IT-Awareness und IT-Sicherheit

in kleinen und mittleren Unternehmen

Ein Leitfaden zum IT-Grundschutz

eine Kooperation von

Service & Consult ServiCon

AWADO

Vorwort

Die Informationstechnologie (IT) ist für kleine und mittlere Unternehmen (KMU) von erheblicher Bedeutung. Sie ermöglicht Effizienz- und Effektivitätsgewinne. Eine Vielzahl von Verfahren befindet sich im Einsatz und es ist von einer noch weiter zunehmenden Bedeutung der IT für diese Unternehmen auszugehen. Je mehr Funktionen und Prozesse mit Hilfe von IT-Systemen automatisiert erledigt werden, umso abhängiger werden die Unternehmen von der fehlerfreien und verlässlichen Funktion der IT-Systeme und – Verfahren und desto unabdingbarer wird es, sich auch mit dem zunehmenden Bedrohungspotentialen sowie den Risiken aus dem IT-Einsatz auseinanderzusetzen.

Unternehmensdaten z.B. Kunden-, Lieferanten- oder auch Produktionsdaten zählen zu den schutzbedürftigen Unternehmenswerten. Daher können Cyberangriffe, Datendiebstahl, finanzielle Schäden und Reputationsverluste gerade für kleine und mittelständische Unternehmen schnell existenzbedrohend werden.

Obwohl eine Vielzahl gesetzlicher Regelungen und Anforderungen existieren – z.B. die Datenschutzgrundverordnung (DSGVO), welche alle Unternehmen einzuhalten haben und es verschiedene Rahmenwerke gibt, welche Empfehlungen und Hinweise zur Ausgestaltung einzelner Aspekte zur IT-Sicherheit vorgeben, wie z. B. die Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hat das Thema IT-Sicherheit aufgrund seiner Komplexität und Schnelllebigkeit im Tagesgeschäft eines KMU hingegen nur wenig Platz.

Zur Schaffung eines geeigneten organisatorischen Rahmens muss neben wirksamen technischen Maßnahmen auch ein Bewusstsein für regelmäßige Schulungen bei den verantwortlichen Personen entstehen. Da diese Bedingung aus Budget- und Zeitgründen sowie Personalmangel in den meisten Fällen nicht erfüllt werden können, sind Störungen in den IT-Systemen z.B. Systemausfälle oder Cyberattacken im Umfeld von KMU oft erfolgreich und die negativen Auswirkungen teilweise um ein Vielfaches größer als bei Großunternehmen.

Effektiver Schutz beginnt damit, dass bei den Unternehmensleitungen das Verständnis erzeugt wird, dass diese für die IT-Sicherheit ihres Unternehmens verantwortlich sind, man aber aus den genannten Gründen den Herausforderungen an die IT-Sicherheit nicht gewachsen ist.

Dieser Leitfaden gibt Auskunft über die Grundanforderungen an die IT-Basissicherheit des BSI auf Grundlage der IT-Grundschutz-Methodik des BSI und soll in kompakter Form eine Hilfestellung dabei sein, ein solides Sicherheitskonzept auch ohne großes IT-Budget in KMU zu implementieren.

Eine interessante Lektüre wünscht Ihnen,

Ihre ServiCon Service & Consult eG in Kooperation mit der AWADO GmbH

Inhaltsverzeichnis

1 Schadensfälle als warnendes Beispiel

1.1 Kein Backup

Ein Großhändler betreibt ein kleines Netz mit einem zentralen Server, auf dem alle Daten gespeichert werden. Der Server enthält ein Bandlaufwerk, auf das in regelmäßigen Abständen eine Sicherungskopie gespeichert wird. Der Administrator bewahrt die Sicherungsbänder in einem verschlossenen Schrank in seinem Büro auf. Als eines Tages der Server durch einen Festplattendefekt ausfällt, sollen die Daten vom Sicherungsband wieder eingespielt werden. Dabei stellt sich jedoch heraus, dass das Bandlaufwerk offenbar bereits längere Zeit defekt war und gar keine Daten auf die Sicherungsbänder geschrieben hatte. Das einzige noch funktionstüchtige Sicherungsband ist mehr als fünf Jahre alt. Alle Daten der letzten Jahre sind damit verloren.

Der Administrator hat bei der Planung der Datensicherung eine weitere potentielle Gefahr übersehen: Selbst, wenn das Bandlaufwerk funktioniert hätte, wären bei einem Feuer oder ähnlichen Katastrophen neben den Originaldaten auch die Sicherungsmedien in seinem Schrank mit vernichtet worden.

Maßnahmen:

- regelmäßige Überprüfung der Backup-Bänder
- Rücksicherungen durchführen/testen
- Lagerung von Sicherungsbändern außerhalb der eigenen Büroräume/Serverräume

1.2 Befall durch Computer Viren

Eine Verbundgruppe setzt flächendeckend Viren-Schutzprogramme ein. Eine Aktualisierung der Viren-Signaturen findet jedoch nur sporadisch statt, beispielsweise im Rahmen von Betriebssystem-Updates. Eines Tages erhält die IT-Abteilung eine Virenwarnung bezüglich eines neuen E-Mail-Virus, der sich in Windeseile über das Internet an immer mehr Empfänger verbreitet. Die Verbundgruppe verfügt jedoch über keine automatisierten Update-Mechanismen, mit deren Hilfe im Eilverfahren die Viren-Schutzprogramme auf allen Rechnern mit den neuen Viren-Signaturen aktualisiert werden könnten. Im Rahmen einer Notfallmaßnahme werden die Mailserver vom Internet getrennt. Der Virus hat sich aber bereits in das interne Netz eingeschlichen und kann nicht an der weiteren Ausbreitung gehindert werden. Da der Virus Office-Dokumente löscht, müssen alle Rechner vom Netz genommen und heruntergefahren werden, bis die Fachverantwortlichen nach und nach alle PCs mit aktuellen Viren-Signaturen versehen und bereits befallene Rechner mühevoll „gesäubert“ haben. Der gesamte IT-Betrieb ist für mehrere Tage nahezu stillgelegt. Durch zerstörte Daten,

Verspätungen bei der Auftragsabwicklung und verlorene Arbeitszeit entsteht ein beträchtlicher Schaden. Kurz nach Abschluss dieser Arbeiten tauchen erste Varianten des Virus im Internet auf, die vom zuvor mühevoll aktualisierten Viren-Schutzprogramm noch nicht erkannt werden. Die gesamte Arbeit muss nochmals wiederholt werden.

Maßnahmen:

- Update-Konzept für Sicherheits-Updates erstellen
- „IT-Inseln“ innerhalb des Unternehmens nicht vergessen (z.B. Notebooks, Testrechner, Heimarbeitsplätze)

1.3 Ausfall eines Administrators

Ein mittelständisches Unternehmen hat einen Administrator, der bereits seit Jahren allein für die Installation und Konfiguration aller PCs sowie den Betrieb des Netzes zuständig ist. Eines Tages fällt der Administrator durch einen schweren Unfall aus und ist nicht mehr arbeitsfähig.

Bereits nach wenigen Tagen häufen sich die Probleme mit den Servern im Netz: Fehlermeldungen und Warnhinweise erscheinen, die von den Mitarbeitern nicht korrekt interpretiert und bearbeitet werden können. Kurze Zeit später stehen mehrere Rechner still, und nach versuchtem Neustart geht fast gar nichts mehr. Die nun beginnende Suche in den Unterlagen des Administrators ergibt, dass die bestehende Systemlandschaft praktisch nicht dokumentiert ist. Selbst Administrations-Passwörter wurden nicht hinterlegt. Eine eiligst zur Unterstützung herbeigerufene Firma für IT-Support sieht sich aufgrund fehlender Passwörter und Unterlagen nicht in der Lage, das bestehende System wieder zum Laufen zu bringen. Mühevoll wird recherchiert, welche Anwendungen auf den Servern installiert waren und wo diese die für das Unternehmen wichtigen Daten gespeichert hatten. Weitere externe Spezialisten müssen hinzugezogen werden. Denn außer weit verbreiteten Standardanwendungen werden auch branchenspezifische Individuallösungen genutzt, die das mit der Wiederherstellung beauftragte Systemhaus zuvor noch nie gesehen hatte.

