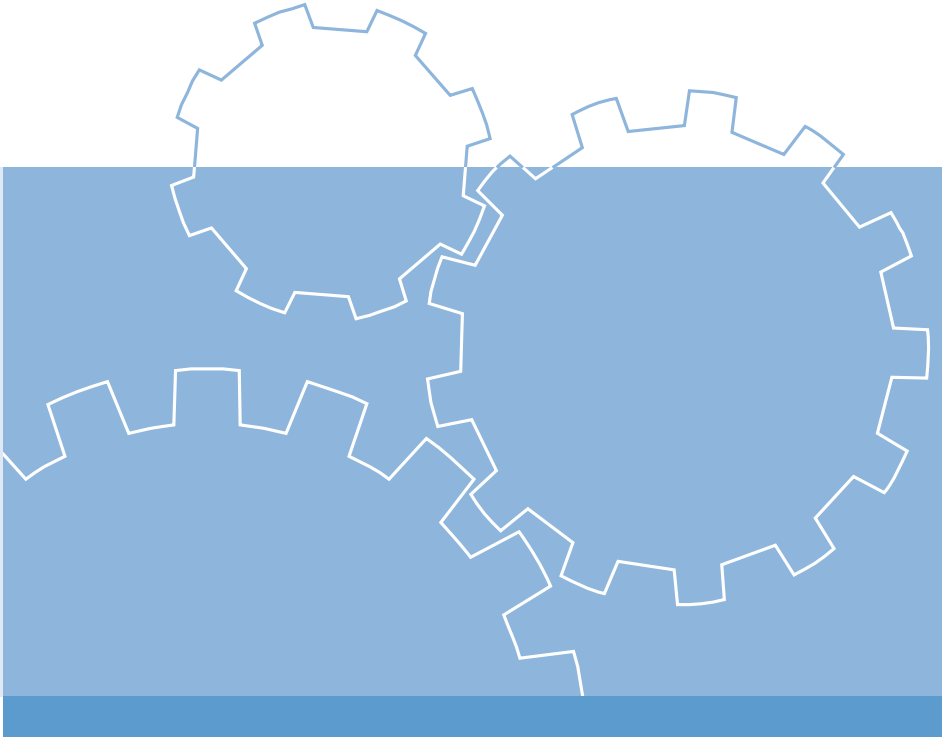
Bundesamt
für Sicherheit in der
Informationstechnik

Leitfaden Informationssicherheit

IT-Grundschutz kompakt



www.bsi.bund.de

Inhaltsverzeichnis

1	Einleitung	6
2	Informationssicherheit im Fokus	7
3	Wichtige Begriffe rund um die Informationssicherheit	11
4	Vorschriften und Gesetzesanforderungen	13
5	So nicht: Schadensfälle als warnendes Beispiel	15
6	Die häufigsten Versäumnisse	21
7	Wichtige Sicherheitsmaßnahmen	28
8	Der IT-Grundschutz des BSI	61
9	Standards und Zertifizierung der eigenen Informationssicherheit	69
10	Anhang	74

Vorwort



Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Arbeits- und Geschäftsprozesse basieren immer stärker auf IT-Lösungen. Die Sicherheit und Zuverlässigkeit der Informations- und Kommunikationstechnik wird deshalb ebenso wie der vertrauenswürdige Umgang mit Informationen immer wichtiger. Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der für manche Institution existenzbedrohend sein kann. Dabei ist ein vernünftiger Informationsschutz ebenso wie eine Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen.

Mit dem richtigen Sicherheitskonzept können Sie ein solides Fundament für ein vertrauenswürdiges Niveau Ihrer Informationssicherheit legen. Dieser Leitfaden hilft Ihnen dabei: In kompakter Form finden Sie einen Überblick über die wichtigsten Sicherheitsmaßnahmen. Praxisbeispiele machen auf Gefahren aufmerksam und veranschaulichen die notwendigen organisatorischen, infrastrukturellen und technischen Maßnahmen. Checklisten unterstützen Sie bei der Analyse der eigenen Situation. Damit steht fest:

Der Weg zu mehr Sicherheit ist auch ohne große IT-Budgets möglich.



Michael Hange
Präsident des Bundesamtes für Sicherheit
in der Informationstechnik (BSI)

Das BSI im Dienst der Öffentlichkeit

Das Bundesamt für Sicherheit in der Informationstechnik wurde am 1. Januar 1991 mit Sitz in Bonn gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern.



Mit seinen derzeit rund 500 Mitarbeiterinnen und Mitarbeitern und 62 Mio. Euro Haushaltsvolumen ist das BSI eine unabhängige und neutrale Stelle für alle Fragen zur IT-Sicherheit in der Informationsgesellschaft.

Als zentraler IT-Sicherheitsdienstleister des Bundes ist das BSI operativ für den Bund, kooperativ mit der Wirtschaft und informativ für den Bürger tätig.

Durch die Grundlagenarbeit im Bereich der IT-Sicherheit übernimmt das BSI als nationale IT-Sicherheitsbehörde Verantwortung für unsere Gesellschaft und ist dadurch eine tragende Säule der Inneren Sicherheit in Deutschland.

Ziel des BSI ist der sichere Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft. IT-Sicherheit soll als wichtiges Thema wahrgenommen und eigenverantwortlich umgesetzt werden. Sicherheitsaspekte sollen schon bei der Entwicklung von IT-Systemen und -Anwendungen berücksichtigt werden.

Das BSI wendet sich mit seinem Angebot an die Anwender und Hersteller von Informationstechnik. Zielgruppe sind die öffentlichen Verwaltungen in Bund, Ländern und Kommunen sowie Privatanwender und Unternehmen.

Der „Leitfaden Informationssicherheit“ gibt einen kompakten Überblick über die wichtigsten organisatorischen, infrastrukturellen und technischen Informationssicherheitsmaßnahmen. Er richtet sich an Fachverantwortliche und Administratoren in kleinen und mittelständischen Unternehmen sowie in Behörden.

1 Einleitung

Das Leben im 21. Jahrhundert ist ohne Informations- und Kommunikationstechnik kaum mehr vorstellbar. Der Schutz von IT-Landschaften wird deshalb immer wichtiger. Auch die geänderte Gesetzeslage trägt dazu bei, die Sensibilität für Informationssicherheitsthemen zu erhöhen: Vorstände und Geschäftsführer sind persönlich für Versäumnisse und mangelnde Risikovorsorge verantwortlich.

