleich 15 mehrjährige Planungsprojekte, bei denen Daten oftmals vor Ort im Außendienst aufgenommen und bearbeitet werden. Zum Schutz der Vertraulichkeit wird ein Großteil der Daten nicht auf den IT-Systemen in den Projektbüros vor Ort gespeichert, sondern auf einem Fileserver in der Zentrale. Der Zugriff darauf erfolgt authentisiert über eine verschlüsselte Verbindung. Der Fileserver in der Zentrale steht in einem zutrittsgesicherten Serverraum mit Brandmeldeanlage und automatischer Löschanlage. Er verfügt über ein sog. RAID-System zur redundanten Datenspeicherung. Zusätzlich läuft jede Nacht eine Bandsicherung. Die Bänder werden vom Administrator jeden Morgen in einem feuerfesten Safe im Nachbargebäude eingelagert. Zur Notfallvorsorge ist im Nachbargebäude ein Technikraum mit Ersatz-Servern und Ersatz-Netzwerkkomponenten (Cold-Standby) eingerichtet.

In einem Lagerraum neben dem Serverraum entzünden sich dort gelagerte Chemikalien, die Trennwand zum Serverraum (Holzständerbauweise) fängt ebenfalls Feuer. Das Feuer weitet sich auf den Serverraum aus, die Brandmeldeanlage löst einen Alarm aus und die automatische Löschanlage springt an, kann aber den Brand nicht stoppen, da die Löschmittelfreisetzung defekt ist. Bevor die alarmierte Feuerwehr den Brand löschen kann, sind die Verkabelung und die IT-Systeme bereits stark geschädigt. Der Fileserver und das angeschlossene RAID-System sowie das Bandlaufwerk sind zerstört. Das Unternehmen beginnt sofort die Cold-Standby IT-Systeme und Infrastruktur in Betrieb zu nehmen. Die

Installation funktioniert planmäßig. Beim Versuch, die Projektdaten von den Sicherungsbändern wieder einzuspielen, wird festgestellt, dass diese unbrauchbar sind. Projektdaten in großem Umfang sind unwiederbringlich verloren, das Ingenieurbüro kann Aufträge nicht bearbeiten und wird zudem auf Schadensersatz verklagt. Es stellt den Geschäftsbetrieb ein und wird liquidiert.

Wie konnte es zu dieser Katastrophe kommen? Das Unternehmen hat doch hinsichtlich Informationssicherheit viel investiert und vieles richtig gemacht. Redundante Systeme, Datensicherung, Brandmelde- und Löschanlage und etliches mehr waren vorhanden.

Dennoch wurden einige – im IT-Grundschutz des BSI empfohlene – Sicherheitsaspekte nicht beachtet bzw. Maßnahmen nicht umgesetzt. Dies in Kombination mit unglücklichen Umständen konnte zur Katastrophe führen. Die einzelnen Defizite waren:

- Schützenswerte Gebäudeteile waren falsch angeordnet.
- Wände erfüllten nicht die notwendigen Brandschutzanforderungen.
- Die automatische Löschanlage wurde nicht gewartet.
- Datensicherungen wurden nicht auf Wiederherstellbarkeit überprüft.

3. Häufige Ursachen für Schäden

Häufige Ursachen für Störungen oder Ausfälle von IT-Systemen und Netzwerken sind technische Defekte, menschliches Versagen oder mutwillige Beschädigungen und Zerstörungen, die sich durch die Vernetzung der Informationsinfrastrukturen untereinander unmittelbar auch auf andere Bereiche auswirken.

IT-Systeme und Netzwerke sind, egal ob es sich um die privater Anwender oder ein ganzes Firmennetz handelt, gezielten Hackerangriffen und Bedrohungen durch Computerviren und -würmer ausgesetzt. Viele der schädlichen Programme und gezielten Angriffe gehen zunehmend auf das Konto organisierter Kriminalität und der Wirtschaftsspionage. Das Hauptmotiv ist nicht mehr, wie bei den so genannten Script-Kiddies, der Wunsch nach Anerkennung im Kreise Gleichgesinnter, sondern es geht darum, mit Angriffen finanziellen Nutzen zu erzielen.

Der vor allem wirtschaftlich begründete Trend, Produkte und Informationssysteme in industriellen Bereichen mit dem Internet (dem sog. Cyberraum) zu verbinden, führt zu neuen Verwundbarkeiten gerade bei KMU. Die Erfahrungen mit Schadprogrammen wie Stuxnet, Duqu oder Flame zeigen, dass auch wichtige industrielle Infrastrukturbereiche von gezielten IT-Angriffen nicht mehr ausgenommen bleiben und dieser Trend setzt sich fort.

Dabei können viele Verwundbarkeiten mit einfachen Mitteln beseitigt und so für die Informationssicherheit besonders schwerwiegende Fehler vermieden werden. Die häufigsten Versäumnisse im Bereich der Informationssicherheit sind im Folgenden beschrieben. Überprüfen Sie, welche davon in Ihrem Unternehmen eine besondere Rolle spielen.

3.1 Unzureichende Strategie für Informationssicherheit

Stellenwert des Schutzes von Informationen und Daten

Für die strategischen Aufgaben ist der Vorstand bzw. der Geschäftsführer zuständig. Die rechtliche Verpflichtung ergibt sich hierfür insbesondere aus dem Gesellschaftsrecht bzw. dem KonTraG, dem „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“. Das vorhandene Aktiengesetz sowie das GmbH-Gesetz wurden entsprechend ergänzt[1] bzw. werden entsprechend angewendet[2]. Nach § 91 II AktG hat der Vorstand einer AG geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit eine Entwicklung, die den Fortbestand der Gesellschaft gefährdet, früh erkannt werden kann.

1 §91 II AktG, §116 AktG
2 §43 GmbHG

Informationssicherheit hat im Vergleich mit anderen Faktoren im Unternehmen (Kosten, Marktpreise, Wettbewerbsfähigkeit, etc.) häufig einen zu geringen Stellenwert. Dabei wird Informationssicherheit als Kostentreiber oder Behinderung in den betrieblichen Abläufen gesehen. Dem Aufwand zur Entwicklung und Produktion stehen eher selten angemessene und wirksame Maßnahmen zum Schutz von Vertraulichkeit, Integrität und Authentizität zur Seite. Selbst Verfügbarkeitsanforderungen wird nicht immer umfänglich nachgekommen. Häufige Gründe dafür sind mangelnde Managementunterstützung für Informationssicherheit, ungenügendes Wissen über Sicherheitsaspekte oder knappe Ressourcen. Informationssicherheit erlangt bei der Umsetzung von wichtigen unternehmerischen Maßnahmen nur selten eine hohe Priorität.

Sicherheitsvorfälle zu erkennen und zu bewerten ist eine anspruchsvolle Führungsaufgabe und ein Versagen führt schnell zu einem signifikanten Risiko für das Funktionieren der Unternehmensprozesse, die immer mehr von einer sicheren IT abhängig sind.

Fehlender Prozess zur Beibehaltung des Sicherheitsniveaus

Beim Einkauf von Technik oder bei zu realisierenden Projekten wird Informationssicherheit in unterschiedlichem Maße als wesentlicher Bestandteil gesehen. So werden etwa bei der Einführung neuer Systeme i.d.R. Empfehlungen für die sichere Installation und Inbetriebnahme genannt. Sicherheit ist jedoch kein statischer Zustand, sondern ist einer ständigen Dynamik unterlegen und muss demzufolge im Blick behalten werden. Was heißt das? Häufig wird versäumt, dass ein sicherer Zustand auf Dauer nur erreicht werden kann, wenn Schwachstellen und Verwundbarkeiten zeitnah beseitigt werden und man sich ändernde Bedrohungslagen erkennt und darauf reagiert. Im Produktivbetrieb ändern sich erfahrungsgemäß auch manche Parametereinstellungen. Daher wäre eine Überprüfung auf die Konformität mit den Sicherheitsvorgaben durchzuführen. Allerdings unterbleibt dies oft, da es keine klare Zuweisung von Aufgaben an die Mitarbeiter gibt oder den Mitarbeitern nicht die Zeit für diese Arbeiten zugestanden wird.

Ohne einen verlässlichen Prozess kann ein angemessenes Sicherheitsniveau nicht dauerhaft erreicht und erhalten werden. Selbst wenn aufwändige Schwachstellenanalysen (sog. Penetrationstests) durchgeführt werden und Maßnahmen empfohlen werden, erfolgt deren Umsetzung manchmal erst mit Verzögerung.

Unzureichende Dokumentation von Sicherheitsvorgaben
In vielen KMU fehlt eine aktuelle, vollständige und leicht nutzbare Sicherheitsdokumentation. Beispielsweise kann die Sicherheitsleitlinie fehlen oder nicht offiziell verabschiedet sein oder Richtlinien sind nur „Schrankware“ und nicht so verständlich und eindeutig formuliert, dass kein Interpretationsspielraum bleibt.

Falls Richtlinien vorhanden sind, sind diese häufig nicht allen Mitarbeitern oder externen Angestellten (bspw. Wartungspersonal) bekannt. Oftmals fehlen vertragliche Vereinbarungen mit Mitarbeitern oder externen Unternehmen, wie eine anerkannte Richtlinie eingehalten werden muss. Dies kann in Einzelfällen dazu führen, dass Verstöße im Bereich der Sicherheit nicht oder nur schwer zu ahnden sind.

Fehlende Kontrollmechanismen und fehlende Aufklärung im Fall von Verstößen
Üblicherweise existieren für die Unternehmensziele und -parameter Kontrollmechanismen, beispielsweise zur Auftragslage oder zur Liquidität. Ein Überwachungssystem soll frühzeitig Alarm schlagen, wenn die Existenz eines Unternehmens gefährdet ist. Hinsichtlich der Sicherheitsziele wird diese Kontrolle in der Praxis jedoch häufig nicht vorgenommen – aus technischen, administrativen oder gar rechtlichen Gründen. Ebenso problematisch ist es, wenn Mitarbeiter im Falle von Sicherheitsverstößen nicht mit Konsequenzen rechnen müssen. Beide Sachverhalte erhöhen das Risiko für Schadensfälle (Know-how-Verlust, Image-Schäden, Lieferausfälle etc.).