Bis alles wiederhergestellt ist und alle für die tägliche Arbeit benötigten Systeme wieder in der gewohnten Weise funktionieren, vergehen mehrere Wochen. In der Zwischenzeit können im Unternehmen wichtige Aufträge nicht erfüllt werden, da die hierfür erforderlichen Informationen und Anwendungen nicht verfügbar sind. Die hierdurch entstehenden Schäden summieren sich zusammen mit den Kosten für die externen Dienstleister auf einen sechsstelligen Betrag. Das Unternehmen ist dadurch in seiner Existenz bedroht. Für den ausgefallenen Administrator muss zusätzlich auch noch ein geeigneter Nachfolger gefunden werden.

Maßnahmen:

- System-Einstellungen und –Parameter ausführlich dokumentieren
- Passwörter sicher hinterlegen
- Notfallplan mit Anweisungen für die Verfahrensweise bei den wichtigsten Schadensfällen erstellen
- Vertretungsregelungen einrichten

1.4 Hackerangriff aus dem Internet

In einer Kleinstadt betreibt ein Einzelhändler sein Geschäft. Seine Kunden- und Lieferantendaten verwaltet er auf einem PC mit Internetanschluss. Er kennt sich mit seinem PC gut aus und installiert seine Software in der Regel selbst. Seine Daten hält er für sicher, da er sich mit einem Passwort am System anmelden muss. Eines Tages verbreitet sich in der ganzen Stadt wie ein Lauffeuer die Nachricht, dass Kunden- und Lieferantendaten anonym in einem lokalen Internet-Diskussionsforum der Stadt veröffentlicht wurden. Die Polizei stößt bei ihren Ermittlungen auf den Einzelhändler und stellt fest: Der betrieblich genutzte PC war völlig unzureichend gegen Fremdzugriffe gesichert und wurde vermutlich Ziel eines Hackerangriffs. Der Staatsanwalt erhebt Anklage, da mit vertraulichen Daten fahrlässig umgegangen wurde. Der entstandene Schaden für die betroffenen Kunden und Lieferanten ist enorm und nicht quantifizierbar.

Maßnahmen:

- Internet-Zugänge sichern
- vertrauliche Daten verschlüsseln

1.5 Innentäter

Ein kleines Traditionsunternehmen stellt seit vielen Jahren spezielle Farben und Lacke nach geheim gehaltenen Rezepturen her. Eines Tages wechselt ein Mitarbeiter aus der Marketingabteilung zur Konkurrenz. Ein halbes Jahr später bringt das Konkurrenzunternehmen nahezu identische Lacke auf den Markt. Es ist zunächst nicht ersichtlich, wie die geheimen Formeln das Unternehmen verlassen konnten, da die Entwicklungsabteilung aus Sicherheitsgründen weder an das Intranet noch an das Internet angeschlossen ist. Das Unternehmen vermutet daher Industriespionage des früheren Mitarbeiters und erstattet Anzeige.

Die Kriminalpolizei kann mit Hilfe geeigneter Werkzeuge nachweisen, dass auf dem PC des Verdächtigen Dateien abgespeichert und später wieder gelöscht wurden, die die fraglichen Rezepturen enthielten. Konfrontiert mit diesem Sachverhalt legt der Verdächtige ein Geständnis ab. Die Räume der Entwicklungsabteilung waren nachts

nicht verschlossen und konnten daher von jedem Mitarbeiter, der über einen Schlüssel zum Gebäude verfügt, unbemerkt betreten werden. Nach Feierabend hatte er die Entwicklungsabteilung aufgesucht und sich mit Hilfe einer Boot-CD unter Umgehung des Kennwortschutzes Zugang zu den entsprechenden Rechnern verschafft. Sein neuer Arbeitgeber hatte ihn nämlich bei seiner Bewerbung gefragt, ob er auch über „wertvolle Zusatzkenntnisse aus dem Unternehmensumfeld“ verfüge, die ihn gegenüber anderen Bewerbern hervorheben würden.

Sowohl der Dieb als auch zwei Manager seines neuen Arbeitgebers werden angeklagt und erhalten eine Haftstrafe. Die beiden Unternehmen einigen sich außergerichtlich auf eine Schadensersatzzahlung. Trotzdem hat das Unternehmen seinen Wettbewerbsvorteil weitgehend eingebüßt, was zu einer zunehmenden Verschlechterung seiner wirtschaftlichen Lage führt.

Maßnahmen:

- Räume und Gebäude gegen unbefugten Zutritt sichern
- wichtige Daten verschlüsseln

2 Die häufigsten Versäumnisse

2.1 Unzureichende Informationssicherheitsstrategie

2.1.1 Sicherheit hat einen zu geringen Stellenwert

Informationssicherheit hat im Vergleich mit anderen Anforderungen (Kosten, Bequemlichkeit, große Funktionalität, ...) häufig einen zu geringen Stellenwert. Stattdessen wird Informationssicherheit lediglich als Kostentreiber und Behinderung gesehen. Besonders bei Neuanschaffungen werden Sicherheitseigenschaften einer Anwendung oder eines Systems häufig vernachlässigt oder gar nicht bedacht. Dafür gibt es verschiedene Gründe: Mangelnde Managementunterstützung für Informationssicherheit, ungenügende Recherche über Sicherheitsaspekte, neue Trends in der Branche, Marketinggesichtspunkte oder knappe Budgets etc. Sicherheitsmängel treten zumeist nicht unmittelbar zu Tage. Stattdessen erhöht sich „nur“, dass aus diesen Defiziten erwachsende Risiko. Im ungünstigsten Fall werden notwendige Sicherheitsmaßnahmen immer wieder auf unbestimmte Zeit verschoben, da sie jedes Mal niedriger priorisiert sind als zwischenzeitlich neu hinzukommende andere Aufgaben.

2.1.2 Dauerhafte Prozesse zur Beibehaltung des Sicherheitsniveaus fehlen

Sicherheit wird häufig nur im Rahmen isolierter Einzelprojekte geschaffen. Diese Projekte sind notwendig, um spezifische Aufgaben anzustoßen und Sachverhalte in angemessener Tiefe zu bearbeiten. Häufig wird jedoch versäumt, im Rahmen solcher

Projekte zugleich verlässliche Prozesse zu definieren, die die im Projektverlauf erarbeiteten Ergebnisse und Ziele dauerhaft erhalten. So werden beispielsweise aufwändige Schwachstellenanalysen durchgeführt und Maßnahmenempfehlungen formuliert. Deren spätere Umsetzung wird jedoch nicht mehr konsequent verfolgt. Ebenso werden bei der Einführung neuer Systeme meistens detaillierte Vorgaben für die sichere Grundinstallation aufgelistet. Im späteren Produktivbetrieb ändern sich die Parametereinstellungen erfahrungsgemäß ständig. Trotzdem findet eine Überprüfung auf Konformität mit den ursprünglichen Vorgaben nur selten statt. Beispiele dieser Art finden sich in zahlreicher Form. Viele dieser Defizite sind eine Ausprägung schlechten internen Informationssicherheitsmanagements: Teils fehlen klare Zuständigkeiten für sicherheitsrelevante Aufgaben, teils werden vereinbarte Maßnahmen nicht regelmäßig überprüft.

2.1.3 Sicherheitsvorgaben sind nicht dokumentiert

Viele große Institutionen verfügen über eine schriftlich fixierte Sicherheitsrichtlinie und zugehörige Hinweise zu deren Anwendung. In den meisten kleineren und mittelständischen Unternehmen und Behörden ist dies jedoch nicht der Fall. Viele Richtlinien sind darüber hinaus zu abstrakt formuliert und lassen zu viel Interpretationsspielraum. Falls Richtlinien existieren, werden diese häufig nicht allen Betroffenen bekannt gegeben. Oftmals fehlt auch der verbindliche Charakter im Sinne einer vom Mitarbeiter explizit vertraglich anerkannten Richtlinie. Dies kann in Einzelfällen dazu führen, dass Sicherheitsverstöße nicht oder nur schwer zu ahnden sind.