In der Praxis ist es aber meistens schwierig, ein angemessenes Sicherheitsniveau zu erreichen und aufrecht zu erhalten. Die Gründe dafür sind vielfältig: fehlende Ressourcen, zu knappe Budgets und nicht zuletzt die steigende Komplexität der IT-Systeme. Eine Vielzahl von IT-Sicherheitsprodukten und -beratern bieten unterschiedlichste Lösungen an. Da haben selbst Experten Mühe, den Überblick zu behalten.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet seit vielen Jahren Informationen und Hilfestellungen rund um das Thema Informationssicherheit: Als ganzheitliches Konzept für Informationssicherheit hat sich das Vorgehen nach IT-Grundschutz zusammen mit den IT-Grundschutz-Katalogen des BSI als Standard etabliert. Diese vom BSI seit 1994 eingeführte und weiterentwickelte Methode bietet sowohl eine Vorgehensweise für den Aufbau einer Sicherheitsorganisation als auch eine umfassende Basis für die Risikobewertung, die Überprüfung des vorhandenen Sicherheitsniveaus und die Implementierung der angemessenen Informationssicherheit. Die IT-Grundschutz-Kataloge dienen außerdem zahlreichen Unternehmen und Behörden als wichtiges Fundament eigener Maßnahmenkataloge. Analog zur Entwicklung in der Informationstechnik sind die Anforderungen an die Informationssicherheit immer komplexer und umfassender geworden. Besonders kleine und mittlere Institutionen mit beschränkten finanziellen und personellen Möglichkeiten wünschen sich deshalb einen leicht überschaubaren Einstieg in die Thematik.

Der vorliegende Leitfaden greift diesen Wunsch auf: Er gibt einen kompakten und allgemeinverständlichen Überblick über die wichtigsten Maßnahmen zur Informationssicherheit. Im Mittelpunkt stehen organisatorische Maßnahmen und die Veranschaulichung von Gefahren durch Praxisbeispiele. Auf technische Details wird bewusst verzichtet.

Fazit: Wer die Empfehlungen aus diesem Leitfaden konsequent umsetzt oder sich bei der Gestaltung von Serviceverträgen mit IT-Dienstleistern daran orientiert, legt bereits ein solides Fundament für ein vertrauenswürdiges Informationssicherheitsniveau.

2 Informationssicherheit im Fokus

Sicherheit ist ein Grundbedürfnis des Menschen – und damit unserer Gesellschaft. Gerade in Zeiten von Globalisierung, steigender Mobilität und wachsender Abhängigkeit der Industrienationen von Informations- und Kommunikationstechnik nimmt das Sicherheitsbedürfnis immer mehr zu.

Wachsende Verwundbarkeit und die Gefahr massiver wirtschaftlicher Schäden in Folge von Risiken bei der Informationsverarbeitung erhöhen den Handlungsdruck, durch aktives Informationssicherheitsmanagement Schäden zu verhindern und das Restrisiko zu minimieren. Die Verantwortung beschränkt sich keineswegs auf die jeweiligen IT-Fachabteilungen. Vielmehr gilt: Sicherheit ist Chefsache. Dem hat auch der Gesetzgeber Rechnung getragen. Verschiedene Gesetze und Regelungen belegen die persönliche Haftung von Geschäftsführern bzw. Vorständen im Falle von Versäumnissen.

Eine weit verbreitete Ansicht ist, dass Sicherheitsmaßnahmen zwangsläufig mit hohen Investitionen in Sicherheitstechnik und der Beschäftigung von hoch qualifiziertem Personal verknüpft sind. Dem ist jedoch nicht so. Die wichtigsten Erfolgsfaktoren sind ein gesunder Menschenverstand, durchdachte organisatorische Regelungen sowie zuverlässige und gut informierte Mitarbeiter, die selbständig Sicherheitserfordernisse diszipliniert und routiniert beachten. Die Erstellung und Umsetzung eines wirksamen und effektiven Informationssicherheitskonzeptes muss darum nicht zwangsläufig unbezahlbar sein. Die wirksamsten Maßnahmen sind überraschend simpel und noch dazu oft kostenlos!

Eine andere weit verbreitete Fehleinschätzung betrifft den eigenen Schutzbedarf. Oft stößt man auf die folgenden Aussagen:

„Bei uns ist noch nie etwas passiert“.
Diese Aussage ist mutig. Vielleicht hat bei früheren Sicherheitsvorfällen niemand etwas bemerkt!

„Was soll bei uns schon zu holen sein, so geheim sind unsere Daten nicht.“
Diese Einschätzung ist in den meisten Fällen zu oberflächlich. Bei sorgfältiger Betrachtung von möglichen Schadensszenarien zeigt sich schnell: Es können durchaus Daten verarbeitet werden, die vielfältigen Missbrauch ermöglichen, wenn sie in die falschen Hände fallen.

„Unser Netz ist sicher.“
Die Fähigkeiten potentieller Angreifer werden oft unterschätzt. Hinzu kommt, dass selbst ein erfahrener Netz- oder Sicherheitsspezialist nicht alles wissen und gelegentlich Fehler machen kann. Externe Überprüfungen decken nahezu immer ernste Schwachstellen auf und sind ein guter Schutz vor „Betriebsblindheit“.

„Unsere Mitarbeiter sind vertrauenswürdig.“

Verschiedene Statistiken zeichnen ein anderes Bild: Die Mehrzahl der Sicherheitsverstöße wird durch Innentäter verursacht. Dabei muss nicht immer Vorsatz im Spiel sein. Auch durch Versehen, Übereifer oder Neugierde gepaart mit mangelndem Problembewusstsein entstehen manchmal große Schäden.

Jeder sollte sich bewusst machen: Sicherheit ist kein statischer Zustand, sondern ein ständiger Prozess. Stellen Sie sich daher immer wieder die folgenden Fragen:

- Welche Formen von Missbrauch wären möglich, wenn vertrauliche Informationen Ihres Unternehmens oder Ihrer Behörde in die Hände Dritter gelangten?

- Welche Konsequenzen hätte es für Sie, wenn wichtige Informationen – z. B. während einer Datenübertragung oder auf ihrem Server – verändert würden? Als Ursache kann nicht nur böse Absicht unbekannter Dritter, sondern auch technisches Versagen in Frage kommen.

- Was würde geschehen, wenn in Ihrer Organisation wichtige Computer oder andere IT-Komponenten plötzlich ausfielen und einen längeren Zeitraum (Tage, Wochen, ...) nicht mehr nutzbar wären? Könnte die Arbeit fortgesetzt werden? Wie hoch wäre der mögliche Schaden?

Wenn Sie ein gut durchdachtes Informationssicherheitskonzept umsetzen, werden sich nach einiger Zeit – neben dem Sicherheitsgewinn – weitere Vorteile einstellen. IT-Leiter beobachten häufig folgende „Nebeneffekte“:

Die Mitarbeiter sind zuverlässiger, die Arbeitsqualität steigt.
Gelebte Informationssicherheit fördert eine Unternehmenskultur, in der verantwortungsbewusstes Handeln, Kundenorientierung und die Identifikation mit den Unternehmenszielen fest verankert sind.

Wettbewerbsvorteile
Nachgewiesene Informationssicherheit schafft Vertrauen bei Kunden und anderen Geschäftspartnern und wird zunehmend von diesen auch eingefordert.

Wartungsarbeiten an IT-Systemen erfordern deutlich weniger Zeit.
Administratoren arbeiten effektiver.
Administratoren und Anwender kennen sich besser mit ihren Systemen aus. IT-Systeme sind gut dokumentiert, was Administrationsarbeiten, Planung, Neuinstallation von Software und Fehlerbeseitigung erleichtert. Ein gutes Informationssicherheitskonzept vermeidet zudem einige Probleme unter denen Administratoren normalerweise besonders leiden: Anwender setzen verschiedene Programme für den gleichen Zweck ein, unterschiedliche Betriebssysteme müssen betreut werden, verschiedene Versionen der gleichen Software sind im Einsatz, jeder Anwender hat individuelle Rechte, Anwender nutzen private Software und gestalten ihren Arbeitsplatz-PC selbst – ohne entsprechendes Know-how. Eine zentrale Administration des „Rechnerzoos“ ist so kaum möglich. Jeder Rechner muss mit hohem Aufwand individuell analysiert und betreut werden.