3.2 Lückenhafte Konfiguration/Administration von IT-Systemen

Rollen und Berechtigungen sind kaum restriktiv genug
Eine der wesentlichen Regeln der Informationssicherheit ist das so genannte Need-to-Know-Prinzip: Jeder Benutzer und auch jeder Administrator von IT-Systemen (PC, mobile Endgeräte usw.) sollte nur auf die Daten zugreifen und Programme ausführen dürfen, die er für seine Aufgabenerfüllung tatsächlich benötigt. Um dies zu erreichen, ist in der Praxis meist zusätzlicher administrativer und technischer Aufwand nötig. Im Falle von KMU ist es noch komplizierter, da aufgrund der geringen Mitarbeiteranzahl im IT-Bereich oft mehrere Rollen auf

eine Person zusammenfallen. Eine zu starke Einschränkung von Rechten kann hier sogar kontraproduktiv sein, z.B. im Vertretungsfall. Dieser Zwiespalt soll andererseits kein „Freifahrtschein“ sein, um Mitarbeitern und Administratoren allzu großzügig Zugriff zu gewähren. Aufgrund zunehmender interner und externer Vernetzung kann ohne geeignete Zugriffsbeschränkungen oftmals auf die Daten anderer Benutzer bzw. Rechner – im schlimmsten Fall von außerhalb des Unternehmens – zugegriffen werden. Die Dateneigentümer sind sich dessen häufig nicht bewusst. Die weitreichenden Berechtigungen können so versehentlich, durch Unkenntnis oder beabsichtigt missbraucht werden.

Unsichere Konfiguration von IT-Systemen
Bequemlichkeit oder Unkenntnis von Nutzern und Administratoren lässt sich für Attacken ausnutzen. Mitarbeiter umgehen manchmal ganz bewusst Sicherheitsfunktionen, um schneller arbeiten zu können. Durch Fehler bei der Konfiguration und Administration entsteht in der Praxis eine Vielzahl an Sicherheitslücken. Würden die vorhandenen Sicherheitsfunktionen von Betriebssystemen und Anwendungen sinnvoll und wirksam genutzt werden, könnte das Sicherheitsniveau bei KMU deutlich erhöht werden. Allerdings steigt die Komplexität von Systemen und Software stetig und Informationssicherheit ist für Administratoren leider meist eine von vielen Arbeitsaufgaben.

3.3 Unsichere Vernetzung und Internet-Anbindung

Nicht ausreichende Abschottung sensitiver IT-Systeme
Eine optimale Konfiguration mit dem Internet verbundener Komponenten (WWW-Server, Firewall, Router usw.) würde voraussetzen, dass Schwachstellen und mögliche Angriffe bekannt sind. Die sichere Anbindung von Systemen und Applikationen an das Internet erfordert daher von den Administratoren spezifische Kenntnisse und Erfahrungen, die aufgrund der Personal- und Kostensituation in KMU nicht immer vorhanden sind. Dabei könnten so konzeptionelle und Konfigurationsfehler bei der Anbindung an den Cyberraum / das Internet vermieden werden. Sensitive Informationen, Daten und IT-Systeme werden oftmals gar nicht oder nur unzureichend von offenen Netzen abgeschottet. Eine Firewall ist wichtig, jedoch ist der Sicherheitszustand der Unternehmens-IT auch vom Einstellen und Einhalten von Regeln für Schutzsysteme abhängig. Auch beim Outsourcing der IT an externe Dienstleister (Cloud Computing, externe Rechen-

zentren/Hosting Provider usw.) sind diese Mindestanforderungen oft weder vertraglich hinreichend bzw. technisch angemessen und wirksam eingerichtet.

3.4 Nichtbeachtung von Sicherheitserfordernissen

Vernachlässigung von Sicherheitsmaßnahmen
Sicherheitsmechanismen und Vorgaben sind unwirksam, falls sie nicht genutzt bzw. nicht beachtet werden. Beispielsweise werden vertrauliche Dokumente oder E-Mails oft nicht verschlüsselt, auch wenn geeignete Mechanismen unmittelbar („mit Bordmitteln“) zur Verfügung stehen, Passwortregeln werden nicht beachtet, Bildschirmschoner nicht genutzt, Büros nicht abgeschlossen, etc. Die Liste möglicher (und leider üblicher) Versäumnisse aus Bequemlichkeit ist lang und macht auch nicht vor Administratoren halt. Beispielsweise werden Arbeiten mit privilegierten Rechten durchgeführt, für die auch Standardrechte gereicht hätten oder Datensicherungen werden nicht ausreichend dokumentiert.

Anwender und Administratoren sind nicht ausreichend geschult
Die Komplexität von IT-Systemen, Netzen und Anwendungen steigt rasant. Ebenso die von Schwachstellen und möglichen Angriffen. Abertausenden Autoren von Schadsoftware und Exploits stehen eine Handvoll IT-Mitarbeiter eines KMU gegenüber. Es ist offensichtlich, das letztere nicht umfassend auf diesen Gebieten geschult werden können. Sie sollten mit dem Handwerkszeug ausgestattet werden, das ihnen hilft, übliche Sicherheitsmaßnahmen zu pflegen. Schulungen und Sensibilisierungen decken allerdings nicht immer die spezifischen Bedürfnisse der Mitarbeiter ab. Zudem sind Qualifikationen in der Regel teuer und müssen stets aktualisiert werden.

Ein zweites Gefährdungsgebiet stellt „Social Engineering“ dar. Das Personal eines Unternehmens ist immer wieder Angriffsziel für „soziale Attacken“ beispielsweise bei Wirtschaftsspionage. Dabei werden menschliche Schwächen für Angriffe auf die Systeme ausgenutzt. Oftmals ist das Personal von KMU unzureichend auf solche Angriffe vorbereitet.

3.5 Unzureichende Wartung von IT-Systemen

Verfügbare Sicherheits-Updates werden nicht eingespielt
Pflege- und Wartungsarbeiten sind für den sicheren Betrieb von IT-Systemen und Netzen ebenso zwingend erforderlich wie für den Maschinen- und Fuhrpark. Administratoren installieren allerdings die dafür erforderlichen Sicherheits-Updates (sog. Patches) oftmals nicht rechtzeitig. Zum einen beansprucht das Einspielen Zeit, zum anderen kann in speziellen Umgebungen möglicherweise nicht von vornherein klar sein, ob der Patch „gut vertragen" wird, d.h. nicht zu Betriebsproblemen führt. Nach der „reinen Lehre" sollte ein Patch vorher in einer Testumgebung getestet werden, was noch mehr Zeit kosten würde, welche den Administratoren in KMU oftmals nicht zur Verfügung steht, ebenso wenig wie eine Testumgebung.

Offen bleibende Sicherheitslücken können zu erheblichen Ausfällen durch Viren oder Trojaner führen.

3.6 Sorgloser Umgang mit Passwörtern und Sicherheitsmechanismen

Sorgloser Umgang mit Passwörtern
Das Aufbewahren von Passwörtern unter der Tastatur oder in der obersten Schreibtischschublade macht es Innen- oder Außentätern leicht, an sensitive Informationen zu gelangen.

Zu kurze oder leicht zu erratende Passwörter machen es Angreifern leicht, ein Passwort zu knacken, sei es durch systematisches Ausprobieren, Raten oder Ausspähen.

Viele Mitarbeiter sind sich nicht bewusst, welche Informationen sie weitergeben dürfen oder wie wichtig es ist, ihre Informationen und Zugänge zu schützen. So geben Mitarbeiter ihre Passwörter oftmals an Kollegen weiter, was beispielsweise zu einem großen Problem werden kann, wenn diese das Unternehmen wechseln.

Angreifer wenden auch zunehmend psychologische Tricks und „das gefühlte Vertrauen" über soziale Netzwerke an, um an das Wissen von Unternehmen oder Zugang zu sensiblen Informationen zu gelangen. Das erbeutete Wissen lässt sich in der Regel leicht für Angriffe auf technischer Ebene nutzen.

Sicherheitsmechanismen, die ungenutzt bleiben
Viele Produkte und Systeme werden mit eingebauten Sicherheitsmechanismen ausgeliefert. Aus Bequemlichkeit, Unwissen oder Zeitmangel werden diese nicht aktiviert oder zu schwach eingestellt.

3.7 Mangelhafter Schutz vor Einbrechern und Elementarschäden

Gebäude und Räume werden ungenügend gegen unbefugten Zutritt, und IT-Systeme ungenügend gegen Diebstahl geschützt
Vandalen, Einbrecher und Diebe haben oft allzu leichtes Spiel. Fehlender Perimeterschutz, falsche Standortwahl, unverschlossene (oder mit leicht brechbaren Schlössern versehene) Gebäude, gekippte Fenster über Nacht, unverschlossene IT-Räume, unbeaufsichtigte Besucher oder im Auto zurückgelassene Notebooks bieten ungebetenen Gästen vielfältige Möglichkeiten. Schwerer als der Verlust von Hardware durch Diebstahl oder Vandalismus wiegt im Allgemeinen der Verlust von Daten. Diese sind nur unter Mühen wiederzubeschaffen (falls sie nicht auch zentral gehalten werden). Besonders schwerwiegend ist die Gefahr, dass ein Dieb vertrauliche Daten missbrauchen könnte.

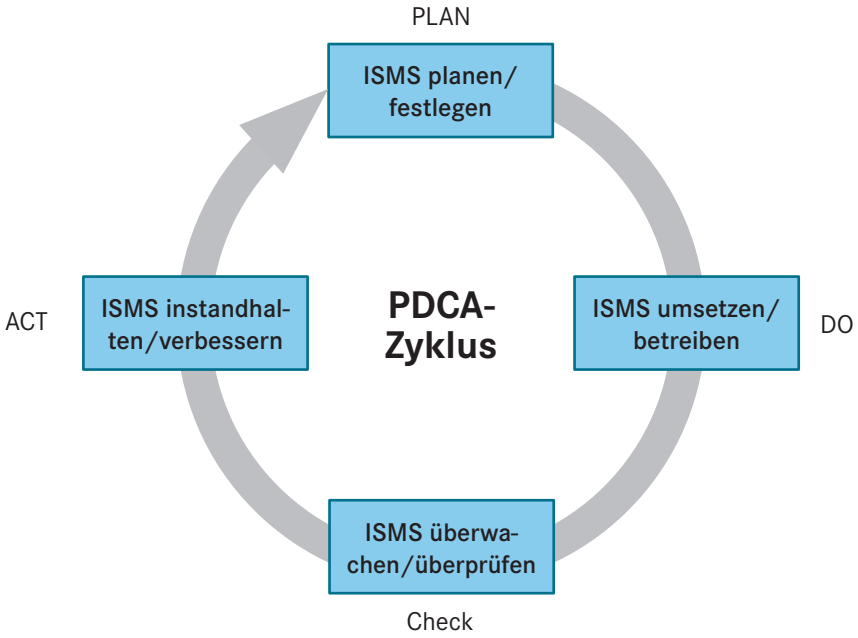
Gebäude und Räume werden nur ungenügend gegen Unfälle und Elementarschäden geschützt
Katastrophen wie Brände oder Überschwemmungen sind zwar recht seltene Ereignisse, aber wenn sie eintreten, sind die Folgen meistens fatal. Daher sollten auch Brandschutzmaßnahmen, Schutz vor Wasserschäden und die Sicherstellung der Stromversorgung als wichtiger Bestandteil der Informationssicherheit verstanden werden. Aber auch wenn dem so ist, kann es im Schadensfall ein böses Erwachen geben, falls nicht gleichzeitig organisatorische und personelle Maßnahmen umgesetzt sind. Typische Beispiele sind der Generator ohne Diesel oder die Ersatzklimaanlage, die nicht bedient werden kann.