2.1.4 Kontrollmechanismen und Aufklärung im Fall von Verstößen fehlen

Bestehende Sicherheitsrichtlinien und -vorgaben sind nur dann wirksam, wenn ihre Einhaltung auch kontrolliert werden kann. Diese Kontrolle wird 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 führen in der Folge zu einer zunehmenden Missachtung bestehender Vorschriften, erhöhen dadurch das Sicherheitsrisiko und enden in tatsächlichen Schadensfällen.

2.2 Unzureichende Konfiguration von IT-Systemen

2.2.1 Die Rechtevergabe wird nicht restriktiv genug gehandhabt

Eine der goldenen Regeln der Informationssicherheit ist das so genannte Need-to-Know-Prinzip: Jeder Benutzer (und auch jeder Administrator) sollte nur auf jene Datenbestände zugreifen und jene Programme ausführen dürfen, die er für seine tägliche Arbeit auch wirklich benötigt. In der Praxis bedeutet dies allerdings zusätzlichen administrativen und technischen Aufwand. Daher haben die meisten

Mitarbeiter Zugriff auf eine Vielzahl sensitiver Daten und Programme, die sie nicht benötigen. Da die Arbeitsplatz-PCs und Server einer Organisation in der Regel alle untereinander vernetzt sind, kann ohne geeignete Zugriffsbeschränkungen oftmals auf die Daten anderer Benutzer bzw. Rechner zugegriffen werden. Den jeweiligen „Besitzern“ dieser Daten ist das häufig nicht bewusst. Die weitreichenden Berechtigungen können so versehentlich, durch Unkenntnis oder beabsichtigt missbraucht werden.

2.2.2 IT-Systeme sind schlecht konfiguriert

Durch Fehler bei der Administration entstehen in der Praxis die mit Abstand meisten Sicherheitslücken – und nicht etwa durch Softwarefehler. Würden die in Standardsoftware vorhandenen Sicherheitsfunktionalitäten vollständig und richtig ausgenutzt, so wäre das Sicherheitsniveau in Unternehmen und Behörden weitaus höher. Die Komplexität von Standard-Büroanwendungen steigt von Jahr zu Jahr. Sicherheit ist für Administratoren nur eine unter vielen, teils konkurrierenden Anforderungen in der täglichen Arbeit. Sie sind de facto kaum noch in der Lage, falsche (unsichere) Parametereinstellungen vollständig zu vermeiden. Vielen Betroffenen ist dieses Dilemma bewusst – doch ohne ausreichende Unterstützung seitens ihrer Vorgesetzten ist eine Änderung unrealistisch.

2.3 Unsichere Vernetzung und Internet-Anbindung

2.3.1 Sensitive Systeme sind gegen offene Netze unzureichend abgeschottet

Solange Informationen und Daten lediglich im internen Netz verfügbar sind, beschränkt sich das Risiko im Fall von Sicherheitslücken auf einen überschaubaren Täterkreis (Mitarbeiter). Bei einer Öffnung zum Internet muss jedoch damit gerechnet werden, dass Schwachstellen von anonymen Dritten, beispielsweise Hackern, aufgespürt und missbraucht werden. Die sichere Anbindung bestehender Applikationen an das Internet erfordert von den betroffenen Administratoren spezifische Kenntnisse, ohne die Konfigurationsfehler kaum zu vermeiden sind. Sensitive Informationen, Systeme und Teilnetze werden oftmals gar nicht oder nur unzureichend von offenen Netzen abgeschottet. Selbst die Existenz einer Firewall sagt nichts über den tatsächlichen Sicherheitszustand aus. Viele Fachverantwortliche denken, ihr Netz sei nach außen abgesichert. Eine Überprüfung durch (externe) Sicherheitsspezialisten zeigt aber in vielen Fällen gravierende Sicherheitslücken auf.

2.4 Nichtbeachtung von Sicherheitserfordernissen

2.4.1 Sicherheitsmaßnahmen werden aus Bequemlichkeit vernachlässigt

Die besten Richtlinien und Sicherheitsfunktionen helfen nichts, falls sie nicht beachtet oder nicht genutzt werden. Vertrauliche Dokumente oder E-Mails werden oftmals nicht verschlüsselt, selbst wenn geeignete Mechanismen unmittelbar zur Verfügung stehen.

Sichere, regelmäßig geänderte Kennwörter werden ebenso als lästig empfunden wie Bildschirmschoner mit Kennwort. Einem x-beliebigen Anrufer, der sich als neuer Mitarbeiter der IT-Abteilung ausgibt, werden Passwörter verraten, wenn er nur „nett“ danach fragt.

Daten, insbesondere von Notebooks, werden selten oder nie gesichert, obgleich den Beteiligten die hohen Risiken eines Datenverlustes durchaus bekannt sind. Selbst wenn regelmäßige Datensicherungen durchgeführt werden, sind diese oft unvollständig oder fehlerhaft. Bei automatisierten Sicherungen wissen Mitarbeiter oftmals gar nicht, welche Daten in welchen Abständen gesichert werden und wie lang die Sicherungsmedien aufbewahrt werden. Zahlreiche weitere Beispiele ähnlicher Art existieren und belegen, dass selbst einfache Sicherheitsmaßnahmen zum Scheitern verurteilt sind, wenn deren Durchführung keine Akzeptanz findet oder sie nicht technisch erzwungen werden können. Dies gilt nicht nur für Anwender, sondern auch für Administratoren. Letztere achten nur selten auf hinreichend sichere Parametereinstellungen. Administratoren arbeiten zudem häufig mit Systemprivilegien. Auch wenn dies technisch nicht erforderlich ist, ist es bequemer als sich ein zweites Mal anzumelden.

2.4.2 Anwender und Administratoren sind mangelhaft geschult

Die sich ständig wandelnden IT-Systeme und Applikationen in Unternehmen und Behörden fordern von allen Beteiligten ein Höchstmaß an Eigeninitiative für den kompetenten Umgang mit diesen Systemen. Um zunehmend komplexe Systeme angemessen zu beherrschen, ist spielerisches Erlernen allerdings wenig geeignet, zumal dies häufig nicht in Testumgebungen erfolgt. Handbücher sind nicht immer vorhanden. Häufig fehlt auch die Zeit, diese zu lesen. Schulungen decken oft nicht die spezifischen Bedürfnisse der Teilnehmer ab. Zudem sind Seminare in der Regel teuer, und die Teilnehmer fallen für die Dauer der Fortbildung für ihr Tagesgeschäft in der eigenen Organisation aus. Detailkenntnisse nur in einzelnen, ausgewählten Vertiefungsgebieten (wie beispielsweise Windows 7, Lotus Domino oder Apache) sind außerdem selten ausreichend, da hierbei die inhaltlichen Querbeziehungen zwischen verschiedenen Aspekten nicht berücksichtigt werden.

2.5 Schlechte Wartung von IT-Systemen

2.5.1 Verfügbare Sicherheits-Updates werden nicht eingespielt

Administratoren spielen oftmals Sicherheits-Patches nicht rechtzeitig ein. Viele durch Viren oder Würmer entstandene Schäden treten erst geraume Zeit nach dem ersten Bekanntwerden des Schädlings auf. Zu diesem Zeitpunkt gibt es in der Regel bereits Sicherheits-Patches von den jeweiligen Herstellern. Inzwischen werden zu den meisten Produkten Sicherheits-Patches in sehr kurzen Abständen veröffentlicht. Auswahl und Tests der im eigenen Kontext tatsächlich relevanten Patches

beanspruchen zusätzliche Zeit. Viele Administratoren warten daher lieber bis zur Installation des nächsten regulären Software-Updates. Ein solches Verhalten ist fahrlässig.

2.6 Sorgloser Umgang mit Passwörtern und Sicherheitsmechanismen

2.6.1 Mit Passwörtern wird zu sorglos umgegangen

Nach wie vor werden die meisten Zugangsschutzverfahren auf Basis von Passwortabfragen realisiert. Dies führt immer dann zu Problemen, wenn unsichere (z. B. zu kurze oder leicht erratbare) Kennwörter gewählt werden. Es finden tagtäglich Einbrüche in IT-Systeme statt, weil ein Angreifer erfolgreich ein Kennwort geknackt hat – wahlweise durch systematisches Ausprobieren, Raten oder Ausspähen. Das sprichwörtliche Aufbewahren des Passwortes unter der Tastatur oder in der obersten Schreibtischschublade macht es Tätern mit Zugang zu Büroräumen besonders leicht, an sensitive Informationen heranzukommen.