3 Wichtige Begriffe rund um die Informationssicherheit

Es gibt drei Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität.

Vertraulichkeit: Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.

Verfügbarkeit: Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.

Integrität: Die Daten sind vollständig und unverändert. Der Begriff „Information" wird in der Informationstechnik für „Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung manipuliert wurde.

Weitere häufig verwendete Begriffe sind:

Authentisierung: Bei der Anmeldung an einem System wird im Rahmen der Authentisierung die Identität der Person, die sich anmeldet, geprüft und verifiziert. Der Begriff wird auch verwendet, wenn die Identität von IT-Komponenten oder Anwendungen geprüft wird.

Autorisierung: Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist.

Datenschutz: Unter Datenschutz versteht man den Schutz personenbezogener Daten vor dem Missbrauch durch Dritte (nicht zu verwechseln mit Datensicherheit).

Datensicherheit: Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein anderer Begriff dafür ist „Informationssicherheit".

Datensicherung (engl. Backup): Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt.

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

Risikoanalyse (engl. Risk Assessment / Analysis): Mit einer Risikoanalyse wird untersucht, wie wahrscheinlich das Eintreten eines bestimmten Schadens ist und welche negativen Folgen der Schaden hätte.

Sicherheitsrichtlinie (engl. 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.

4 Vorschriften und Gesetzesanforderungen

Stellen Sie sich vor, bei Ihnen gespeicherte Daten gelangen an die Öffentlichkeit, Daten werden mutwillig oder durch ein Unglück unwiederbringlich zerstört. Oder aus Ihrem Haus werden Massen-E-Mails mit Computer-Viren verschickt. Welche Konsequenzen drohen dem Unternehmen bzw. der Behörde und den verantwortlichen Personen?

Überblick über gesetzliche Regelungen mit Bezug zur Informationssicherheit

Während der vergangenen Jahre wurden mehrere Rechtsvorschriften erlassen, aus denen sich zu Fragen der Informationssicherheit unmittelbare Handlungs- und Haftungsverpflichtungen der Geschäftsführung bzw. des Vorstands eines Unternehmens ableiten lassen. Diese Regelungen gelten sowohl für Aktiengesellschaften als auch für GmbHs. Dies ist in der Öffentlichkeit noch nicht hinreichend bekannt.

In diesem Zusammenhang wird immer wieder auf das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich **(KonTraG)** hingewiesen. Das KonTraG ist ein sog. Artikelgesetz und ergänzt bzw. ändert verschiedene Gesetze wie das Handelsgesetzbuch und das Aktiengesetz. Insbesondere die Forderung nach einem Risikomanagement für Kapitalgesellschaften – d. h. für Aktiengesellschaften und GmbHs – waren in den bisherigen Vorschriften nicht enthalten.

Im Einzelnen könnten Sie z. B. von folgenden Regelungen betroffen sein:

Im **Aktiengesetz** wird festgelegt, dass ein Vorstand persönlich haftet, wenn er Entwicklungen, die zukünftig ein Risiko für das Unternehmen darstellen könnten, nicht durch ein Risikomanagement überwacht und durch geeignete Maßnahmen vorbeugt (§ 91 Abs. 2 und § 93 Abs. 2 AktG).

Geschäftsführern einer GmbH wird im **GmbH-Gesetz** „die Sorgfalt eines ordentlichen Geschäftsmannes“ auferlegt (§ 43 Abs. 1 GmbHG).

Die im Aktiengesetz genannten Pflichten eines Vorstands gelten auch im Rahmen des **Handelsgesetzbuches** (§ 317 Abs. 4 HGB). Weiterhin verpflichtet das Handelsgesetzbuch Abschlussprüfer zu prüfen, „ob die Risiken der künftigen Entwicklung zutreffend dargestellt sind“ (§ 317 Abs. 2 HGB).

Die oben genannten Formulierungen klingen für den juristischen Laien teilweise recht allgemein und unverbindlich. In der Tat lassen sich hieraus jedoch konkrete Verpflichtungen für die Gewährleistung eines angemessenen Informationssicherheitsniveaus im eigenen Unternehmen ableiten. Informationssicherheitsvorfälle können massive wirtschaftliche Schäden verursachen und schlimmstenfalls den Bestand eines Unternehmens gefährden.

Für bestimmte Berufsgruppen wie Ärzte, Rechtsanwälte oder Angehörige sozialer Berufe gibt es darüber hinaus Sonderregelungen im **Strafgesetzbuch**, die sogar Freiheitsstrafen vorsehen, wenn vertrauliche Angaben von Patienten, Mandanten bzw. Klienten ohne Einwilligung öffentlich gemacht werden (§ 203 StGB). Ein fahrlässiger Umgang mit Informationstechnik kann diesen Tatbestand unter Umständen bereits erfüllen.

Belange des Verbraucherschutzes werden in verschiedenen Gesetzen behandelt. Die Verwendung von Informationstechnik, die Nutzung des Internets oder von Telekommunikationsdiensten werden zum Teil sehr genau geregelt. Einschlägig sind z. B.: Gesetz zur Nutzung von Telediensten, Telekommunikationsgesetz, Mediendienste-Staatsvertrag, Urheberrecht sowie verschiedene Richtlinien auf EU-Ebene.

Der Umgang mit personenbezogenen Daten wird in den Datenschutzgesetzen des Bundes und der Länder, dem Gesetz über den Datenschutz bei Tele-

diensten, der Telekommunikations-Datenschutzverordnung sowie teilweise in den bereits aufgezählten Gesetzen geregelt.

Auch Banken sind inzwischen gezwungen, bei der Kreditvergabe IT-Risiken des Kreditnehmers zu berücksichtigen, was sich unmittelbar auf die angebotenen Konditionen auswirken wird (Stichwort: Basel II).

Sie sehen: Es gibt genügend Gründe, sich mit dem Thema Informationssicherheit eingehend zu beschäftigen. Lassen Sie sich – zu Ihrer Sicherheit – die individuelle Rechtslage von einem Experten erklären!

5 So nicht: Schadensfälle als warnendes Beispiel

Szenario 1: „Kein Backup“

Eine Anwaltskanzlei 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
- Rücksicherung prüfen und üben
- Lagerung von Sicherungsbändern außerhalb der eigenen Büroräume, beispielsweise in einem Bankschließfach

Szenario 2: „Befall durch Computer-Viren“

Ein Unternehmen 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. Das Unternehmen verfügt jedoch über keinen automatisierten Update-Mechanismus, mit dessen 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 ins 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 und Testrechner)

Szenario 3: „Ausfall des 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
- Vertretungsregeln einrichten

Szenario 4: „Hackerangriff aus dem Internet“

In einer Kleinstadt betreibt ein Psychologe seine Praxis. Seine Patientenakten 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 vertrauliche Patienteninformationen anonym in einem lokalen Internet-Diskussionsforum der Stadt veröffentlicht wurden. Die Polizei stößt bei ihren Ermittlungen auf den Psychologen und stellt fest: Der Praxis-PC war völlig unzureichend gegen Fremdzugriffe gesichert und wurde vermutlich Ziel eines Hackerangriffs. Der Staatsanwalt erhebt Anklage, da mit vertraulichen Patientendaten fahrlässig umgegangen wurde. Der entstandene Schaden für die betroffenen Patienten ist enorm und kaum quantifizierbar.