4. Maßnahmen

Der Schutz der Daten und der eingesetzten Informationstechnik ist für gewöhnlich nur durch die Etablierung von Regeln und Mechanismen in verschiedenen Bereichen möglich. Wie aus den oben genannten Schadensszenarien ersichtlich, können ganz unterschiedliche Ursachen für einen Vorfall bzw. Schaden verantwortlich sein und meist ist es die Kombination von Schwachstellen und Versäumnissen. Im Folgenden werden für typische Bereiche der Informationssicherheit wirkungsvolle Maßnahmen aufgeführt. Diese sind so gewählt, dass sie ein günstiges Kosten-/Nutzenverhältnis aufweisen. Nichtsdestotrotz kann es sein, dass für kleinere Unternehmen die Kosten für die Umsetzung zu hoch sind. Für diesen Fall ist zu jedem Sicherheitsbereich noch angegeben, welche Maßnahmen mit „wenig Geld“ umgesetzt werden können. Die alleinige Umsetzung dieser Maßnahmen wird noch keine ausreichende Informationssicherheit herstellen, sie kann aber als Einstieg dienen.

4.1 Informationssicherheitsmanagement, Personal, Organisation

Materielle und technische Sicherheitsmaßnahmen sind zur Absicherung von Gebäuden, Räumen, IT-Systemen, Netzen und Anwendungen unverzichtbar. Alleine reichen sie aber nicht aus. Unter Umständen verfehlen sie sogar ihren Zweck, beispielsweise die Firewall, bei der die Filterregeln nicht gepflegt werden, oder ein Zutrittskontrollsystem ohne restriktive Verwaltung der Schlüssel. Technische Sicherheitsmaßnahmen sollten daher Teil eines umfassenden Informationssicherheitsmanagementsystems (ISMS) sein, welches mit dem Plan-Do-Check-Act (PDCA)-Zyklus einen geeigneten Regelkreis abbildet und ebenso personelle wie organisatorische Sicherheitsmaßnahmen enthält.



Checkliste:

- Gibt es eine Leitlinie zur Informationssicherheit und ist sie von der Leitung unterschrieben?
- Gibt es einen Beauftragten für Informationssicherheit (ggf. in Personalunion)? Ist er für die Aufgabe geeignet und verfügt er über die notwendigen Ressourcen (finanziell und zeitlich)?
- Gibt es ein Sicherheitskonzept bzw. wurde mit der Erstellung begonnen? Welchen Bearbeitungsstand hat es?

Typische Sicherheitsmaßnahmen sind:

- Die Leitungsebene muss die Gesamtverantwortung für Informationssicherheit in der Institution übernehmen. Sichtbares Zeichen ist eine übergeordnete Leitlinie zur Informationssicherheit, die den Stellenwert der Informationssicherheit, die Sicherheitsziele und die wichtigsten Aspekte der Sicherheitsstrategie beschreibt.
- Die Leitungsebene muss einen mit angemessenen Ressourcen ausgestatteten Beauftragten benennen, der die Informationssicherheit fördert und den Sicherheitsprozess steuert und koordiniert.

- Alle Sicherheitsmaßnahmen sollten systematisch in einem Sicherheitskonzept dokumentiert und regelmäßig aktualisiert werden. Dabei sollte auf anerkannte Standards zurückgegriffen werden, z.B. IT-Grundschutz des BSI.
- Der Sicherheitsprozess, das Sicherheitskonzept, die Leitlinie zur Informationssicherheit und die Organisationsstruktur für Informationssicherheit sollten regelmäßig auf Wirksamkeit und Angemessenheit überprüft (z.B. durch eine IS-Revision) und aktualisiert werden.

Was geht für wenig Geld?

- Übertragen Sie die Rolle des Sicherheitsbeauftragten an einen technisch versierten Mitarbeiter und gleichen Sie eventuelle Defizite im administrativen/organisatorischen Bereich durch entsprechende Schulungen aus. Dies ist meist günstiger, als einen Mitarbeiter ohne technischen Hintergrund für die Rolle zu befähigen.
- Nutzen Sie die Angebote des BSI, z.B. Webkurse IT-Grundschutz und GSTOOL.

4.2 Infrastruktursicherheit

Die bauliche Infrastruktur, welche den physischen Rahmen zum Betrieb der IT-Systeme und Netze bildet, muss, als eine Art „erste Verteidigungslinie“, angemessen geschützt werden. Besonders wichtig sind der Schutz vor Umwelteinflüssen und Unfällen sowie die Zutrittssicherung.

Einzelanforderungen und Einzelmaßnahmen sind hier stark von der Art und Größe des Unternehmens abhängig. Es stellen sich Fragen, wie z.B.: Herrscht intensiver Publikumsverkehr? Teilt man sich eine Lokation mit anderen Firmen? Sind gefährliche Güter im Spiel? Etc.

Checkliste:

- Ist für alle Areale, Gebäude(teile) und Räume spezifiziert, wem Zutritt gewährt werden soll?
- Wird die Zutrittsregelung durch entsprechende bauliche Absicherung und Zutrittskontrollen umgesetzt?
- Existieren für den Schutzbedarf und die Gefahrenlage angemessene Überwachungssysteme (z.B. Brandmelder, Wassermelder, Einbruchsmelder, etc.)?
- Wurden alle baulichen Arbeiten gemäß den geltenden Vorschriften und Normen ausgeführt und wurde dies in Abnahmen bestätigt?
- Existieren Einrichtungen zum Brandschutz? Werden diese gewartet und wird die Einhaltung von Brandschutzvorschriften geprüft?
- Ist bekannt, ob gefährdende Einrichtungen oder Umweltbedingungen im Umfeld vorhanden/möglich sind (z.B. Brandlasten oder Hochwasser)? Ist ggf. für mögliche Schadensfälle Vorsorge getroffen?
- Werden wichtige Versorgungseinrichtungen (z.B. Klimatisierung) regelmäßig gewartet? Stehen Ersatzgeräte zur Verfügung?

Typische Sicherheitsmaßnahmen sind:

- Schützenswerte Räume oder Gebäudeteile sollten nicht in besonders gefährdeten Bereichen angesiedelt sein.
- Die Strom- und Datenverkabelung, einschließlich Blitz- und Überspannungsschutzkonzept, sollten den einschlägigen Vorschriften und Normen entsprechen, nach Errichtung/Änderung abgenommen, dokumentiert und regelmäßig überprüft werden.
- Es ist ein IT-bezogenes Brandschutzkonzept zu erstellen und umzusetzen. Es sollte ein Brandschutzbeauftragter benannt und zu allen den Brandschutz tangierenden Aktivitäten hinzugezogen werden. Brandschutzbegehungen sollten ein- bis zweimal im Jahr stattfinden.
- Für alle schutzbedürftigen Areale, Gebäudeteile und Räume ist eine Zutrittsregelung und -kontrolle festzulegen und technisch und organisatorisch umzusetzen.

- Für alle schutzbedürftigen Areale, Gebäudeteile und Räume sollte der Grad der Gefährdung durch Naturkatastrophen, Unfälle etc. bekannt sein und es sollten angepasste Sicherungseinrichtungen vorhanden sein.
- Alle Versorgungssysteme und -leitungen sollten regelmäßig gewartet und kontrolliert werden und es sollten aktuelle Lagepläne vorhanden sein.
- Unterstützende Infrastrukturkomponenten (z.B. Stromversorgung, Klimaanlage) sollten bedarfsgerecht geplant und regelmäßig gewartet und kontrolliert werden.

Was geht für wenig Geld?

- Beschränken Sie die Zahl der zu sicherheitskritischen Bereichen zutrittsberechtigten Personen auf das notwendige Mindestmaß.
- Weisen Sie die Mitarbeiter an, schutzbedürftige Räume zu verschließen und nicht die Zutrittskontrollen zu umgehen (z.B. Türkeile).
- Schließen Sie in unbenutzten Räumen die Fenster und nach außen gehende Türen (Balkone, Terrassen).
- Nutzen sie innenliegende Räume als Serverraum (dabei Beachtung der Klimatisierung).

4.3 Schutz vor Schadsoftware und Software-Schwachstellen

Durch Schadsoftware kann in erster Linie die Integrität und Verfügbarkeit von Daten und Programmen sowohl im Verwaltungsbereich als auch zunehmend bei Industrieanlagen beeinträchtigt werden. Auch die Vertraulichkeit gespeicherter und verarbeiteter Informationen kann gefährdet sein, beispielsweise durch Trojaner, welche Authentisierungsinformationen mitlesen und weitergeben. Waren in der Vergangenheit ungerichtete Computerviren und Würmer, welche ihr mehr oder weniger desaströses Zerstörungswerk meist zufällig absolvierten, die Regel, so ist in letzter Zeit eine Zunahme von Angriffen mit ganz konkreten Zielen – oft auch als Auftragsarbeit – zu verzeichnen. Gefährdet sind beispielsweise geheime Firmendaten oder die Verfügbarkeit von essentiellen Anwendungen und Diensten.