2.6.2 Vorhandene Sicherheitsmechanismen werden nicht genutzt

Viele Produkte werden mit eingebauten Sicherheitsmechanismen geliefert, die aber aus Bequemlichkeit, Misstrauen oder Kompatibilitätsgründen nicht aktiviert oder zu schwach eingestellt werden. Beispielsweise wird die vorhandene Verschlüsselungsfunktion in drahtlosen Netzen (WLANs) viel zu selten genutzt.

2.7 Mangelhafter Schutz vor Einbrechern und Elementarschäden

2.7.1 Räume und IT-Systeme werden nur ungenügend gegen Diebstahl oder Elementarschäden geschützt

Einbrecher und Diebe haben oft allzu leichtes Spiel. 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 einerseits nur unter Mühen wiederzubeschaffen. Andererseits droht die Gefahr, dass der Dieb vertrauliche Daten missbrauchen könnte. Katastrophen wie Brände oder Überschwemmungen sind zwar recht seltene Ereignisse, aber wenn sie eintreten, sind die Folgen meistens fatal. Brandschutzmaßnahmen, Schutz vor Wasserschäden und die Sicherstellung der Stromversorgung sollten daher als wichtiger Bestandteil der Informationssicherheit verstanden werden.

3 Organisation des Sicherheitsprozesses

Informationssicherheit gilt als wesentliche Aufgabe im Unternehmen und muss als solche im Unternehmen fest verankert sein. Hierzu bedarf es einer

Organisationsstruktur, verantwortlicher Rollen und zugewiesener Aufgaben und Prozesse.

3.1 Aufbau der Informationssicherheitsorganisation

Die grundlegende Verantwortung für die Informationssicherheit trägt die Geschäftsleitung. Diese muss verantwortlich in die Informationssicherheitsorganisation eingebunden sein. Die Geschäftsleitung trägt die Gesamtverantwortung für den gesamten Informationssicherheitsprozess und dazugehörige und benachbarte Themen wie z.B. Datenschutz. Die Geschäftsleitung initiiert, steuert und kontrolliert den Informationssicherheitsprozess und erlässt die notwendigen Leitlinien (Ziele der Informationssicherheit, Strategie der Umsetzung, Verantwortlichkeiten, Ressourcen).

Durch die Geschäftsleitung ist ein Informationssicherheitsbeauftragter (ISB) als Ansprechpartner für alle Aspekte rund um das Thema Informationssicherheit zu ernennen. Der ISB steuert und koordiniert den Informationssicherheitsprozess, berät und unterstützt die Geschäftsleitung bei allen Fragen rund um die Informationssicherheit, entwürft die Informationssicherheitskonzepte- und Richtlinien und initiiert und koordiniert die Umsetzung von Informationssicherheitsmaßnahmen, die Untersuchung sicherheitsrelevanter Vorfälle und ist verantwortlich für Sensibilisierung und Schulung von Mitarbeitern (Awareness).

Die Rolle des Informationssicherheitsbeauftragten sollte im Unternehmen unabhängig sein. Interessenskonflikte durch andere Tätigkeitsfelder (z.B. IT-Admin, IT-Projektleiter) sind zu vermeiden. Die Aufgaben und Verantwortlichkeiten des ISB sind festzulegen.

3.2 Konzeption des Sicherheitsprozesses

Informationssicherheit auf einem angemessenen Niveau trägt einen elementaren Anteil daran, dass eine Institution ihre Geschäftsziele erreichen kann. Daher müssen die folgenden Einflussfaktoren betrachtet werden:

- **Geschäftsziele**: Welche Faktoren sind wesentlich für den Erfolg des Unternehmens oder der Behörde? Welche Produkte, Angebote und Aufträge bilden die Grundlage der Geschäftstätigkeit? Was sind die generellen Ziele der Institution? Welche Rolle spielt Informationssicherheit hierbei?
- **Organisationsstruktur**: Wie ist die Institution organisiert und strukturiert? Welche Managementsysteme sind vorhanden (beispielsweise Risikomanagement oder Qualitätsmanagement)?
- **Zusammenarbeit mit Externen**: Wer sind die wichtigsten Kunden, Partner und Gremien? Welche grundlegenden Anforderungen und Erwartungen an die

Informationssicherheit der Institution bringen sie mit? Wer sind die wichtigsten Dienstleister und Zulieferer? Welche Rolle spielen diese für die Informationssicherheit der Institution?

- **Strategischer Kontext**: Was sind die wesentlichen Herausforderungen für die Institution? Wie ist die Wettbewerbsposition?

4 Erstellung einer Sicherheitskonzeption nach der Vorgehensweise Basis Absicherung des BSI

4.1 Festlegung des Geltungsbereichs für die Basis-Absicherung

Bei der Erstellung einer Sicherheitskonzeption muss als Erstes festgelegt werden, welchen Bereich der Institution sie abdecken soll (Geltungsbereich). Der Geltungsbereich kann die gesamte Institution umfassen oder auch nur einzelne Bereiche. Auf jeden Fall muss der Geltungsbereich klar abgegrenzt und sinnvoll in sich abgeschlossen sein, mit wenigen, eindeutig definierten Schnittstellen. So könnte eine Institution beispielsweise für eine neu hinzugekommene Abteilung mit ihren Geschäftsprozessen und Assets zunächst die Basis-Absicherung umsetzen.

Der Geltungsbereich für die Erstellung der Sicherheitskonzeption wird im Folgenden „Informationsverbund“ genannt. Ein Informationsverbund umfasst die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Informationsverarbeitung einer Institution oder auch einzelne Bereiche umfassen, die nach organisatorischen oder technischen Strukturen (z. B. Abteilungsnetz) oder gemeinsamen Geschäftsprozessen bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind.

4.2 Auswahl und Priorisierung für die Basis-Absicherung

Der nächste Schritt besteht darin, den betrachteten Informationsverbund mithilfe der in der Ersterfassung identifizierten Prozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume und den vorhandenen Bausteinen aus dem IT-Grundschutz-Kompendium nachzubilden. Das Ergebnis ist ein IT-Grundschutz-Modell des Informationsverbunds, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten Bausteinen besteht und durch die Verwendung der Bausteine die sicherheitsrelevanten Aspekte des Informationsverbunds beinhaltet.

4.2.1 Modellierung nach IT-Grundschutz

Die Modellierung nach IT-Grundschutz besteht nun darin, für die Bausteine einer jeden Schicht zu entscheiden, ob und wie sie zur Abbildung des Informationsverbunds

herangezogen werden können. Je nach betrachtetem Baustein können die Zielobjekte dieser Abbildung von unterschiedlicher Art sein: einzelne Geschäftsprozesse oder Komponenten, Gruppen von Komponenten, Gebäude, Liegenschaften, Organisationseinheiten usw. Können einzelne Zielobjekte nicht unmittelbar mit den vorhandenen Bausteinen abgebildet werden, muss gewährleistet sein, dass ähnliche, verallgemeinerte Bausteine berücksichtigt werden.

4.2.2 Reihenfolge der Baustein-Umsetzung

Um grundlegende Risiken abzudecken und eine ganzheitliche Informationssicherheit aufzubauen, müssen die essenziellen Sicherheitsanforderungen frühzeitig erfüllt und entsprechende Sicherheitsmaßnahmen umgesetzt werden. Daher wird im IT-Grundschutz eine Reihenfolge für die umzusetzenden Bausteine vorgeschlagen.

4.2.3 Ermittlung konkreter Maßnahmen aus Anforderungen

Über die Modellierung wurden die Bausteine des IT-Grundschutz-Kompendiums ausgewählt, die für die einzelnen Zielobjekte des betrachteten Informationsverbunds umzusetzen sind. In den Bausteinen werden die Anforderungen aufgeführt, die typischerweise für diese Komponenten geeignet und angemessen sind.