Maßnahmen

- Internet-Zugänge sichern
- vertrauliche Daten verschlüsseln

Szenario 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 Vorstrafe. 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

6 Die häufigsten Versäumnisse

Bei einer Analyse der typischen Fehler und Versäumnisse finden sich nur geringe Abhängigkeiten von Unternehmensgröße und Branche. Anhand der dargestellten Liste können Sie überprüfen, welche spezifischen Versäumnisse in Ihrem Umfeld eine Rolle spielen und wie dieser Sachverhalt zu bewerten ist. Das nächste Kapitel greift die geschilderten Defizite nochmals auf und zeigt anhand konkreter Maßnahmen, wie Sie diesen mit angemessenem Aufwand begegnen können.

6.1 Unzureichende Informationssicherheitstrategie

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“ das 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 hinzu kommende andere Aufgaben.

Ein Beispiel in diesem Zusammenhang ist die rasant wachsende Zahl völlig ungesicherter drahtloser Netze, seit entsprechende WLAN-Karten preiswert für jedermann zur Verfügung stehen. Begeisterung für eine neue Technik und die Möglichkeit, auf lästige Verkabelung verzichten zu können, lassen Sicher-

heitsaspekte vergessen. Unzählige Firmen „veröffentlichen“ somit unfreiwillig ihre vertraulichen Daten und bieten teilweise allen Interessierten kostenlose Internetzugänge an.

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.

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 zuviel 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.

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.

6.2 Schlechte Konfiguration von IT-Systemen

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.

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.

6.3 Unsichere Vernetzung und Internet-Anbindung

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.

6.4 Nichtbeachtung von Sicherheitserfordernissen

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.

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. Schulun-

gen 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.

6.5 Schlechte Wartung von IT-Systemen

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.

6.6 Sorgloser Umgang mit Passwörtern und Sicherheitsmechanismen

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.

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.

6.7 Mangelhafter Schutz vor Einbrechern und Elementarschäden

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.

7 Wichtige Sicherheitsmaßnahmen

7.1 Systematisches Herangehen an Informationssicherheit

Angemessene Berücksichtigung von Informationssicherheit:

1. Informationssicherheitsaspekte müssen bei allen Projekten frühzeitig und ausreichend berücksichtigt werden

Eine möglichst große Programmvielfalt mit hoher Funktionalität, bequeme Bedienung, niedrige Anschaffungs- und Betriebskosten sowie Informationssicherheit stehen fast immer in Konkurrenz zueinander. Es empfiehlt sich aber unbedingt, Informationssicherheitsaspekte schon zu Beginn eines Projektes (z. B. bei der Anschaffung neuer Software oder bei der Planung von Geschäftsprozessen) zu berücksichtigen. Gerade neue Techniken dürfen nicht unkritisch eingesetzt werden. Unabdingbare Voraussetzung dafür ist eine klare Unterstützung der Informationssicherheitsziele durch die Leitungsebene! Später auftretende Sicherheitsmängel können unangenehme Konsequenzen zur Folge haben. Werden nachträglich Design- oder Planungsfehler offenkundig, sind Nachbesserungen oftmals unverhältnismäßig teuer oder sogar unmöglich. Der Mut, Abstriche beim Komfort zu machen oder auf eine bestimmte Funktionalität zu verzichten, kann hohe Kosten durch Sicherheitsvorfälle verhindern oder hohe Investitionen in zusätzliche Informationssicherheitsprodukte ersparen.

2. Im Falle mangelnder Ressourcen sollten alternative Lösungsansätze in Erwägung gezogen werden

Oft führen viele Wege zum gleichen Ziel. Kostspielige und langwierige Projekte sind einem höheren Risiko ausgesetzt, mangels Zeit, Geld oder wegen

veränderter Rahmenbedingungen wieder „gekippt“ zu werden. Daher sollten auch alternative Lösungsansätze mit zunächst bescheidenerer Zielsetzung in Erwägung gezogen werden. Mehrere kleine Schritte lassen sich einfacher realisieren als ein großer. Auch das ist ein Sicherheitsaspekt.

Schritt für Schritt zu mehr Informationssicherheit:

3. Die Informationssicherheitsziele müssen festgelegt werden, damit angemessene Maßnahmen definiert werden können

Der erste Schritt bei der Beschäftigung mit Informationssicherheit ist die Bestandsaufnahme:

- Welche Rahmenbedingungen gibt es (Gesetze, Verträge, Kundenanforderungen, Konkurrenzsituation)?
- Welche Rolle spielen IT und Informationssicherheit für das Unternehmen bzw. die Behörde?
- Welche Werte sind zu schützen (Know-how, Betriebsgeheimnisse, personenbezogene Daten, IT-Systeme)? Was sind mögliche Schadensfälle?

Die „Schutzbedarfsfeststellung“ ist notwendiger Bestandteil jeder Sicherheitsanalyse. Sie soll sicherstellen, dass die definierten Schutzziele und die hieraus abgeleiteten Sicherheitsmaßnahmen angemessen sind und den individuellen Gegebenheiten entsprechen. Da sich Rahmenbedingungen im Laufe der Zeit ändern können, sollte regelmäßig überprüft werden, ob die Einstufung des Schutzbedarfs noch der aktuellen Situation entspricht. Bei der Schutzbedarfsfeststellung ist die Orientierung an den drei Grundwerten der Informationssicherheit Vertraulichkeit, Integrität und Verfügbarkeit hilfreich.

4. Zu jedem vorhandenen Sicherheitsziel und jeder zugehörigen Maßnahme sollten geeignete Regelungen getroffen werden

„Informationssicherheit ist ein dauerhafter Prozess." Diese Aussage trifft das Kernproblem sehr gut: Die meisten mit Informationssicherheit assoziierten Aufgaben müssen regelmäßig wiederholt und neu durchlaufen werden. Jede identifizierte Maßnahme sollte dahingehend untersucht werden, ob sie nur ein einziges Mal oder regelmäßig ausgeführt werden muss (Beispiel: regelmäßiges Update des Viren-Schutzprogramms und dessen Viren-Signaturen).

5. Ein Handlungsplan mit klaren Prioritäten der Sicherheitsziele und -maßnahmen sollte erstellt werden

Wer eine Weile über sinnvolle Schritte zur Erhöhung der eigenen Informationssicherheit nachgedacht hat, wird sich bald vor mehr Aufgaben gestellt sehen als er zeitlich und finanziell bewältigen kann. Daher ist eine geeignete Priorisierung identifizierter Sicherheitsziele und -maßnahmen erforderlich. Diese Priorisierung sollte auch unter Abwägung des Kosten-Nutzen-Verhältnisses getroffen werden.