Die wesentliche Schutzmöglichkeit besteht im Einsatz von sog. Scannern, welche Schadsoftware in der Regel mit Hilfe von Erkennungsmustern (sog. Signaturen) aufspüren. Sicher erkannt werden können über ihre Signaturen allerdings nur bereits bekannte Viren und andere Schadprogramme. Zum Auffinden unbekannter, neuer Schadsoftware bedarf es weitergehender Verfahren, wie Heuristiken oder der Erkennung von Anomalien. Diese Verfahren sind aufwändig und bringen auch nur eine teilweise Sicherheit. Umso wichtiger ist es, dass flankierende organisatorische Maßnahmen etabliert werden.

Schwachstellen vor allem in Anwendungen – aber auch Betriebssysteme und Middleware sind betroffen – ermöglichen Angreifern das Eindringen in Systeme und die illegitime Aneignung von Rechten. Die probate Verteidigungsstrategie besteht in einem wirkungsvollen Patchmanagement, also dem unverzüglichen Einspielen von Programmkorrekturen zur Behebung der Schwachstellen.

Checkliste:

- Sind alle Systeme mit einem Programm zum Schutz vor Schadsoftware ausgestattet?
- Werden regelmäßig in kurzen Abständen Aktualisierungen des Virenschutzes vorgenommen?
- Gibt es Richtlinien und Regelungen zum Schutz vor Schadsoftware und beim Eintreten eines Vorfalls?
- Werden alle zutreffenden Sicherheitsupdates für die gesamte Software zeitnah eingespielt?

Typische Sicherheitsmaßnahmen sind:

- Es sollten zum Thema Schadsoftware ein zentraler Ansprechpartner ernannt und Regelungen und Richtlinien zum Vermeiden von Infektionen sowie zum Verhalten bei erfolgten Infektionen erstellt werden.
- Auf allen IT-Systemen sollten wirkungsvolle Schutzprogramme im Einsatz sein.
- Es sollte eine regelmäßige Aktualisierung der Viren-Schutzprogramme durch zeitnahes Einspielen von neuen Schadprogramm-Signaturen und Patches erfolgen.

- Auf allen IT-Systemen sollten für die Betriebssysteme, Middleware und Anwendungen (insbesondere Web-Browser) zeitnah sicherheitsrelevante Updates und Patches eingespielt werden.
- Die Mitarbeiter sollten darüber informiert sein, wie sie eine Infektion mit Schadsoftware verhindern können, woran sie sie erkennen und wie sie sich in einem solchen Fall zu verhalten haben.
- Infizierte IT-Systeme müssen isoliert werden und dürfen bis zur vollständigen Bereinigung nicht mehr produktiv genutzt werden. Schadprogramme sollten durch geschulte und berechtigte Personen entfernt werden.

Was geht für wenig Geld?

- Setzen Sie kostengünstige Basisschutz-Lösungen zur Abwehr von Schadsoftware ein. Diese sind bei verschiedenen Anbietern erhältlich.
- Nutzen Sie die Mittel des eingesetzten Betriebssystems.
- Weisen Sie Ihre Mitarbeiter mit einem Merkblatt (auch elektronisch) auf den sicheren Umgang mit unbekannten Daten / Daten von unbekannten Absendern hin.
- Verfolgen und berücksichtigen Sie die Informationen der Softwarehersteller und des BSI.

4.4 Sichere Nutzung mobiler IT-Systeme

Durch die immer stärker zunehmende Verwendung von mobilen Endgeräten (Notebooks, Smartphones, Tablet PCs) und die Synchronisation von Datenbeständen (z.B. E-Mail, Kalender) werden Unternehmensinformationen extern gespeichert und über das Internet übertragen. Auch im handwerklichen Gewerbe existieren viele Anwendungsgebiete für den Einsatz mobiler Technologien. Es sind dabei nicht nur die mobil genutzten Daten und Anwendungen, beispielsweise Angebote oder Abnahme von Leistungen, gefährdet. Durch logische und physische Schnittstellen können Schwachstellen entstehen, über die Angriffe gegen das interne Firmennetz wirksam werden können.

Checkliste:

- Sind alle genutzten mobilen Systeme inventarisiert?
- Gibt es Regelungen mit Vorgaben zur Nutzung mobiler Systeme?
- Werden die Sicherheitsmechanismen der Betriebssysteme im Firmennetz und der mobilen Systeme genutzt?

Typische Sicherheitsmaßnahmen sind:

- Es sollte eine eigene Sicherheitsrichtlinie zur Nutzung und Anbindung der mobilen Systeme existieren und die mobilen Systeme sind im Sicherheitskonzept zu behandeln.
- Festplatten von Notebooks sollten verschlüsselt werden.
- Zur Synchronisation von Unternehmensinformationen und zur zentralen Verwaltung der Systeme sollten sichere Lösungen eingesetzt werden, wie sie von verschiedenen Mobile Device Management-Herstellern angeboten werden.
- Zur Authentisierung könnten stärkere Verfahren als Benutzername/Passwort eingesetzt werden, z.B. Einmalpasswort-Verfahren, Biometrie oder Smart-Cards.
- Die Kommunikation sollte kryptografisch gesichert werden – abhängig vom Schutzbedarf durch Verschlüsselung und/oder elektronische Signatur.
- Die Benutzer sollten eingeschränkte Rechte haben, insbesondere was die Installation von zusätzlicher Software („Apps“) betrifft, und diese auch nicht ausweiten können.

Was geht für wenig Geld?

- Verarbeiten und speichern Sie Daten mit erhöhtem Schutzbedarf nicht auf mobilen Systemen.
- Setzen Sie mobile Systeme nur da ein, wo dies auch wirklich betriebliche Vorteile bringt.
- Sensibilisieren Sie die Mitarbeiter mit einem Merkblatt bezüglich möglicher Gefahren.
- Nutzen Sie die Möglichkeiten ihres Betriebssystems im stationären Netz und die der mobilen Systeme und/oder setzen Sie frei erhältliche bzw. günstige Basis-Versionen von Mobile Device Management Software ein.
- Speichern Sie Daten nicht nur auf einem mobilen Gerät, sondern auch auf einem stationären System, dies gilt verstärkt für Daten mit hohen Verfügbarkeitsanforderungen.
- Ist der Einsatz einer qualifizierten elektronischen Signatur organisatorisch und wirtschaftlich nicht vertretbar, sollten Sie zumindest eine einfache elektronische Signatur verwenden.

4.5 Datensicherung und Notfallvorsorge

Ein Notfall ist ein Schadensereignis, bei dem wesentliche Abläufe eines Unternehmens über das Ausmaß einer Störung hinaus nicht wie vorgesehen funktionieren. Um Notfällen vorzubeugen, sind der Aufbau und Betrieb eines Notfallmanagement-Prozesses notwendig. Ein geplantes und organisiertes Vorgehen garantiert eine optimale Notfallvorsorge und Notfallbewältigung. Dies verringert die Wahrscheinlichkeit des Auftretens eines Notfalls und mindert die negativen Folgen und sichert somit das Überleben des Unternehmens. Es sind daher zum einen geeignete Vorbeugemaßnahmen zu treffen, welche die Robustheit und Ausfallsicherheit erhöhen, und zum anderen Maßnahmen zur Wiederherstellung bei Eintritt eines Notfalls vorzusehen. Ziel ist es, Ausfallzeiten so zu minimieren, dass die Existenz des Unternehmens nicht gefährdet wird.

Checkliste:

- Sind Ansprechpartner und Meldewege festgelegt und allen Mitarbeitern bekannt?
- Existiert ein Notfallplan mit Anweisungen für die Verfahrensweise bei den wichtigsten Schadensfällen?
- Existieren für die Verfahren/IT-Systeme mit hohen Verfügbarkeitsanforderungen Ausweichlösungen?
- Werden Datenbestände regelmäßig planvoll gesichert?
- Werden die Datensicherungen geschützt aufbewahrt?
- Werden Übungen zur Datenrekonstruktion und zum Wiederanlauf (ggf. in anderer Infrastrukturumgebung) durchgeführt?

Typische Sicherheitsmaßnahmen sind:

- Notfallpläne sollten erstellt werden und jedem Mitarbeiter bekannt sein.
- Der Bestand an Hard- und Software sollte in einer Inventarliste erfasst und hinsichtlich seiner Verfügbarkeitsanforderungen bewertet werden.
- Für IT-Systeme und unterstützende Infrastruktur mit hohen Verfügbarkeitsanforderungen sollten Ersatzsysteme bzw. Ersatzteile vorhanden sein.
- Alle wichtigen Daten sollten regelmäßig gesichert werden (Backup).
- Die Datensicherungen sollten getrennt von den Daten an einem feuerfesten und gegenüber Elementarschäden gesicherten Aufbewahrungsort gelagert werden.
- IT-Systeme und unterstützende Infrastruktur sollten angemessen gegen unautorisierten Zutritt, Feuer, Überhitzung, Staub, Wasserschäden und Stromausfall geschützt sein.
- Das Personal sollte mit Sofortmaßnahmen für den Notfall vertraut sein.

Was geht für wenig Geld?

- Treffen Sie mit einem anderen Unternehmen eine (gegenseitige) Vereinbarung zur Hilfe im Notfall, beispielsweise der Mitnutzung von Räumen oder Überlassung von Geräten.
- Lagern Sie Datensicherungen in einem anderen Brandabschnitt als dem Aufstellungsort der IT-Systeme.

4.6 Sichere Konfiguration und Wartung der IT-Systeme

Fehler bei der Bereitstellung und Nutzung von IT-Systemen sind oftmals die Ursache für Ausfälle oder stellen den Eintrittspunkt für Angriffe dar. Würden die in Betriebssystemen und Anwendungssoftware vorhandenen Sicherheitsfunktionalitäten vollständig und richtig ausgenutzt, so wäre das Sicherheitsniveau in Unternehmen höher.

Neben wichtigen Themen, welche die Sicherheit von IT-Systemen betreffen und die in diesem Leitfaden querschnittlich behandelt werden (Virenschutz, Notfallvorsorge, etc.), ist auch die Installation, Konfiguration, Administration und Wartung der IT-Systeme sicher zu gestalten. Ein wichtiges Prinzip ist dabei „so viel wie nötig und so wenig wie möglich“. Dies trifft auf die Benutzerrechte (Need-to-Know-Prinzip) ebenso zu wie auf die installierten Programme und aktivierten Dienste und Konten. Speziell bei kleinen und mittleren Unternehmen kann dies zu Interessenskonflikten führen, da hier möglicherweise eine geringere Spezialisierung bei der IT-Nutzung vorliegt und viele Aufgaben in Personalunion durchgeführt werden. Es muss dann zwischen den Interessen abgewogen werden.