4.3 IT-Grundschutz für Basis-Absicherung

4.3.1 Organisatorische Vorarbeiten für den IT-Grundschutz

Zunächst sollten alle hausinternen Dokumentationen, Arbeitsanweisungen, die die sicherheitsrelevanten Abläufe regeln, gesichtet werden. Diese Dokumente können bei der Ermittlung des Umsetzungsgrades hilfreich sein. Für jeden Baustein, der für die Modellierung des Informationsverbunds herangezogen wurde, sollte ein Hauptansprechpartner (Fachverantwortlicher) festgelegt werden. Bei den Anforderungen in den Bausteinen werden die Rollen genannt, die für die Umsetzung der Anforderungen zuständig sind. Hieraus können die geeigneten Ansprechpartner für die jeweilige Thematik in der Institution identifiziert werden.

Als Nächstes sollte festgestellt werden, ob und in welchem Umfang externe Stellen an der Ermittlung des Umsetzungsstatus beteiligt werden müssen. Dies kann beispielsweise bei Firmen, die Teile von Geschäftsprozessen oder des IT-Betriebes als outgesourcte Dienstleistungen übernehmen, erforderlich sein.

4.3.2 Durchführung des Soll-Ist-Vergleichs

Bei der Erhebung des erreichten Sicherheitsstatus werden die Sicherheitsanforderungen des jeweiligen Bausteins der Reihe nach durchgearbeitet. Diese können vollständig, teilweise oder nicht erfüllt sein. Als Umsetzungsstatus ist daher jeweils eine der folgenden Aussagen möglich:

- **„entbehrlich“**: Die Erfüllung der Anforderung ist in der vorgeschlagenen Art nicht notwendig, weil die Anforderung im betrachteten Informationsverbund nicht relevant ist (z. B. weil Dienste nicht aktiviert wurden).
- **„ja“**: Zu der Anforderung wurden geeignete Maßnahmen vollständig, wirksam und angemessen umgesetzt.
- **„teilweise“**: Die Anforderung wurde nur teilweise umgesetzt.
- **„nein“**: Die Anforderung wurde noch nicht erfüllt, also geeignete Maßnahmen sind größtenteils noch nicht umgesetzt.

4.3.3 Dokumentation der Ergebnisse

Die Ergebnisse des IT-Grundschutz-Checks sollten so dokumentiert werden, dass sie für alle Beteiligten nachvollziehbar sind und als Grundlage für die Umsetzungsplanung der defizitären Anforderungen und Maßnahmen genutzt werden können. Es sollten geeignete Hilfsmittel verwendet werden, die bei der Erstellung und Aktualisierung aller im Sicherheitsprozess erforderlichen Dokumente unterstützen, beispielsweise spezielle IT-Grundschutz-Tools oder selbst entwickelte Tabellen. Als Hilfsmittel stehen auch auf der IT-Grundschutz-Website entsprechende Formulare für die jeweiligen Bausteine zur Verfügung.

4.4 Realisierung

Generell müssen für die Basis-Absicherung alle identifizierten Basis-Anforderungen erfüllt werden. Auch für die Erfüllung der Basis-Anforderungen stehen in der Regel nur beschränkte Ressourcen an Geld und Personal zur Verfügung. Das primäre Ziel der nachfolgend beschriebenen Schritte ist es daher, eine möglichst effiziente Erfüllung der vorgesehenen Basis-Anforderungen zu erreichen:

- **Sichtung der Untersuchungsergebnisse:** In einer Gesamtsicht sollten zuerst die fehlenden oder nur teilweise erfüllten Basis-Anforderungen ausgewertet werden.
- **Konsolidierung der Basis-Anforderungen**: In diesem Schritt werden zunächst die noch zu erfüllenden Basis-Anforderungen konsolidiert.
- **Kosten- und Aufwandsschätzung:** Es sollte für jede zu erfüllende Basis-Anforderung festgehalten werden, welche Investitionskosten und welcher Personalaufwand dafür notwendig sind.
- **Festlegung der Umsetzungsreihenfolge der Basis-Anforderungen:** Wenn das vorhandene Budget oder die personellen Ressourcen nicht ausreichen, um die fehlenden Basis-Anforderungen sofort erfüllen zu können, muss eine Umsetzungsreihenfolge festgelegt werden.
- **Festlegung der Aufgaben und der Verantwortung:** Es muss festgelegt werden, wer bis wann welche Basis-Anforderungen erfüllen muss.

- **Realisierungsbegleitende Basis-Anforderungen:** Überaus wichtig ist es, notwendige realisierungsbegleitende Basis-Anforderungen, wie beispielsweise Schulungen, rechtzeitig zu konzipieren und für die Realisierung mit einzuplanen.

4.5 Auswahl einer folgenden Vorgehensweise

Informationssicherheit muss gelebt werden. Um das Sicherheitsniveau aufrechtzuerhalten und kontinuierlich verbessern zu können, müssen nicht nur die erforderlichen Sicherheitsmaßnahmen umgesetzt und fortlaufend aktualisiert werden, sondern auch der gesamte Prozess der Informationssicherheit muss regelmäßig auf seine Wirksamkeit und Effizienz hin überprüft werden.

Die Basis-Absicherung ist eine IT-Grundschutz-Vorgehensweise für den Einstieg, um zunächst zeitnah die wichtigsten Sicherheitsempfehlungen für den ausgewählten Einsatzbereich identifizieren und umsetzen zu können. Ziel ist es daher, mittelfristig ein vollständiges Sicherheitskonzept gemäß der Standard-Absicherung zu erstellen. Als Zwischenschritt könnte nach der Basis-Absicherung und vor der Standard-Absicherung die nun erstellte Sicherheitskonzeption um die Kern-Absicherung ergänzt werden.

Nachdem die Basis-Absicherung realisiert wurde, sollte zeitnah entschieden werden, wann mit dem notwendigen Verbesserungsprozess begonnen wird.

5 Wichtige Sicherungsmaßnahmen

5.1 Access Management/Berechtigungsmanagement

Benutzer oder auch IT-Komponenten, die auf die Ressourcen einer Institution zugreifen, müssen zweifelsfrei identifiziert und authentisiert werden.

Beim Berechtigungsmanagement geht es darum, ob und wie Benutzer oder IT-Komponenten auf Informationen oder Dienste zugreifen und diese benutzen dürfen, ihnen also basierend auf dem Benutzerprofil Zutritt, Zugang oder Zugriff zu gewähren oder zu verweigern ist. Berechtigungsmanagement bezeichnet die Prozesse, die für Zuweisung, Entzug und Kontrolle der Rechte erforderlich sind.

Es muss geregelt werden, wie Benutzer und Benutzergruppen einzurichten sind. Alle Benutzer und Benutzergruppen dürfen nur über separate administrative Rollen eingerichtet werden.

Benutzerkennungen und Berechtigungen dürfen nur aufgrund des tatsächlichen Bedarfs vergeben werden. Bei personellen Veränderungen sind die nicht mehr benötigten Benutzerkennungen und Berechtigungen zu entfernen. Beantragen

Mitarbeiter Berechtigungen, die über den Standard hinausgehen, sind diese nur nach zusätzlicher Begründung zu vergeben.

Es muss eine Dokumentation der zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile erfolgen. Die Dokumentation der zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile muss regelmäßig auf Aktualität überprüft werden. Die Dokumentation MUSS vor unberechtigtem Zugriff geschützt werden. Sofern sie in elektronischer Form erfolgt, sollte sie in das Datensicherungsverfahren einbezogen werden.

Es müssen die für den IT-Einsatz relevanten Aufgaben und Funktionen definiert werden. Auch muss festgelegt werden, welche Aufgaben und Funktionen nicht miteinander vereinbar sind. Diese Trennungen müssen umgesetzt und sollten dokumentiert werden.