6. Besonders umständliche Sicherheitsanforderungen sollten vermieden werden

Es sollten möglichst nur solche Sicherheitsvorgaben gemacht werden, deren Einhaltung praktikabel ist und die nicht von einem Großteil der Betroffenen als realitätsfremd oder gar schikanös erachtet werden. Zudem versteht sich von selbst, dass zur Umsetzung von Vorgaben und Maßnahmen auch die technische und organisatorische Infrastruktur bereitgestellt werden muss. Anderenfalls besteht die Gefahr, dass die Richtlinien in ihrer Gesamtheit nicht mehr ernst

genommen und zunehmend missachtet werden. Im Zweifelsfall sollten die Anforderungen eher etwas heruntergeschraubt werden und dafür strenger auf deren Einhaltung geachtet werden. Es empfiehlt sich auch, alle Maßnahmen, die besonders tief in die gewohnte Arbeitsweise eingreifen, mit betroffenen Anwendern vorher zu besprechen.

7. Zuständigkeiten müssen festgelegt werden

Für jede identifizierte Aufgabe muss festgelegt werden, wer für die Durchführung verantwortlich ist. Ebenso sollte für alle allgemein formulierte Sicherheitsrichtlinien genau dargelegt werden, für welchen Personenkreis diese verbindlich sind: Betreffen diese nur festangestellte Mitarbeiter, eine bestimmte Abteilung oder alle?

Jeder Verantwortliche braucht einen Stellvertreter. Wichtig ist, dass der Vertreter auch in der Lage ist, seine Aufgaben wahrzunehmen. Wurde er in seine Aufgaben eingewiesen? Sind notwendige Passwörter für den Notfall hinterlegt? Benötigt er Dokumentationen?

8. Bestehende Richtlinien und Zuständigkeiten müssen bekannt gemacht werden

Bei Mitarbeiterbefragungen in Unternehmen fällt beim Thema Informationssicherheit oft auf, dass bestehende Richtlinien nicht oder nur in Teilen bekannt sind. Gelegentlich ist deren Existenz schlicht unbekannt. Deshalb muss sichergestellt sein, dass alle Betroffenen die Unternehmensrichtlinien – in ihrer aktuellen Fassung – kennen. Alle Mitarbeiter sollten ihre internen und externen Ansprechpartner und deren Kompetenzen kennen. Das dient nicht nur dazu, bei Problemen

schneller Hilfe zu erhalten. Es verhindert auch, dass sich Mitarbeiter durch Überredungskunst oder Einschüchterung dazu verleiten lassen, vertrauliche Informationen (Passwörter etc.) an Unberechtigte weiterzugeben.

Hierbei sind auch juristische Aspekte zu berücksichtigen, damit im Falle von Sicherheitsverstößen eine Ahndung nicht bereits daran scheitert, dass sich der Beschuldigte zurecht auf seine Unkenntnis beruft. Im Bedarfsfall ist es vorteilhaft, die Kenntnisnahme wichtiger Richtlinien von den Mitarbeitern schriftlich bestätigen zu lassen.

Kontrolle und Aufrechterhaltung der Informationssicherheit:

9. Die Informationssicherheit sollte regelmäßig überprüft werden

Das Niveau der Informationssicherheit sollte regelmäßig bewertet und kontrolliert werden. Wenn ein ausreichendes Budget zur Verfügung steht, sollte überlegt werden, einmal pro Jahr unabhängige Experten mit der Überprüfung von besonders kritischen Bereichen der IT zu beauftragen. Der Blick muss in die Zukunft gehen: Gibt es neue Sicherheitsstandards oder neue, wichtige Techniken? Haben sich die Erwartungen von Kunden und Geschäftspartnern geändert?

10. Vorhandene Arbeitsabläufe und Sicherheitsrichtlinien sollten regelmäßig hinsichtlich Zweckmäßigkeit und Effizienz überprüft werden

Die ständige Optimierung bestehender Prozesse und Richtlinien ist nicht nur ein Anliegen von Informationssicherheitsverantwortlichen. Im Zusammenhang mit der Formulierung von Sicherheitsrichtlinien gibt es drei Hauptgefahren: Sie sind veraltet, sie sind unvollständig oder sie sind nicht praktikabel.

Gerade für die Akzeptanz von Sicherheitsvorgaben dürfen diese nicht als umständlich oder unsinnig empfunden werden. Unter diesem Gesichtspunkt sollten alle im Zusammenhang mit Informationssicherheitsaufgaben stehenden Arbeitsabläufe kritisch geprüft werden. Nichts ersetzt hierbei die persönliche Bewertung der Arbeitsabläufe durch die ausführenden Personen. Ergibt eine Befragung, dass einzelne Maßnahmen als nicht zweckmäßig eingestuft werden, so sollte gemeinsam nach Ursachen und Verbesserungspotential gesucht werden.

Weiterführende Schritte:

Die Bedeutung der beiden folgenden Maßnahmen hängt sehr stark von der Größe des Unternehmens bzw. der Behörde ab. Je mehr Mitarbeiter betroffen sind, desto notwendiger und sinnvoller ist ihre Umsetzung.

11. Langfristig sollte ein umfassendes Sicherheitsmanagement aufgebaut werden

Ein gutes Sicherheitsniveau lässt sich vor allem in größeren Organisationen nur dann erreichen, wenn Schritt für Schritt die Einrichtung eines umfassenden Sicherheitsmanagements vorgenommen wird. Dies beinhaltet die im vorliegenden Leitfaden aufgezeigten Aspekte, geht über diese jedoch weit hinaus. Umfragen zeigen, dass in Unternehmen, die ein umfassendes Sicherheitsmanagement aufgebaut haben, die Anzahl der Sicherheitsvorfälle deutlich zurückgegangen ist.

12. Alle bestehenden Sicherheitsrichtlinien sollten schriftlich in einem Sicherheitskonzept dokumentiert werden

Es ist empfehlenswert, die Sicherheitsrichtlinien einer Organisation schriftlich zu dokumentieren. Hierfür gibt es inzwischen im Internet und in der Fachliteratur zahlreiche Beispiele, die frei verwendet und an die eigenen Bedürfnisse angepasst werden können. Manchmal erweist es sich als einfacher, eine fremde, gut strukturierte Richtlinie zu übernehmen und anzupassen, statt historisch gewachsene, schlecht strukturierte und teils in sich widersprüchliche eigene Regelwerke zu überarbeiten.

Solche Richtlinien können erfahrungsgemäß am besten ergänzt und aktualisiert werden, wenn sie sorgfältig in mehrere (mindestens drei) Abstraktionsschichten untergliedert werden:

Die oberste und abstrakteste Ausprägung formuliert nur allgemeine Sicherheitsziele und gibt im Wesentlichen eine Zusammenfassung der eigenen Unternehmensphilosophie in Sachen Informationssicherheit. Diese beinhaltet nur wenige Seiten, ist „managementtauglich“ und sollte von der obersten Leitungsebene verabschiedet werden.

Die zweite, darunter liegende Schicht formuliert detaillierte Sicherheitsziele, ausführliche technische Anforderungen und zugehörige Maßnahmen. Dies sollte so detailliert wie möglich erfolgen, ohne jedoch produktspezifische Aspekte oder Eigenschaften zu berühren. Ergeben sich Änderungen in den eingesetzten Produkten und IT-Lösungen, müssen die Sicherheitsziele nicht permanent geändert werden.