Checkliste:

- Sind nicht benötigte Programme und Dienste deinstalliert bzw. deaktiviert?
- Werden vorhandene Schutzmechanismen in Anwendungen und Programmen genutzt?
- Sind allen Systembenutzern Rollen und Profile zugeordnet oder gibt es sog. Sammelaccounts, d.h. ein Benutzerkonto für mehrere Personen?
- Ist geregelt, welche Funktionen jeder Mitarbeiter nutzen darf und auf welche Datenbestände er zugreifen darf? Sind die Rechte entsprechend eingeschränkt?

- Ist bekannt und geregelt, welche Privilegien und Rechte Programme haben?
- Werden sicherheitsrelevante Standardeinstellungen von Programmen und IT-Systemen geeignet angepasst oder wird der Auslieferungszustand beibehalten?
- Werden Wartungsaufgaben durch qualifiziertes Personal durchgeführt?

Typische Sicherheitsmaßnahmen sind:

- Vor der Installation sollte festgelegt werden, welche Komponenten des Betriebssystems und welche Anwendungsprogramme und Tools installiert werden sollen. Für die Installation sollten nur Medien und Dateien benutzt werden, die aus einer sicheren Quelle stammen.
- Es sollte mindestens eine Administrator- und eine Benutzer-Umgebung eingerichtet werden. Die Administratorrolle sollte nur für Arbeiten genutzt werden, zu denen die Rechte tatsächlich nötig sind.
- Nach der Installation sollte überprüft werden, welche Programme und Netzdienste auf dem System installiert und aktiviert sind. Nicht benötigte Programme und Netzdienste sollten deaktiviert oder ganz deinstalliert werden.
- Es sollte überprüft werden, ob die Berechtigungen für Systemverzeichnisse und -dateien den Vorgaben der Sicherheitsrichtlinie entsprechen.
- Es sollte geprüft werden, welche Benutzerkonten wirklich gebraucht werden. Nicht benötigte Benutzerkonten sollten entweder gelöscht oder zumindest deaktiviert werden.
- Server und Clients mit hohem Schutzbedarf sollten zusätzlich zum Schutz durch die unternehmensweiten Firewall(s) mit einem lokalen Paketfilter abgesichert werden.
- Zugriffsrechte auf Dateien, die auf Servern gespeichert sind, sollten restriktiv vergeben werden. Jeder Benutzer darf nur auf die Dateien Zugriffsrechte erhalten, die er für seine Aufgabenerfüllung benötigt.
- Sicherheitsrelevante Ereignisse sollten protokolliert werden. Die Protokolle sollten regelmäßig ausgewertet werden.

Was geht für wenig Geld?

- Installieren und konfigurieren Sie gleichartige Systeme einheitlich.
- Deaktivieren oder deinstallieren Sie nicht benötigte Programme und Dienste.
- Deaktivieren oder löschen Sie nicht benötigte Benutzerkonten.
- Verwenden Sie einheitliche Benutzerprofile mit eingeschränkten Rechten.
- Erlauben Sie keine anonymen oder von mehreren Personen gemeinsam genutzten Konten.
- Richten Sie eine Bildschirmsperre mit Passwort ein, die sich manuell vom Benutzer aktivieren lässt und nach z.B. 15 Minuten Inaktivität automatisch erscheint.
- Orientieren Sie sich zur sicheren Konfiguration an den Leitlinien der Betriebssystemhersteller und des BSI.

4.7 Sichere Architektur und Konfiguration des Unternehmensnetzes und der Schnittstellen

Netzwerksicherheit hat für KMU zwei wesentliche Aspekte. Zum einen benötigt das KMU ein lokales Netz, das für die betrieblichen Abläufe optimiert ist und eine hohe Verfügbarkeit aufweist. Von der Verkabelung, über die einzelnen Protokollschichten bis zu verteilten Daten und Anwendungen sind Sicherheitsvorgaben und Funktionalität/Durchsatz in Einklang zu bringen. Zum anderen ist dieses Netz mit anderen Netzen, üblicherweise auch dem Internet, gekoppelt. Die Herausforderung besteht darin, die Vorteile der Vernetzung unter gleichzeitiger Beibehaltung eines hohen Sicherheitsniveaus zu gewährleisten.

Checkliste:

- Ist jedweder Zugang von außen in das Unternehmensnetzwerk nur über eine Firewall möglich?
- Werden die Firewalls professionell überwacht und administriert?
- Sind auf den Servern und aktiven Netzwerkgeräten nur die nötigen Programme installiert und Dienste aktiviert?

Typische Sicherheitsmaßnahmen sind:

- Bei der Planung der Netztopologie und Netztechnologie sollten neben den betrieblichen Anforderungen auch Sicherheitsanforderungen (resultierend aus dem Schutzbedarf der Netzdienste und übertragenen Daten) berücksichtigt werden.
- Das gesamte Netz des Unternehmens muss durch ein entsprechendes Sicherheitsgateway geschützt sein. Server, die Dienste nach außen hin anbieten, sollten in einer Demilitarisierten Zone (DMZ) aufgestellt werden.
- Server sollten möglichst nicht im selben IP-Subnetz wie die Clients platziert werden. Wenn Server zumindest durch einen Router von den Clients getrennt sind, bestehen wesentlich bessere Sicherheitseigenschaften.
- Sicherheitsrelevante Ereignisse im Netz sollten protokolliert werden. Die Protokolle sollten regelmäßig ausgewertet werden.
- Bei der Bildung von Teilnetzen sollte darauf geachtet werden, dass alle IT-Systeme und Kommunikationsverbindungen in einem Teilnetz in Bezug auf den Grundwert Vertraulichkeit den gleichen Schutzbedarf haben. Teilnetze mit unterschiedlichem Schutzbedarf sollten durch ein Sicherheitsgateway getrennt werden.
- Die Sicherheit des Unternehmensnetzwerkes sollte ständig überwacht und wenn nötig verbessert werden. Firewallsoftware und -einstellungen sollten durch geschultes Personal administriert und auf dem neuesten Stand sein.

Was geht für wenig Geld?

- Installieren und konfigurieren Sie gleichartige aktive Netzkomponenten einheitlich.
- Wenden Sie zum Zugang zu Routern und Switches strenge Passwortregeln an.
- Deaktivieren oder deinstallieren Sie nicht benötigte Netzdienste.
- Orientieren Sie sich zur sicheren Konfiguration an den Leitlinien von Geräteherstellern und des BSI.

4.8 Schulung und Sensibilisierung

Die besten Sicherheitsprodukte und -funktionen helfen nichts, wenn sie nicht richtig konfiguriert und bedient werden können. Die besten Regelungen helfen nichts, wenn sie nicht richtig verstanden oder nicht beachtet werden.

IT-Systeme, Netze und Anwendungen werden immer komplexer und sowohl für das IT-Personal als auch die Benutzer ist Weiterbildung, auch hinsichtlich Informationssicherheit, unumgänglich. Da diese mit nicht unerheblichen Kosten (Trainingskosten und Arbeitszeit) verbunden ist, sollte sie insbesondere bei kleinen und mittleren Unternehmen sehr zielgerichtet und effizient erfolgen.

Checkliste:

- Verfügen alle Mitarbeiter über die für ihre Aufgabe notwendige Expertise, einschließlich Kenntnissen zur Aufrechterhaltung der Informationssicherheit?
- Ist allen Mitarbeitern bewusst, welchen Stellenwert Informationssicherheit für das Unternehmen und für ihren Arbeitsbereich hat?
- Wie und wann wird der Ausbildungsstand zur Informationssicherheit erfasst?
- Gibt es ein maßgeschneidertes Schulungsprogramm?
- Gab es schon Sicherheitsvorfälle, die auf mangelnden Kenntnisstand oder mangelnde Einsicht zurückzuführen waren?

Typische Sicherheitsmaßnahmen sind:

- Es sollte ein Schulungs- und Sensibilisierungskonzept erstellt werden, mit Festlegungen zu Zielgruppen, Schulungsformen, Schulungsanbietern und Schulungsinhalten sowie zum Schulungsprozess, beginnend beim Erkennen von Schulungsbedarf bis hin zur Überprüfung des Schulungserfolges.
- Basierend auf dem Konzept sollen mit einer Vorschau von drei bis neun Monaten konkrete Schulungen für die entsprechenden Mitarbeiter geplant und durchgeführt werden.
- Die Wirksamkeit des Schulungs- und Sensibilisierungskonzeptes ist regelmäßig, beispielsweise jährlich, zu prüfen. Im Falle der Nachbereitung

von Sicherheitsvorfällen sollte auch immer die Frage gestellt werden, ob mangelnder Kenntnisstand oder mangelnde Einsicht dazu beigetragen haben.

Was geht für wenig Geld?

- Leben Sie (als Unternehmer/Führungskraft) praktische Informationssicherheit vor.
- Machen Sie eine Einweisung in die Informationssicherheit zum Bestandteil des Prozederes bei Neueinstellungen.
- Führen Sie Informationssicherheit bei Betriebsversammlungen als festen Tagesordnungspunkt ein.
- Belohnen Sie sicherheitsorientiertes Verhalten.

4.9 Passwörter und andere Authentisierungsmittel

Authentisierung (Nachweisen der eigenen Identität) ist ein elementarer Sicherheitsmechanismus. Ein Benutzer kann dies auf drei verschiedenen Wegen erreichen:

- Nachweis der Kenntnis einer Information (z.B. Passwort)
- Verwendung eines Besitztums (z.B. Chipkarte)
- Gegenwart eines Merkmals des Benutzers selbst (Biometrie)

Obwohl, vor allem im Hochsicherheitsbereich, geraten wird, Mechanismen aus zwei Bereichen kombiniert zu verwenden, trifft man vielfach auf Authentisierungsmechanismen, die sich nur auf die Verwendung von Passwörtern abstützen. Für KMU ist dies oft auch eine Kostenfrage.

Bei geeigneten technischen, organisatorischen und personellen Maßnahmen lässt sich auch mit der Verwendung von Passwörtern ein vernünftiges Sicherheitsniveau herstellen.

Checkliste:

- Gibt es eine Passwortrichtlinie?
- Werden Festlegungen der Passwortrichtlinie technisch erzwungen?