Es muss festgelegt werden, welche Zugangsberechtigungen, Zutrittsberechtigungen und Zugriffsrechte an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Werden Zugangsmittel wie Chipkarten verwendet, so muss die Ausgabe bzw. der Entzug dokumentiert werden. Die Zugangsberechtigten sollten auf den korrekten Umgang mit den Zugangsmitteln geschult werden. Bei längeren Abwesenheiten sollten berechtigte Personen vorübergehend gesperrt werden.

Die Institution muss den Passwortgebrauch verbindlich regeln. Dabei ist festzulegen, dass nur Passwörter mit ausreichender Länge und Komplexität verwendet werden. Die Passwörter sollten in angemessenen Zeitabständen geändert werden. Die Passwörter müssen sofort gewechselt, sobald sie unautorisierten Personen bekannt geworden sind oder der Verdacht darauf besteht. Passwörter müssen geheim gehalten werden. Standardpasswörter sind durch ausreichend starke Passwörter ersetzt und vordefinierte Logins zu ändern. Es sollte überprüft werden, dass die mögliche Passwortlänge auch im vollen Umfang von dem IT-System geprüft wird.

5.2 Patch- und Änderungsmanagement

Wenn Änderungen an IT-Komponenten, Software oder Konfigurationsdaten umgesetzt werden sollen, muss es dafür Vorgaben geben, die auch Sicherheitsaspekte berücksichtigen. Alle Patches und Änderungen müssen geeignet geplant, genehmigt und dokumentiert werden. Patches und Änderungen sollten vorab geeignet getestet werden. Patches und Änderungen sollten nach Wichtigkeit und Dringlichkeit klassifiziert und entsprechend umgesetzt werden. Wenn Patches und Änderungen durchgeführt werden, müssen Rückfall-Lösungen vorhanden sein. An größeren Änderungen müssen zudem das Informationssicherheitsmanagement und der Informationssicherheitsbeauftragte beteiligt sein. Insgesamt muss sichergestellt

werden, dass das angestrebte Sicherheitsniveau während und nach den Änderungen erhalten bleibt.

Für alle Organisationsbereiche müssen Verantwortliche für das Patch- und Änderungsmanagement festgelegt werden.

Innerhalb des Patch- und Änderungsmanagement muss definiert werden, wie mit integrierten Update-Mechanismen (Autoupdate) der eingesetzten Software umzugehen ist. Insbesondere muss festgelegt werden, wie diese Mechanismen abgesichert und passend konfiguriert werden, um den Vorgaben aus dem Konzept zum Patchmanagement gerecht zu werden. Außerdem sollten neue Komponenten daraufhin überprüft werden, ob und welche Update-Mechanismen diese haben.

5.3 Datensicherung

Für jedes IT-System und eventuell für einzelne besonders wichtige IT-Anwendung müssen die relevanten Einflussfaktoren ermittelt werden, wie z. B. Änderungsvolumen, Änderungszeitpunkte, Verfügbarkeitsanforderungen, Integritätsbedarf. Dazu sollten die Administratoren und die Verantwortlichen der einzelnen IT-Anwendungen befragt werden. Die Ergebnisse müssen nachvollziehbar und auf geeignete Weise festgehalten werden. Neue Anforderungen müssen zeitnah in einem aktualisierten Datensicherungskonzept berücksichtigt werden.

Für jedes IT-System und für jede Datenart muss ein Verfahren festgelegt werden, wie die Daten zu sichern sind. Dazu müssen Art, Häufigkeit und Zeitpunkte der Datensicherungen bestimmt werden. Weiterhin müssen die Verantwortlichkeiten für die Datensicherungen festgelegt werden. Auch muss definiert sein, welche Speichermedien benutzt werden und wie die Transport- und Aufbewahrungsmodalitäten auszusehen haben.

Die rechtlichen Anforderungen an die Datensicherung müssen ermittelt und in das Minimal- bzw. in das Datensicherungskonzept einfließen

Es muss ein Minimaldatensicherungskonzept erstellt werden, das festgelegt, welche Anforderungen für die Datensicherung mindestens einzuhalten sind. Dazu zählen kurze Beschreibungen, wie die Datensicherung erstellt und wiederhergestellt werden kann, welche Parameter gewählt wurden und welche Hard- und Software eingesetzt wird.

Es müssen regelmäßige Datensicherungen durchgeführt werden. Dabei müssen mindestens die Daten regelmäßig gesichert werden, die nicht aus anderen Informationen ableitbar sind. Die erstellten Datensicherungen müssen in geeigneter Weise vor dem Zugriff Dritter geschützt werden. Es muss regelmäßig getestet werden,

ob die Datensicherung auch wie gewünscht funktioniert, vor allem, ob gesicherte Daten problemlos zurückgespielt (Rücksicherungstests) werden können.

5.4 Datenträger

Mobile Datenträger werden für viele unterschiedliche Zwecke eingesetzt, beispielsweise für den Datentransport, die Speicherung von Daten oder die Datennutzung unterwegs. Es gibt zahlreiche verschiedene Varianten von mobilen Datenträgern, hierzu gehören unter anderem Wechselplatten, CD-ROMs, DVDs, Magnetbänder, USB-Festplatten und USB-Sticks.

Alle Mitarbeiter müssen über die Arten und Einsatzmöglichkeiten von mobilen Datenträgern aufgeklärt werden. Dazu gehört auch, sie über die verschiedenen Bauformen und Varianten zu informieren, also dass beispielsweise auch ein Smartphone ein mobiler Datenträger ist. Außerdem sollten die Mitarbeiter über potenzielle Risiken und Probleme bei der Nutzung informiert sowie über den Nutzen, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen aufgeklärt werden. Die Mitarbeiter sind zudem regelmäßig über neue Gefahren und Aspekte von mobilen Datenträgern zu unterrichten, z. B. über entsprechende Artikel im Intranet oder in der Mitarbeiterzeitschrift.

Die Benutzer müssen darauf hingewiesen werden, wie sie sorgfältig mit den mobilen Datenträgern umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten. Dabei sollten beispielsweise Fragen zur Aufbewahrung außerhalb von Büro- oder Wohnräumen sowie zur Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen behandelt werden. Beschädigungen oder Verluste sind zeitnah zu melden.

Verlust oder Diebstahl eines dienstlich genutzten mobilen Datenträgers muss umgehend gemeldet werden. Das gilt auch für private Datenträger, die dienstlich genutzt werden. Hierfür muss es in jeder Institution klare Meldewege und Ansprechpartner geben.

Ausfälle oder Defekte sollten ebenfalls gemeldet werden. Insbesondere bei Datenträgern, die für Datensicherungen und Archivierung eingesetzt werden, ist eine hohe Verlässlichkeit und eine lange Lebensdauer wichtig. Verliert ein Mitarbeiter einen mobilen Datenträger oder wird er gestohlen, muss wiederum schnell gehandelt werden, da es hier nicht nur darum geht, das Gerät wiederzubeschaffen, sondern auch darum, potenziellen Missbrauch der betroffenen Informationen zu verhindern.

5.5 Schadsoftware

Schadprogramme sind Programme, die in der Regel ohne Wissen und Einwilligung des Benutzers oder Besitzers eines IT-Systems schädliche Funktionen auf diesem

ausführen. Diese Funktionen können ein breites Feld abdecken, das von Spionagemöglichkeiten über Erpressung (sogenannte Ransomware) bis hin zur Sabotage und Zerstörung von Informationen oder gar Geräten reicht.

Schadprogramme können grundsätzlich auf allen Betriebssystemen und IT-Systemen auftreten. Dazu gehören neben klassischen IT-Systemen wie Clients und Server auch mobile Geräte wie Smartphones. Netzkomponenten wie Router, Industriesteuerungsanlagen und sogar IoT-Geräte wie vernetzte Kameras sind heutzutage ebenfalls vielfach durch Schadprogramme gefährdet.

Schadprogramme verbreiten sich auf klassischen IT-Systemen zumeist über E-Mail-Anhänge, manipulierte Webseiten (Drive-by-Downloads) oder Datenträger. Smartphones werden in der Regel über die Installation von schädlichen Apps infiziert, auch Drive-by-Downloads sind möglich. Darüber hinaus sind offene Netzschnittstellen, fehlerhafte Konfigurationen und Softwareschwachstellen häufige Einfallstore auf allen IT-Systemen.