Die Interpretation der hier formulierten Vorgaben in konkrete Produkteinstellungen und zu verwendende Mechanismen liefert die dritte Ebene. Sobald sich ein eingesetztes Produkt geändert hat, müssen Anpassungen vorgenommen werden. Leider tritt hierbei oft der Fall auf, dass zuvor formulierte Anforderungen mangels Produktfunktionalität oder fehlender Praktikabilität nicht umgesetzt werden können. Dann müssen entweder die Anforderungen nochmals überdacht werden oder eine andere Lösung eingesetzt werden. Fest steht: Defizite bei der Umsetzung müssen explizit festgehalten werden. Alle Verantwortlichen müssen informiert werden, damit sie das entstandene Risiko bewerten können.

7.2 Sicherheit von IT-Systemen

13. Vorhandene Schutzmechanismen sollten genutzt werden

Viele Programme, die in einem gewöhnlichen Client-Server-basierten Netz zur Bürokommunikation genutzt werden, verfügen inzwischen über eine Vielzahl hervorragender Schutzmechanismen. Fast immer resultieren Schwachstellen aus falscher Konfiguration oder aus Unkenntnis der vorhandenen Möglichkeiten zur Absicherung. Die vom Hersteller implementierten Sicherheitsfunktionen und -mechanismen sollten daher analysiert, verstanden und eingesetzt werden – bevor existierende Sicherheitsanforderungen nicht oder nur auf Umwegen umgesetzt werden. So können auch Sicherheitsanforderungen technisch erzwungen werden, die anderenfalls nur durch Kooperationsbereitschaft der Benutzer möglich sind.

14. Viren-Schutzprogramme müssen flächendeckend eingesetzt werden

Aktuelle Viren-Schutzprogramme sind unverzichtbar. Schadprogramme können über Datenträger oder über Netze (Internet, Intranet) verbreitet werden. Auch für Rechner ohne Internetanschluss sind solche Schutzprogramme Pflicht!

Es empfiehlt sich, E-Mails und jegliche Kommunikation über das Internet zentral auf Viren zu untersuchen. Zusätzlich sollte jeder Computer mit einem lokalen Viren-Schutzprogramm ausgestattet sein, das ständig (resident) im Hintergrund läuft. In der Regel genügt es, nur ausführbare Dateien, Skripte, Makrodateien etc. zu überprüfen. Ein vollständiges Durchsuchen aller Dateien empfiehlt sich trotzdem in regelmäßigen Abständen (z. B. vor einer Tages- oder Monatssicherung). Bei einem festgestellten Befall durch Schadprogramme ist es immer notwendig!

Aktuelle Empfehlungen und ausführliche Hintergrundinformationen finden Sie auf der BSI-Webseite unter dem Stichwort „Schadprogramme“.

Achtung:

Selbst wenn Ihr Viren-Schutzprogramm immer auf dem neuesten Stand ist, bietet es dennoch keinen absoluten Schutz vor Schadprogrammen. Sie müssen davon ausgehen, dass Ihr System neuen Schadprogrammen zumindest solange ausgesetzt ist, bis geeignete Schadprogramm-Signaturen von den Herstellern von Schutzprogrammen zur Verfügung gestellt werden können. Gefährlich sind auch Schadprogramme, die sich über das Internet verbreiten und technisch so konstruiert sind, dass sie über eine nicht geschlossene Sicherheitslücke direkt den Rechner infizieren. Ein berühmtes Beispiel ist der Wurm „Conficker“, der eine Schwachstelle in Windows ausnutzte.

15. Datenzugriffsmöglichkeiten sollten auf das erforderliche Mindestmaß beschränkt werden

Eine der goldenen Regeln der Informationssicherheit ist das „Need-to-Know-Prinzip“: Jeder Benutzer (und auch jeder Administrator) sollte nur auf die Datenbestände zugreifen und die Programme ausführen dürfen, die er für seine tägliche Arbeit auch wirklich benötigt. Dazu gehört auch, dass Informationen einer Abteilung (z. B. Vertrieb, Entwicklung. Personal, Leitung etc.) nicht ohne weiteres von abteilungsfremden Mitarbeitern einsehbar sind, sofern sie diese Informationen nicht für ihre Arbeit benötigen. Anwendungsprogramme – insbesondere Programme für die Systemadministration – sollten ebenfalls nur den Mitarbeitern zur Verfügung stehen, die diese wirklich brauchen.

Die Umsetzung dieses Prinzips ist mit vertretbarem Aufwand möglich: Erforderliche Berechtigungen werden in passenden Berechtigungsprofilen zusammengefasst. Auf deren Grundlage werden dann wahlweise geeignete Benutzergruppen oder Rollen definiert. Die individuellen Rechte eines Systembenutzers lassen sich über dessen Gruppenzugehörigkeiten oder über die Rollen steuern, die der Benutzer annehmen darf. In regelmäßigen Abständen sollte überprüft werden, ob die von einer Person verfügbaren Zugriffsrechte noch deren Tätigkeitsprofil entsprechen oder ob Einschränkungen zweckmäßig wären. Um leichter einen Überblick über Zugriffsberechtigungen zu erhalten, kann das eigene Netz regelmäßig mit passenden Tools untersucht werden. Das deckt Ressourcen auf, die möglicherweise ungewollt für beliebige Dritte zugreifbar sind. Viele geeignete Werkzeuge sind kostenlos verfügbar.

Ebenso muss ein geeigneter Prozess existieren, um Berechtigungen bei Einstellung, Funktionsänderung oder Weggang von Mitarbeitern geeignet einzuräumen bzw. zu widerrufen.

16. Allen Systembenutzern sollten Rollen und Profile zugeordnet werden

Zugriffsberechtigungen dürfen einzelnen Personen oder Personengruppen nicht als Sammelsurium verschiedener Berechtigungen zugeordnet werden. Denn diese Vorgehensweise führt bei der Verwaltung größerer Personenmengen zwangsläufig zu hohem Verwaltungsaufwand, hoher Komplexität und entsprechend hoher Fehleranfälligkeit. Daher bieten fast alle Standardanwendungen die Möglichkeit, passende Berechtigungsprofile zu definieren und mit deren Hilfe geeignete Rollen zu kreieren. Jeder Benutzer (ebenso wie jeder Administrator) erhält eine oder mehrere zulässige Rollen zugeordnet, die er während seiner Arbeit annehmen kann. Dies erlaubt einerseits eine einfachere (und deshalb sicherere) Berechtigungsverwaltung. Andererseits ermöglicht es mehr Flexibilität, da dieselbe Person in Abhängigkeit von ihren jeweiligen Aufgaben oder Tätigkeiten unterschiedliche Rollen annehmen kann.