Typische Sicherheitsmaßnahmen sind:

- Hersteller- und sonstige Default-Passwörter müssen geändert werden.
- Es muss vernünftige Mindestanforderungen an die Komplexität geben (z.B. mindestens 8 Zeichen lang, Sonderzeichen, Groß-/Kleinbuchstaben, Zahlen).
- Passwortregeln, wie z.B. Verschwiegenheit, nicht notieren, keine Trivialpasswörter, Wechsel nach n Tagen, etc. sollten verbindlich festgelegt und den Mitarbeitern kommuniziert werden.
- Wenn es das Betriebssystem/die Anwendung erlaubt, sind Passwortregeln technisch durchzusetzen.
- Bei erhöhten Sicherheitsanforderungen ist Zwei-Faktor-Authentisierung vorzusehen.

Was geht für wenig Geld?

- Erläutern Sie Ihren Mitarbeitern, wie man zu komplexen und dennoch leicht merkbaren Passwörtern kommt, indem man ein Passwortschema anwendet. Beispielsweise beginnend mit einem leicht merkbaren Satz „Viele Köche verderben den Brei.“ Von jedem Wort den ersten und letzten Buchstaben „VeKevndnBi.“ Ersetzen („i“ durch „1“ oder „!“, „e“ durch „€“, „s“ durch „?“ oder „$“, etc.) „V€K€vndnB!.“ Wichtig ist, dass sich jeder Mitarbeiter sein persönliches Passwortschema einprägt und dies nicht weitergibt.

4.10 Sichere E-Mail- und Internet-Nutzung

Mit vertraulichen Inhalten sollte keine ungesicherte Kommunikation im Internet stattfinden, ebenso wenig bei erhöhtem Schutzbedarf für Datenintegrität und Authentizität (Echtheit) des Kommunikationspartners. E-Mails als einer der meistgenutzten Kommunikationsdienste bieten per se keinen Schutz, oft wird ein Vergleich mit Postkarten herangezogen und tatsächlich ist es für Betrüger und Spione sehr einfach, E-Mails im Internet mitzulesen oder zu fälschen.

Es gibt aber weit verbreitete und kostengünstige Lösungen zur Absicherung von E-Mailverkehr. Durch Verschlüsselung kann die Vertraulichkeit und durch eine elektronische Signatur die Integrität und Authentizität geschützt werden.

Bei der Internetnutzung zur Informationsbeschaffung, Kommunikation und Geschäftsabwicklung sollte ebenfalls immer bedacht werden, dass man es mit einem unsicheren Übertragungsmedium zu tun hat und auf Funktionen und Daten zugreift, deren Integrität nicht von vornherein feststeht. Ebenso wenig kann davon ausgegangen werden, dass der Kommunikationspartner auch immer der ist, wer er vorgibt, zu sein. Die Absicherung der Internetnutzung ist deshalb eine große Herausforderung im Zwiespalt von erwünschter Funktionalität und Informationssicherheit, die aber durch technische und organisatorische Maßnahmen gemeistert werden kann.

Checkliste:

- Existieren eine Sicherheitspolitik mit grundsätzlichen Zielen und Vorgaben und eine Sicherheitsrichtlinie mit genauen Anleitungen für die Nutzer zu diesem Thema?
- Steht E-Mail-Verschlüsselung und -Signatur zur Verfügung und wissen die Mitarbeiter, wie man sie nutzt?
- Ist die (potenzielle) private Nutzung von E-Mail und Internet im Unternehmen klar geregelt?
- Sind die eingesetzten Browser und E-Mail-Clients auf dem neuestem Softwarestand?
- Sind die Browser und E-Mail-Clients auf eine sinnvolle Sicherheitsstufe konfiguriert? Erfolgt die Konfiguration einheitlich und kann sie von den Nutzern nicht geändert werden?

Typische Sicherheitsmaßnahmen sind:

- Es sollte verbindliche Richtlinien für E-Mail- und Internet-Nutzung geben.
- Schutzbedürftige E-Mails sollten verschlüsselt und elektronisch signiert werden. Es empfiehlt sich beispielsweise der Einsatz von PGP (Pretty Good Privacy) oder S/MIME (Secure Multipurpose Internet Mail Extension).
- Dateien, die als E-Mail-Anhang übermittelt wurden, sollten mit besonderer Vorsicht und Sorgfalt behandelt werden, insbesondere wenn sie nicht erwartet wurden.
- In den Client-Programmen für die Nutzung von Internet-Diensten wie Web-Browser und E-Mail-Programmen sollten nicht benötigte Funktionen deaktiviert sein.

- Im Web-Browser sollten nur die aktiven Inhalte bzw. Skriptsprachen und Multimedia-PlugIns zugelassen werden, die für die Arbeit wirklich unverzichtbar sind. Besonders riskante Konstrukte, wie z.B. unsignierte ActiveX-Controls, sollten in jedem Fall deaktiviert werden.

Was geht für wenig Geld?

- Falls Sie keine E-Mail-Verschlüsselung einsetzen, schützen Sie die Dateien, die Sie mit E-Mail versenden, mit Passwörtern (z.B. möglich bei PDF-Dokumenten, ZIP-Dateien oder Office-Dokumenten), und wählen Sie dafür ausreichend sichere Passwörter.
- Sensibilisieren Sie die Mitarbeiter zu Gefahren bei der E-Mail-Nutzung.

4.11 Sicherheit bei der Beteiligung Dritter / Nutzung Leistungen Dritter

Die Möglichkeiten für die Beteiligung Dritter bzw. der Nutzung von Leistungen Dritter spannen einen weiten Bogen. Von einfachen Wartungsverträgen, über die Nutzung von Diensten in der „Cloud“ bis hin zu kompletten Outsourcing-Konstellationen kommen unterschiedlichste Varianten und Abhängigkeiten vor. Aus diesen Verhältnissen können ganz unterschiedliche Gefahren für jeden Grundwert der Informationssicherheit erwachsen, beispielsweise könnte der Dritte gezielt Angriffe durchführen, alleine oder zusammen mit einem Mitarbeiter oder einem Hintermann. Er könnte aber auch unabsichtlich Fehler machen oder wiederum selbst das Opfer eines Angriffs werden. Mögliche Abwehrstrategien sind ebenso vielfältig und auf unterschiedlichen Ebenen möglich. Sie sollten sich vor allem an der Schutzbedürftigkeit der Daten und Verfahren bzw. potenziellen Schäden ausrichten.

Checkliste:

- Gibt es eine Übersicht, in welcher Form Dritte beim IT-Betrieb beteiligt sind bzw. welche externen Leistungen genutzt werden?
- Sind alle sicherheitsrelevanten Fragestellungen in entsprechenden Verträgen geregelt?
- Bestehen Ausweichmöglichkeiten?

Typische Sicherheitsmaßnahmen sind:

- Bei jeder Entscheidung, Dritte zu beteiligen bzw. externe Leistungen zu nutzen, sind auch Sicherheitskriterien miteinzubeziehen (neben wirtschaftlichen Gesichtspunkten).
- Bei der Auswahl eines geeigneten Dienstleisters sollten Qualifikationen der Mitarbeiter und Sicherheitsnachweise nachgefragt werden. Hierbei können Zertifikate hilfreich sein.
- Zu allen entsprechenden Geschäftsbeziehungen sollten vertraglich auch die Anforderungen und Rahmenbedingungen zur Informationssicherheit vereinbart werden, und das für alle Phasen des Lebenszyklusses, einschließlich der Beendigung der Beziehung.
- Zwischen beauftragender Firma und Dienstleister sollte ein Sicherheitskonzept abgestimmt werden, so dass alle sicherheitsbezogenen Rechte und Pflichten abgedeckt und eindeutig einer Seite zugewiesen sind.
- Die beauftragende Firma sollte den Dienstleister hinsichtlich der vereinbarten Leistungen und eigener Sicherheitserfordernisse kontrollieren können, beispielsweise durch nicht manipulierbare Aufzeichnungen.
- Bei hohen Verfügbarkeitsanforderungen sollte die beauftragende Firma bei Ausfall des Dienstleisters innerhalb einer das Unternehmen nicht gefährdenden Unterbrechungsdauer Ersatzlösungen aktivieren können.

Was geht für wenig Geld?

- Stecken Sie tendenziell mehr Aufwand in die vorbereitenden bzw. initialen Aktivitäten bei der Beteiligung von Dritten bzw. der Nutzung von Leistungen Dritter. Dadurch werden Konflikte und Folgekosten minimiert.

4.12 Einhaltung von Regelungen und Vorschriften – Compliance

Eine elektronische Information wird zunehmend der papiergebundenen Information rechtlich gleichgestellt. In Deutschland fand dies, ausgehend von der Änderung des BGB (Bürgerliches Gesetzbuch), in Zusammenhang mit der elektronischen Signatur seinen Niederschlag in fast allen Gesetzen und Verordnungen.

In Europa und in Deutschland gibt es zahlreiche Compliance-Anforderungen, nur wurden diese bisher so nicht bezeichnet. Hierzu gehören aus der deutschen Steuer- und Handelsgesetzgebung beispielsweise HGB, AO, GDPdU, GoBS ebenso wie in der Finanzwirtschaft das Thema Risikocontrolling nach Basel II, KonTraG usw.

Gemäß der Studie „IT-Sicherheitslage im Mittelstand 2011“ von „Deutschland sicher im Netz e.V.“ haben KMU beim Thema Compliance noch Nachholbedarf. So besitzen demnach nur 24% eine Compliance-Strategie, in der das Unternehmen Verhaltensmaßregeln und die Berücksichtigung von Gesetzen sowie Richtlinien im IT-Bereich definiert und dokumentiert. 69% der Unternehmen haben mit einzelnen Compliance-Maßnahmen begonnen, wobei aber anscheinend erst 21% den Schutzbedarf für ihre IT-Infrastruktur von ihren übergreifenden Sicherheitszielen ableiten.

Anders als bei großen Konzernen sind bei KMU nicht die Ressourcen für eine dedizierte Organisationsstruktur für Compliance vorhanden. Compliance-Aktivitäten sollten dort mit Bedacht durchgeführt werden und in das ISMS integriert sein. Entsprechende Aufgaben können durchaus dem Beauftragten für die Informationssicherheit übertragen werden, wobei sich die Leitung immer bewusst sein sollte, dass sie die letztendliche Verantwortung trägt.

In der Regel können KMU aus ihrer Rechtsform (z.B. Aktiengesellschaft, GmbH, OHG) ableiten, welche fordernden Kontrollstandards (BSI-Standards oder ISO 27000) die Compliance gegenüber einer Wirtschaftsprüfung sowie ihren Kunden herstellen.