Es muss ein Konzept erstellt werden, welche IT-Systeme vor Schadprogrammen geschützt werden müssen. Außerdem muss festgehalten werden, wie der Schutz zu erfolgen hat. Ist kein verlässlicher Schutz möglich, so sollten die identifizierten IT-Systeme nicht betrieben werden. Das Konzept sollte nachvollziehbar dokumentiert werden.

In Abhängigkeit vom verwendeten Betriebssystem, anderen vorhandenen Schutzmechanismen sowie der Verfügbarkeit geeigneter Viren-Schutzprogramme muss für den konkreten Einsatzzweck ein solches Schutzprogramm ausgewählt und installiert werden.

Auf den damit ausgestatteten IT-Systemen müssen die Scan-Engine des Viren-Schutzprogramms sowie die Signaturen für die Schadprogramme regelmäßig aktualisiert werden. Die Häufigkeit von qualitätsgesicherten Signatur-Updates muss dabei den Empfehlungen des Herstellers entsprechen.

Ein Update auf neue Programmversionen sollte zeitnah nach Veröffentlichung erfolgen. Bei jedem Programmupdate des Viren-Schutzprogramms sollte die Änderungsdokumentation des Herstellers auf relevante Änderungen hin überprüft werden. Nachdem das Update installiert wurde, müssen die Konfigurationseinstellungen überprüft und mit den dokumentierten Vorgaben abgeglichen werden.

Benutzer sind regelmäßig über die Bedrohung durch Schadprogramme aufzuklären. Sie müssen die grundlegenden Verhaltensregeln einhalten, um die Gefahr eines Befalls durch Schadprogramme zu reduzieren. Dateien aus nicht vertrauenswürdigen Quellen sollten nicht geöffnet werden.

5.6 Sensibilisierung und Schulung

Um Informationssicherheit innerhalb einer Institution erfolgreich und effizient zu verwirklichen, sind die Mitarbeiter ein notwendiger und bedeutender Erfolgsfaktor. Daher müssen sich alle Mitarbeiter über ihre Rollen im Informationssicherheitsmanagement bewusst sein. Sie müssen die Sicherheitsziele der Institution kennen sowie die Sicherheitsmaßnahmen verstehen und bereit sein, sie wirkungsvoll zu unterstützen. Hierfür müssen in der Institution ein Sicherheitsbewusstsein (Awareness) sowie eine Sicherheitskultur aufgebaut und gestaltet werden.

Mitarbeiter müssen für relevante Gefährdungen sensibilisiert werden und wissen, wie sich diese auf ihre Institution auswirken können. Je besser die Mitarbeiter die Gefährdungslage kennen, desto eher werden entsprechende Sicherheitsmaßnahmen akzeptiert. Mitarbeiter müssen über die erforderlichen Kenntnisse verfügen, um Maßnahmen richtig verstehen und anwenden zu können. Insbesondere muss ihnen bekannt sein, was von ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollen.

Die Institutionsleitung muss die Sicherheitskampagnen und Schulungsmaßnahmen für die Mitarbeiter nachdrücklich und aktiv unterstützen. Daher muss vor dem Beginn eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit die Unterstützung des Managements eingeholt werden.

Alle Vorgesetzten müssen die Informationssicherheit unterstützen, indem sie mit gutem Beispiel vorangehen. Durch die Führungskräfte sind die Sicherheitsvorgaben umzusetzen und ihre Mitarbeiter auf deren Einhaltung hinzuweisen.

In jeder Institution muss es Ansprechpartner für Sicherheitsfragen (z.B. Informationssicherheitsbeauftragter) geben, die sowohl scheinbar einfache wie auch komplexe oder technische Fragen beantworten können. Die Ansprechpartner müssen allen Mitarbeitern der Institution bekannt sein. Diesbezügliche Informationen müssen in der Institution für alle leicht zugänglich sein und verfügbar sein.

Alle Mitarbeiter und externen Benutzer sind in den sicheren Umgang mit IT-Komponenten einzuweisen und zu sensibilisieren, soweit dies für ihre Arbeitszusammenhänge relevant ist. Dafür sind verbindliche, verständliche, aktuelle und verfügbare Richtlinien zur Nutzung der jeweiligen Komponenten zur Verfügung zu stellen.

5.7 CEO-Fraud

CEO-Fraud nennt man die betrügerische Masche, bei dem sich Betrüger per E-Mail als Firmenchefs ausgeben, um die Überweisung von teils hohen Geldbeträgen durch

die Mitarbeiter des Unternehmens zu veranlassen. Um das Unternehmen vor Betrug mittels CEO-Fraud zu schützen ist es Linie wichtig, die Mitarbeiter auf die Gefahr hinzuweisen und dafür zu sensibilisieren. Die Sensibilisierung kann durch regelmäßige Tests und Übungen überprüft werden. Durch das Unternehmen sind klare Abwesenheitsregelungen für ihre Mitarbeiter zu treffen.

Bei verdächtigen Zahlungsanweisungen sollten durch die Mitarbeiter die Vorgesetzten oder die Unternehmensleitung zur Rücksprache kontaktiert werden.

5.8 Protokollierung/Monitoring

Für einen verlässlichen IT-Betrieb sollten IT-Systeme und Anwendungen alle oder ausgewählte Betriebs- und sicherheitsrelevanten Ereignisse protokollieren, d.h. sie automatisch speichern und für die Auswertung bereitstellen. Eine Protokollierung wird in vielen Institutionen eingesetzt, um Hard- und Softwareprobleme sowie Ressourcenengpässe zeitnah entdecken zu können. Aber auch Sicherheitsprobleme und Angriffe auf die betriebenen Dienste können anhand von Protokollierungsdaten nachvollzogen werden.

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution, ist eine spezifische Sicherheitsrichtlinie zu erstellen, in der nachvollziehbare Anforderungen und Vorgaben beschrieben sind, wie die Protokollierung sicher geplant, aufgebaut und betrieben werden soll. In der Richtlinie muss geregelt werden, wie, wo und was protokolliert werden soll. Dabei sollten sich Art und Umfang der Protokollierung am Schutzbedarf der Informationen orientieren.

Die Richtlinie muss vom ISB gemeinsam mit den Fachverantwortlichen erstellt werden. Sie muss allen für die Protokollierung verantwortlichen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, ist dies mit dem ISB abzustimmen und zu dokumentieren. Es ist regelmäßig zu überprüfen, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse sind zu dokumentieren.

Bei der Protokollierung müssen die gesetzlichen Bestimmungen aus den aktuellen Gesetzen zum Datenschutz eingehalten werden. Darüber hinaus müssen eventuelle Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitervertretungen gewahrt werden. Ebenso ist sicherzustellen, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden. Protokollierungsdaten sind nach einem festgelegten Prozess zu löschen. Es ist technisch zu unterbinden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.

5.9 Notfallmanagement

In Notfallsituationen ist ein Zugriff auf Informationen zur Wiederherstellung eines Geschäftsprozesses, eines IT-Systems oder einer Fachaufgabe unentbehrlich. Hierzu sollten die entsprechenden Prozesse zur Aufrechterhaltung der Informationssicherheit in einem Notfall geplant, etabliert und überprüft werden.

Nur wenn geplant und organisiert vorgegangen wird, ist eine optimale Notfallvorsorge und Notfallbewältigung möglich. Ein professioneller Prozess zum Notfallmanagement reduziert deren Auswirkungen und sichert somit den Betrieb und Fortbestand der Institution. Es sind geeignete Maßnahmen zu identifizieren und umzusetzen, durch die Geschäftsprozesse und Fachaufgaben zum einen robuster und ausfallsicherer werden und die es zum anderen ermöglichen, den Notfall schnell und zielgerichtet zu bewältigen.

Die Aufrechterhaltung der Informationssicherheit ist deshalb in ein übergreifendes Notfallmanagement einzubinden. Das Notfallmanagement hat jedoch einen eigenen Prozessverantwortlichen (den Notfallbeauftragten), mit dem sich der Informationssicherheitsbeauftragte abstimmt.