17. Administratorrechte sollten auf das erforderliche Maß eingeschränkt werden

Viele Systemadministratoren arbeiten unter einer administrativen Rolle, die praktisch keinen Einschränkungen unterliegt und alle Systemprivilegien beinhaltet. Dies ermöglicht zum einen den Missbrauch durch den Administrator selbst, andererseits erhöht sich das Risiko im Falle einer erfolgreichen Übernahme der Administratorrolle durch unbefugte Dritte. Daher sollte nach Möglichkeit zwischen unterschiedlichen administrativen Aufgaben differenziert werden. Je nach administrativer Rolle kann beispielsweise ein Administrator nur Drucker verwalten, ein anderer neue Benutzer anlegen, ein Dritter ist für Backups zuständig. Im Idealfall gibt es sogar einen gesonderten Admi-

nistrator, der die Auswertung von Protokollierungsdaten vornimmt und die Aufgaben der anderen Administratoren überwachen kann.

18. Programmprivilegien sollten begrenzt werden

Ausführbare Programme verfügen – analog zu Anwendern – über bestimmte Zugriffsrechte und Systemprivilegien. In vielen Fällen erbt ein Programm einfach die Berechtigungen des Benutzers, der das Programm gestartet hat. Manchmal genügen diese Berechtigungen nicht. Oder es handelt sich um Serverprozesse, die oft mit hohen Privilegien ausgestattet sein müssen. In solchen Fällen besitzen Programme manchmal so genannte Root-Rechte und können ebenso wie ein „allmächtiger" Systemadministrator alle Systemressourcen nutzen. Werden solche Programme von einem Angreifer zweckentfremdet, so erbt dieser wiederum alle Rechte von dem missbrauchten Programm. Auch Programme dürfen nur mit den Berechtigungen ausgestattet sein, die sie für ein fehlerfreies Funktionieren benötigen.

19. Die Standardeinstellungen gemäß Auslieferungszustand sollten geeignet angepasst werden

Viele Betriebssysteme und Softwareapplikationen sind vom Hersteller derart vorkonfiguriert, dass nach erfolgter Installation ein möglichst reibungsloser und komfortabler Betrieb ermöglicht wird. Die gleiche Aussage gilt für komplette IT-Systeme und TK-Anlagen. Informationssicherheitsaspekte spielen leider häufig keine Rolle bei der Wahl der Standardinstallation durch den Hersteller. Zweifelsohne ist dieser Komfort für all jene Benutzer angenehm, die mit dem betreffenden System nicht oder noch nicht hinreichend vertraut sind. Die vorhandene Produktfunktionalität wird in der Grundkonfiguration möglichst

wenig eingeschränkt und erlaubt die ungestörte Kommunikation mit der eigenen Umgebung. Häufig sind Standardpasswörter und Standard-Benutzer-Accounts eingerichtet. Um Missbrauch zu vermeiden, müssen diese deaktiviert werden. Ein frisch installiertes und noch nicht an die eigenen (Sicherheits-) Bedürfnisse angepasstes System sollte deshalb nie im produktiven Betrieb genutzt werden!

Betriebssysteme besonders exponierter Rechner sowie wichtige Server müssen gehärtet werden. „Härten“ (engl. Hardening) bedeutet in der Informationssicherheit die Entfernung aller Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe durch das Programm nicht zwingend notwendig sind. Oftmals gelingt einem Angreifer der Einbruch in einen Server durch den Missbrauch eines Programms, das auf diesem Server gar nicht installiert sein müsste. Außerdem macht die regelmäßige Pflege und Aktualisierung eines Rechners natürlich mehr Arbeit, wenn dieser mehr Programme enthält. Aus diesen Gründen sollten alle unnötigen Anwendungsprogramme entfernt werden. Dasselbe gilt für einzelne Tools, Treiber, Teilkomponenten etc. In der letzten Konsequenz lassen sich sogar einzelne nicht benötigte „Befehle“ entfernen (d. h. die zugehörigen Betriebssystemroutinen).

20. Handbücher und Produktdokumentationen sollten frühzeitig gelesen werden

Ein erfahrener Administrator wird in vielen Fällen in der Lage sein, ein System auch ohne vorheriges Lesen der Betriebshandbücher zum Laufen zu bringen. Der Erfolg ist jedoch oft trügerisch. So können beispielsweise Warnhinweise des Herstellers übersehen werden, wodurch dann später überraschende Probleme auftreten: Inkompatibilitäten, Systemabstürze oder unentdeckte Schwachstellen. Insofern ist es fahrlässig und unprofessionell, angebotene Hilfsmittel und Infor-

mationen des Herstellers zu ignorieren und dadurch unnötige Risiken zu generieren.

21. Ausführliche Installations- und Systemdokumentationen müssen erstellt und regelmäßig aktualisiert werden

Es ist ratsam, alle Arbeitsschritte vor, während und nach einer Installation schriftlich zu dokumentieren. Dies hilft einem, im Wiederholungsfall schneller ans Ziel zu gelangen und im Problemfall die möglichen Ursachen aufzufinden. Ebenso wichtig ist es, dass die Systemdokumentation auch von Dritten (beispielsweise im Sinne eines „Ersatzadministrators" oder einer Urlaubsvertretung) nachvollzogen und verstanden werden kann. Dadurch werden Ausfallrisiken reduziert, wenn der hauptamtliche Administrator plötzlich nicht mehr zur Verfügung stehen sollte. Im Fall eines erfolgten Hackereinbruchs können zudem unbefugte Veränderungen am System schneller identifiziert werden.

7.3 Vernetzung und Internet-Anbindung

Für die meisten Benutzer mit Internetzugang sind E-Mail und Web-Browser die beiden wichtigsten Internetanwendungen. Kein Wunder, dass hier besonders viele Gefahren lauern. Beim Herunterladen von Dateien können Schadensroutinen eingeschleppt werden, die gegebenenfalls nicht vom Viren-Schutzprogramm erkannt werden. Beim Surfen im Internet können unerwünschte Aktionen ausgelöst werden – vor allem dann, wenn riskante aktive Inhalte (siehe auch Maßnahme 26) zur Ausführung zugelassen werden.

Auf den Internetseiten des BSI finden Sie stets aktuelle Informationen, Studien zu verschiedenen Themen sowie ausführliche Beispiele unter dem Stichwort „Internet-Sicherheit".

22. Zum Schutz von Netzen muss eine Firewall verwendet werden

Kein Computer, der geschäftsmäßig genutzt wird, darf ohne Schutz durch eine geeignete Firewall mit dem Internet verbunden werden!

Auch innerhalb größerer interner Netze existieren normalerweise mehrere Teilnetze mit unterschiedlichen Benutzergruppen und unterschiedlichem Schutzbedarf. Das „eigene" Teilnetz muss daher oftmals gegen benachbarte Netze abgesichert werden, um Bedrohungen vorzubeugen, die qualitativ mit jenen aus dem Internet vergleichbar sind (z. B. Abschottung der Personalabteilung gegen den Rest des Unternehmens). Deshalb sollten auch an diesen Netzübergängen Schutzmechanismen installiert werden.

Was ist eine Firewall?

Eine Firewall ist ein Hard- oder Softwaresystem, das die Verbindung zwischen Netzen kontrolliert und insbesondere Angriffe aus dem Internet auf das eigene Netz (Intranet) abwehrt. Das Spektrum beginnt bei einfachen, z. T. kostenlosen Computerprogrammen („Personal Firewall"), die meist nur den Rechner schützen, auf dem sie installiert sind. In großen Netzen werden dagegen komplexe Firewallsysteme eingesetzt, die aus mehreren Hard- und Softwarekomponenten bestehen.