Checkliste:

- Sind alle IT-Werte („assets“) inventarisiert und wurde ihr Schutzbedarf hergeleitet?
- Wurde das Sicherheitsmanagement nach einem anerkannten Standard aufgebaut?
- Gibt es eine aktuelle Übersicht über vertragliche und gesetzliche Anforderungen an die Informationsverarbeitung und ist diese Mitarbeitern und ggf. Partnern bekannt?
- Wird geprüft, ob die Anforderungen eingehalten werden?
- Werden bei erkannten Defiziten Korrekturmaßnahmen eingeleitet?

Typische Sicherheitsmaßnahmen sind:

- Es sollten mindestens ein geeigneter Verantwortlicher benannt werden und seine Aufgaben in Bezug auf das Compliance-Management festgelegt werden.
- Es sollte eine strukturierte Übersicht über für das KMU relevante Gesetze, Vorschriften und Verträge geben.
- Dem Unternehmen muss bekannt sein, welche Werte (Systeme, Dienste, Daten etc.) vorhanden sind und wie hoch deren Schutzbedarf ist. Unter Umständen kann es erforderlich sein, dass detaillierte Risikoanalysen durchzuführen sind.
- Rechte für Zutritt zu Gebäuden/Räumen, Zugang zu Systemen und Zugriff auf Daten sollten restriktiv vergeben und verwaltet werden.
- Es sollten geeignete Maßnahmen identifiziert und umgesetzt werden, um Verstöße gegen relevante Anforderungen zu vermeiden. Falls Verstöße doch passieren, sollte klar sein, welche Aktionen zur Korrektur bzw. Schadensbegrenzung und ggf. Sanktionierung durch wen zu ergreifen sind.
- Es sollte regelmäßig überprüft werden, ob die Sicherheitsvorgaben, die das KMU zur Erfüllungen der Anforderungen erstellt hat, eingehalten werden. Ebenso sollte regelmäßig überprüft werden, ob die internen Regelungen und die rechtlichen Rahmenbedingungen noch aktuell sind.

- Mitarbeiter, Partner, Kunden, externe Dienstleister und Besucher sollten auf ihre Sorgfaltspflichten im Umgang mit Informationen und IT-Systemen hingewiesen werden.
- Beim Outsourcing der IT sollte insbesondere gewährleistet sein, dass Kontrollmechanismen zur Prüfung
  - der Ordnungsmäßigkeit der externen Durchführung (Verträge, Technik, Wartung),
  - der Gewährleistung der Sicherheit und
  - der Einhaltung des Datenschutzes

  existieren.

Was geht für wenig Geld?

- Orientieren Sie sich an anerkannten Standards und Normen, wie z.B. den Vorgaben des BSI (ISO 27001 auf Basis IT-Grundschutz, BSI 100-4 Notfallmanagement, Technische Richtlinien, Empfehlungen zu kryptografischen Verfahren, sicherem Löschen und weiteren Sicherheitsmechanismen).
- Übertragen Sie einem Mitarbeiter die Rolle als Verantwortlicher für Compliance in der Informationsverarbeitung, beispielsweise als Ergänzung zur Rolle des Sicherheitsbeauftragten.

5. Weiterführende Informationen

Publikationen des BSI stehen auf der nachfolgenden Webseite bereit: www.bsi.bund.de/DE/Publikationen/publikationen_node.html

Zur Informationssicherheit sind u.a. die folgenden Publikationen veröffentlicht worden:

- BSI-Standards 100-1 bis 100-4
- IT-Grundschutz-Kataloge mit IT-GS-Profil für den Mittelstand
- IT-Grundschutz kompakt
- Zertifizierte IT-Produkte, Softwareangebote des BSI
- CERT-Bund und Lageberichte des BSI

Wichtige Adressen in Bayern:

www.cio.bayern.de
: IT-Beauftragter der Bayerischen Staatsregierung

www.wirtschaftsschutz.bayern.de
: Wirtschaftsschutz Bayern

www.bihk.de
: Bayerischer Industrie- und Handelskammertag

www.iabg.de/infokom/it_sicherheit/index_de.php
: IABG mbH – Dienstleistungen für KMU - Beratung und Realisierung: BSI-akkreditierte Prüfstelle für Informationssicherheitsberatung und Revisionen

www.baymevbm.de
: BayME

www.it-sicherheit-bayern.de
: IT-Sicherheitscluster Regensburg

www.bvsw.de
: BVSW

www.kosib.de
KOSIB

www.bicc-net.de
Bayerischer Cluster für Informations- und Kommunikationstechnologie

Weitere Adressen zum Thema Informationssicherheit

www.ec-net.de
Themenschwerpunkt ‚Netz- und Informationssicherheit' innerhalb des ‚Netzwerks Elektronischer Geschäftsverkehr'

www.it-sicherheit.de
Die Website gibt einen Überblick über Anbieter und Produkte in der IT-Sicherheit. Anwenderberichte zeigen, wie Sicherheit in der Praxis umgesetzt wird.

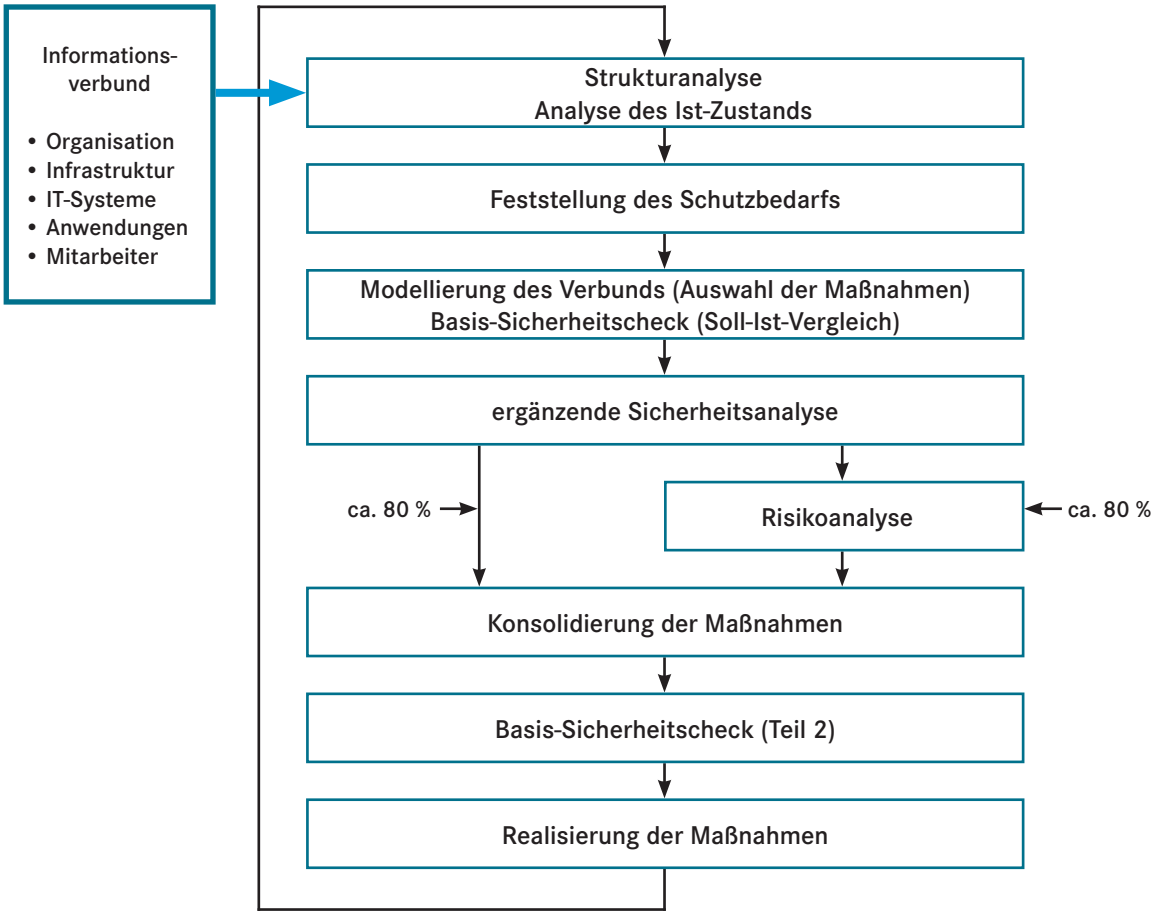
www.sicher-im-netz.de
Initiative ‚Deutschland sicher im Netz' mit dem ‚IT-Sicherheitspaket Mittelstand' für kleine und mittelständische Unternehmen

6. IT-Grundschutz

Der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist eine mit Katalogen hinterlegte Methodik zum Aufbau eines Sicherheitsmanagementsystems sowie zur Absicherung von Informationsverbünden über Standard-Sicherheitsmaßnahmen. Er besteht aus den Standards

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
- BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
- BSI-Standard 100-4: Notfallmanagement

und den sehr umfangreichen IT-Grundschutzkatalogen mit ca. 80 Bausteinen, ca. 500 Gefährdungen und über 1200 Maßnahmen. Die grundsätzliche Vorgehensweise, deren Kerngedanke ist, dass einer pauschal angenommenen Gefährdungslage mit vordefinierten Standardsicherheitsmaßnahmen begegnet wird, ist in nachfolgender Grafik dargestellt (Quelle: BSI 100-2).



Nach einer Strukturanalyse zur Aufnahme der Infrastruktur, IT-Systeme, Netze und Anwendungen (sog. „Zielobjekte“) wird für diese der Schutzbedarf hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit bestimmt. Nach der sog. „Modellierung“, der Auswahl der Bausteine mit den empfohlenen Maßnahmen, wird im Basis-Sicherheitscheck geprüft und dokumentiert, ob die Maßnahmen umgesetzt sind. Nach der Analyse und Entscheidung, ob der Grundschutz ausreicht oder ob spezielle Risikobetrachtungen durchzuführen sind (und ggf. deren Durchführung), erfolgt eine Konsolidierung offener Maßnahmen mit Festlegung von Umsetzungsreihenfolge und Verantwortlichkeiten und schließlich deren Implementierung. Zur Anwendung des Grundschutzes gibt es geeignete Werkzeuge (z.B. das GSTOOL des BSI). Bei erfolgreicher Umsetzung kann ein Zertifikat oder Auditor-Testat beantragt werden.

7. Glossar Informationssicherheit

In diesem Glossar[3] werden einige wichtige Begriffe zur Informationssicherheit erläutert.