Es sollte ein Notfallhandbuch erstellt werden, in dem die wichtigsten Informationen zu

- Rollen,
- Sofortmaßnahmen,
- Alarmierung und Eskalation,
- Kommunikations-, grundsätzlichen Geschäftsfortführungs-, Wiederanlauf- und
- Wiederherstellungsplänen

enthalten sind. Zuständigkeiten und Befugnisse sollten an die entsprechenden Ansprechpartner und Fachverantwortlichen zugewiesen, kommuniziert und im Notfallhandbuch festgehalten werden. Es sollte sichergestellt sein, dass im Notfall entsprechend geschultes Personal zur Verfügung steht. Durch regelmäßige Tests und Übungen wird überprüft, ob die im Notfallhandbuch beschriebenen Maßnahmen auch wie vorgesehen funktionieren.

Das Notfallhandbuch sollte regelmäßig übergeprüft und, falls erforderlich, aktualisiert werden. Es sollte auch im Notfall zugänglich sein. Ergänzt werden sollte das Notfallhandbuch um Verhaltensregeln für Fälle (z. B. Brand, Hochwasser), die allen Mitarbeitern bekannt gegeben werden sollten.

Die Prozesse im Sicherheitsmanagement sind grundsätzlich mit dem Notfallmanagement abzustimmen.

Sehr geehrte Leserin, sehr geehrter Leser,

vielen Dank, dass Sie sich die Zeit für die Lektüre dieses Leitfadens genommen haben. Wir hoffen, dass wir Ihnen einige praktische Hinweise und Anregungen im Zusammenhang mit dem Thema „IT-Sicherheit“ für Ihr Unternehmen geben konnten. Für alles weitere stehen die Spezialisten der AWADO GmbH als kompetenter Ansprechpartner für Sie bereit.

Über die AWADO GmbH

Business as unusual – die AWADO GmbH ist die etwas andere Wirtschaftsprüfungs- und Beratungsgesellschaft. Menschlich, verantwortungsvoll, mit Gemeinschaftssinn. Für uns sind klassische Werte wie Vertrauen, Ehrlichkeit, Loyalität und auch Verantwortungsbewusstsein ein hohes Gut.

Die AWADO GmbH zählt gemeinsam mit Ihrem Netzwerkpartner – einem großen Prüfungs- und Beratungsunternehmen mit rund 125 Wirtschaftsprüfern, 70 Steuerberatern und 60 Rechtsanwälten sowie rund 1.500 weiteren Mitarbeitern – zu den Top 10 Prüfungs- und Beratungsgesellschaften in Deutschland. Die AWADO GmbH steht für:

- Regionalität – durch insgesamt acht bundesweite Standorte bieten wir kurze Wege, Beratungsdienstleistungen aus einer Hand und garantieren Ansprechpartner vor Ort
- Interdisziplinäre, kollegiale, kooperative und effiziente Zusammenarbeit – Grundlagen für eine Maximum an Kundenzufriedenheit
- Schnelle Reaktionszeiten und innovative Lösungsansätze – Basen für individualisierte, bedarfsgerechte und praxistaugliche Lösungen

Als mittelständisch geprägtes Beratungsunternehmen mit einer hohen Spezialisierung im IT-Beratungsmarkt bieten wir vor allem mittelständischen Unternehmen, Einkaufskooperationen und Verbundgruppen jeglicher Größe die nachfolgenden IT-Dienstleistungen an:

- Durchführung von Basischecks zur IT-Sicherheit inklusive adressatengerechten Reporting
- Beratung beim Aufbau- und der Einführung von Informationssicherheitsmanagementsystemen
- Unterstützung bei Umsetzung von Digitalisierungsprojekten
- Unterstützung bei der Umsetzung von technischen und organisatorischen Maßnahmen gemäß Datenschutzgrundverordnung und Bundesdatenschutzgesetz
- Unterstützung bei Auf- bzw. Ausbau sowie Prüfung von internen (IT)-Kontroll- und (IT) Compliance Management-Systemen
- Auditierung digitaler Prozesse
- Anti-Fraud Management

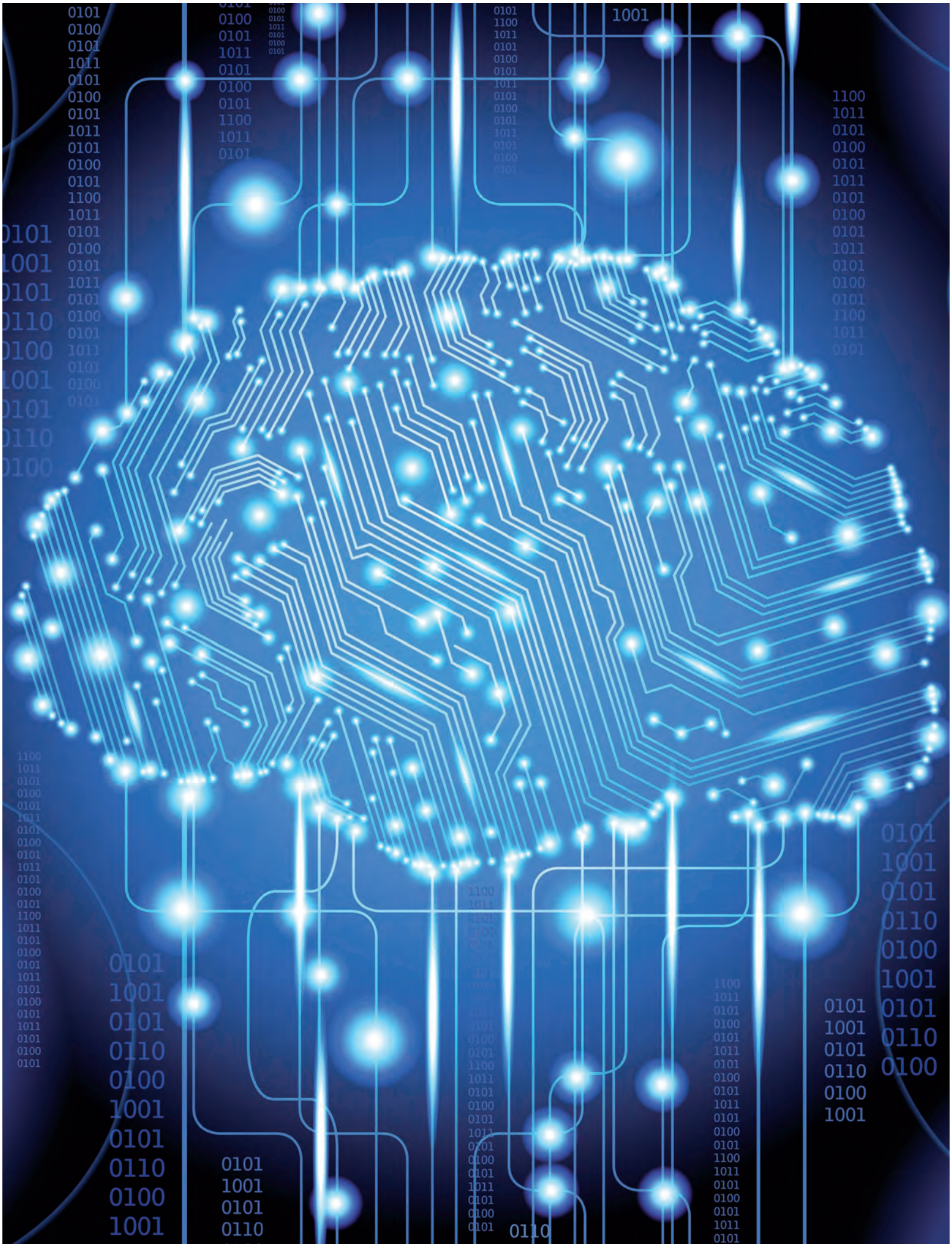
AWADO GmbH

Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft
Peter-Müller-Straße 26
40468 Düsseldorf
www.awado-wpg.de

Ansprechpartner

WP / StB Christian Buschfort
christian.buschfort@awado-wpg.de

Andreas Schmidt,
Leiter IT-Prüfung & IT-Beratung
andreas.schmidt@awado-gruppe.de



eine Kooperation von

Service & Consult ServiCon

AWADO