Administrator

Ein Administrator verwaltet und betreut Rechner sowie Computernetze. Er hat im Allgemeinen weitreichende oder sogar uneingeschränkte Zugriffsrechte auf die betreuten Rechner oder Netze.

Angriff

Ein Angriff ist eine vorsätzliche Form einer Gefährdung, mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Authentisierung (englisch „authentication“)

Authentisierung bezeichnet den Nachweis eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt, zu sein. Dies kann unter anderem durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen.

Authentizität

Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner (im weitesten Sinne, z.B. auch Anwendungen) tatsächlich derjenige ist, der er vorgibt, zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden.

Bedrohung

Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann.

Biometrie

Unter Biometrie ist die automatisierte Erkennung von Personen anhand ihrer körperlichen Merkmale (z.B. Iris, Fingerabdruck, Handschrift, Gesicht) zu verstehen.

3 Quelle: BSI

Browser

Mit Browser wird Software zum Zugriff auf das World Wide Web bezeichnet. Das Programm interpretiert die ankommenden Daten und stellt sie als Text und Bild auf dem Bildschirm dar.

Datenschutz

Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Beim Datenschutz geht es um den Schutz des Einzelnen bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten und deren technischer Sicherung gegen unbefugtem Zugriff, Verlust oder Zerstörung.

Datensicherheit

Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Neuerdings ist meist von „Informationssicherheit“ die Rede, was der übergreifendere Begriff ist.

Datensicherung (englisch „Backup“)

Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt.

Demilitarisierte Zone (DMZ)

Eine DMZ ist ein Zwischennetz, das an Netzübergängen (üblicherweise zum Internet) gebildet wird. Sie stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie das eigentlich zu schützende Netz.

Elektronische Signatur

Elektronische Signaturen sind mit elektronischen Informationen verknüpfte Daten, mit denen man den Unterzeichner bzw. Signaturersteller identifizieren und die Integrität der signierten elektronischen Informationen prüfen kann.

Exploit

Programm, das Schwachstellen in anderen Programmen ausnutzt, z.B. Pufferüberlauf. Besonders gefürchtet sind Exploits, die nahezu unmittelbar nach Bekanntwerden einer Schwachstelle auftauchen („Zero-Day-Exploit“).

Firewall

Eine Firewall (synonym: Sicherheitsgateway) ist ein System aus soft- und hardware-technischen Komponenten. Es gewährleistet – richtig konfiguriert – die sichere Kopplung von Netzen durch Einschränkung der technisch möglichen auf die in einer Sicherheitsrichtlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden.

Gefährdung (englisch „applied threat“)

Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.

Grundwerte der Informationssicherheit

Der IT-Grundschutz betrachtet die drei Grundwerte der Informationssicherheit:

- Vertraulichkeit: Schutz vor unbefugter Preisgabe von Informationen
- Integrität: Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen
- Verfügbarkeit: Nutzbarkeit von Daten, Diensten, Funktionen und IT-Systemen für Berechtigte

Darauf basierend können noch weitere Grundwerte, teilweise als Verfeinerung der Integrität, betrachtet werden, wie Authentizität, Verbindlichkeit oder Nichtabstreitbarkeit.

Informationssicherheitsmanagement (IS-Management)

Die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet.

IT-Sicherheit

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vor-

handen sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind. Der modernere und weiter greifende Begriff ist **„Informationssicherheit“.**

Beauftragter für die Informationssicherheit (IT-Sicherheitsbeauftragter)

Person mit eigener Fachkompetenz zur Informationssicherheit in einer Stabsstelle eines Unternehmens oder einer Behörde, die für alle Aspekte rund um die Informationssicherheit zuständig ist.

IT-System

IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Einzelplatz-Computer, Mobiltelefone, Router, Switches und Sicherheitsgateways.

Patch

Ein Patch (aus dem englischen, auf Deutsch: Flicken) ist ein kleines Programm, das Softwarefehler, wie z.B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen, behebt.

Penetrationstest

Ein Penetrationstest ist ein gezielter, in der Regel simulierter, Angriffsversuch auf ein IT-System. Er wird als Wirksamkeitsprüfung vorhandener Sicherheitsmaßnahmen eingesetzt.

Informationssicherheits-Revision (IS-Revision)

IS-Revision ist die systematische Überprüfung der Eignung und Einhaltung vorgegebener Richtlinien und Sicherheitseigenschaften. Die IS-Revision sollte unabhängig und neutral sein. Auf den Webseiten des BSI finden sich die Kontaktdaten von zertifizierten IS-Revisoren.

Risiko

Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven

Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab.

Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.

Schadprogramm / Schadsoftware / Malware

Die Begriffe Schadprogramm / Schadsoftware / Malware werden häufig synonym benutzt. Sie bezeichnen Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computer-Viren, Würmer, Trojanische Pferde, Rootkits, Hintertüren und Keylogger. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

Schwachstelle (englisch „vulnerability“)

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

Sicherheitskonzept

Ein Sicherheitskonzept dient zur Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Sicherheitsmaßnahme sollte sich letztlich darauf zurückführen lassen. Sicherheitskonzepte können beispielsweise nach der Methode des BSI Grundschutzes erstellt werden.

Sicherheitsrichtlinie (englisch „Security Policy“)

In einer Sicherheitsrichtlinie werden Schutzziele und allgemeine Sicherheitsmaßnahmen im Sinne offizieller Vorgaben eines Unternehmens oder einer Behörde formuliert. Detaillierte Sicherheitsmaßnahmen sind in einem umfangreicheren Sicherheitskonzept enthalten.

Starke Authentisierung

Starke Authentisierung bezeichnet die Kombination von zwei Authentisierungstechniken, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte. Daher wird dies auch häufig als Zwei-Faktor-Authentisierung bezeichnet.

Verschlüsselung

Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die „Schlüssel“ genannt wird, in einen zugehörigen Geheimtext, der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation – die Zurückgewinnung des Klartextes aus dem Geheimtext – wird Entschlüsselung genannt.

VPN

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internets) betrieben wird, jedoch logisch von diesem Netz getrennt wird.

Wert (englisch „asset“)

Werte sind alles, was wichtig für eine Institution ist (Vermögen, Wissen, Gegenstände, Gesundheit).

Zertifikat

Der Begriff Zertifikat wird in der Informationssicherheit in verschiedenen Bereichen mit unterschiedlichen Bedeutungen verwendet. Zu unterscheiden sind vor allem:

ISO 27001-Zertifikate auf der Basis von IT-Grundschutz: Seit Anfang 2006 können ISO 27001-Zertifikate auf der Basis von IT-Grundschutz beim BSI beantragt werden. Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist eine Überprüfung durch einen vom BSI zertifizierten ISO 27001-Grundschutz-Auditor. Zu den Aufgaben eines ISO 27001-Grundschutz-Auditors gehören eine Sichtung der von der Institution erstellten Referenzdokumente, die Durchführung einer Vor-Ort-Prüfung und die Erstellung eines Audit-Reports. Die Zertifizierungsstelle BSI stellt aufgrund des Audit-Reports fest, ob die notwendigen Sicherheitsmaßnahmen umgesetzt sind, erteilt im positiven Falle ein Zertifikat und veröffentlicht es.

Zertifikat (Schlüsselzertifikat): Ein Schlüsselzertifikat ist eine elektronische Bescheinigung, mit der Signaturprüfschlüssel einer Person zugeordnet werden. Bei digitalen Signaturen wird ein Zertifikat als Bestätigung einer vertrauenswürdigen dritten Partei benötigt, um nachzuweisen, dass die zur Erzeugung der Digitalen Signatur eingesetzten kryptografischen Schlüssel wirklich zu dem Unterzeichnenden gehören.

Weitere Arten von Zertifikaten sind z.B. solche, die Sicherheitseigenschaften von Produkten bestätigen (Common Criteria – Zertifikat) oder Zertifikate von Schutzprofilen zur Festlegung produktklassen-typischer und dienstleistungsspezifischer Sicherheitsanforderungen.

Zugang

Mit Zugang wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet. Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen wie IT-Systeme bzw. System-Komponenten und Netze zu nutzen.

Zugriff

Mit Zugriff wird die Nutzung von Informationen bzw. Daten bezeichnet. Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen, zu nutzen oder Transaktionen auszuführen.

Zutritt

Mit Zutritt wird das Betreten von abgegrenzten Bereichen wie z.B. Räumen oder geschützten Arealen in einem Gelände bezeichnet.

8. Abkürzungsverzeichnis

AG	Aktiengesellschaft
AktG	Aktiengesetz
AO	Abgabenordnung
BGB	Bürgerliches Gesetzbuch
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVSW	Bayerischer Verband für Sicherheit in der Wirtschaft e.V.
CERT	Computer Emergency Response Team
DMZ	Demilitarisierte Zone
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GmbH	Gesellschaft mit beschränkter Haftung
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
GS	Grundschutz
HGB	Handelsgesetzbuch
ISMS	Informationssicherheitsmanagementsystem
KMU	Kleine und mittlere Unternehmen
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KOSIB	Kompetenzzentrum für Sicherheit in Bayern
OHG	offene Handelsgesellschaft
PDCA	Plan-Do-Check-Act
PDF	Portable Document Format
PGP	Pretty Good Privacy
RAID	Redundant Array of Independent Disks
S/MIME	Secure Multipurpose Internet Mail Extension
VPN	Virtuelles Privates Netz
www	World Wide Web

Impressum

Herausgeber	Der IT-Beauftrage der Bayerischen Staatsregierung Odeonsplatz 4 80539 München
E-Mail	poststelle@cio.bayern.de
Internet	www.cio.bayern.de
Titelbilder	PantherMedia/Andrew Ostrovsky
Stand	Oktober 2012 1. Auflage 2012

Weitere Informationen zur Zukunftsstrategie der Bayerischen Staatsregierung erhalten Sie unter:
www.aufbruch.bayern.de

Aufbruch Bayern

BAYERN | DIREKT ist Ihr direkter Draht zur Bayerischen Staatsregierung. Unter www.servicestelle.bayern.de oder per E-Mail unter direkt@bayern.de erhalten Sie Informationsmaterial und Broschüren, Auskunft zu aktuellen Themen und Internetquellen sowie Hinweise zu Behörden, zuständigen Stellen und Ansprechpartnern bei der Bayerischen Staatsregierung.

BAYERN | DIREKT
www.bayern.de Tel. 089 12 22 20