23. Eine sichere Firewall muss bestimmten Mindestanforderungen genügen

Zum Schutz des internen Netzes gegen benachbarte, weniger vertrauenswürdige Netze muss ein geeigneter Firewalltyp ausgewählt werden. Die Konzeption der Firewallarchitektur und die Installation der Firewall sollte Spezialisten vorbehalten bleiben.

In der Regel empfiehlt sich ein mehrstufiges Firewallkonzept, bei dem zusätzliche Filterelemente (beispielsweise Router) vor- und nachgeschaltet werden. Im Einzelfall, wenn beispielsweise nur ein einzelner Rechner vorhanden ist oder ein komplexes Firewall-System aus anderen Gründen nicht in Frage kommt, bietet die Installation einer so genannten Personal Firewall auf dem zu schützenden Rechner zumindest einen Basisschutz.

Die Filterregeln in Firewalls neigen dazu, im Laufe der Zeit länger und unübersichtlicher zu werden. Firewalladministratoren geben nachträglichen Anforderungen der Anwender oft allzu leicht nach und weichen die Regeln auf. Auch für den Chef sollten keine Ausnahmen gemacht werden! Daher muss regelmäßig geprüft werden, ob die bestehenden Filterregeln noch konsistent sind, ob sie vereinfacht werden können und ob sie noch hinreichend restriktiv sind. Außerdem sollte von Zeit zu Zeit überprüft werden, ob die bestehende Firewallkonzeption noch den bereits eingeführten oder in Kürze zu erwartenden Kommunikationsprotokollen aus Sicht der Informationssicherheit gewachsen ist. Ebenso können neue Techniken zusätzliche Herausforderungen an bestehende Firewallkonzepte stellen. Ausführliche technische Hinweise zu Firewalls (Sicherheitsgateways) finden Sie in den IT-Grundschutz-Katalogen und auf den Internetseiten des BSI.

Weiterführende Informationen zur Firewallarchitektur

Auch eine Firewall kann einem erfolgreichen Angriff zum Opfer fallen. Mehrstufig konzipierte Verteidigungsstrategien sind erforderlich, um auch im Falle der Kompromittierung einer Firewallkomponente noch ein Mindestmaß an Schutz aufrecht erhalten zu können.

All jene Server, die aufgrund ihrer Funktionalität eine direkte Kommunikation mit dem Internet erfordern und von diesem nur noch durch Firewalls oder andere Schutzmechanismen (z. B. Proxies) getrennt sind, werden in einer so genannten „Demilitarisierten Zone" (DMZ) positioniert. Hier spielt die richtige Kaskadierung und Untergliederung der Server in verschiedene Teilbereiche der DMZ (mit jeweils eigenen IP-Adressbereichen) eine wesentliche Rolle für die Gesamtsicherheit.

24. Nach außen angebotene Daten sollten auf das erforderliche Mindestmaß beschränkt werden

Zahlreiche sensitive Informationen werden für berechtigte Benutzer auch über offene Netze bereitgestellt. Vertrauliche Daten sind damit von außen zugreifbar. Ihr Schutz hängt ausschließlich von zuverlässigen Authentisierungs- und Autorisierungsmechanismen ab. Sind diese jedoch falsch konfiguriert oder enthalten sie eine Schwachstelle, so geraten schutzbedürftige Informationen leicht in die falschen Hände. Solche Fehler sind eher die Regel als die Ausnahme. Daher sollte im Einzelfall stets geprüft werden, ob schutzbedürftige Daten überhaupt außerhalb des eigenen, gut geschützten Netzes bereitgestellt und verarbeitet werden müssen.

25. Nach außen angebotene Dienste und Programmfunktionalität sollten auf das erforderliche Mindestmaß beschränkt werden

Alle Funktionen, Serverdienste und offenen Kommunikationsports, die nach außen angeboten werden, erhöhen das Risiko einer möglichen Sicherheitslücke. Deshalb sollte in jedem einzelnen Fall sorgfältig geprüft werden, ob es wirklich erforderlich ist, einen potentiellen „Problemkandidaten“ zu aktivieren und nach außen anzubieten. Das damit verbundene Sicherheitsrisiko kann in Abhängigkeit von der jeweiligen Technik und Implementierung sehr unterschiedlich sein. Bei bestehenden Installationen sollte regelmäßig überprüft werden, ob einzelne Dienste oder Funktionen nicht schlicht aus Versehen oder Bequemlichkeit aktiviert sind, obwohl sie von niemandem benötigt werden. Der durch diese Beschränkungen reduzierte Administrationsaufwand erlaubt darüber hinaus, die gewonnene Zeit gewinnbringend in eine vertiefte Sicherheitsadministration der verbleibenden
Prozesse zu investieren.

26. Beim Umgang mit Web-Browsern ist besondere Vorsicht geboten, riskante Aktionen sollten unterbunden werden

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

Weiterführende Informationen

Welche Skripte, Protokolle oder Zusatzprogramme Sie meiden sollten, kann sich mit neuen technischen Entwicklungen immer wieder ändern. Aktuelle Hinweise über riskante Techniken finden Sie auf den Internetseiten des BSI. Zurzeit gilt ActiveX als besonders gefährlich.

27. Bei E-Mail-Anhängen ist besondere Vorsicht notwendig

Von Schadfunktionen in Dateianhängen empfangener E-Mails geht eine große Gefahr aus, wenn diese ungewollt ausgeführt werden. Kein Anwender darf solche Anhänge arglos ohne Überprüfung öffnen. Die Verwendung eines Viren-Schutzprogramms ist Pflicht! In Zweifelsfällen sollte der Empfänger vor dem Öffnen eines Anhangs beim Absender nachfragen. Besonders tückisch ist, dass bestimmte E-Mail-Programme ohne Rückfrage beim Anwender direkt Anhänge öffnen und ausführen. Das automatische Öffnen von E-Mail-Anhängen kann durch Wahl eines E-Mail-Programms ohne diese Funktionalität, durch geeignete Konfiguration sowie durch Zusatzprogramme technisch verhindert werden.

28. Ein gesonderter Internet-PC zum Surfen ist eine kostengünstige Lösung für die meisten Sicherheitsprobleme bei der Internet-Nutzung

Eine einfache und kostengünstige Möglichkeit zur Reduzierung zahlreicher Risiken, die durch das Surfen im Internet entstehen, ist das Aufstellen eines gesonderten PCs ohne Verbindung zum sonstigen internen Netz. Dieser kann für Recherchen im Internet genutzt werden, ohne auf Funktionalität und Komfort verzichten zu müssen. Heruntergeladene Dateien können hier auf Inhalt und Viren geprüft werden und anschließend per Datenträger oder E-Mail ins interne Netz weitertransportiert werden.

Weiterführende Maßnahmen

Es ist empfehlenswert, Sicherheitsmaßnahmen technisch zu erzwingen, um zu unterbinden, dass Anwender durch Fehlbedienung oder in voller Absicht Sicherheitsmechanismen abschalten oder umgehen.

Die Übertragung gefährlicher Skripte beim Surfen oder potentiell verdächtiger E-Mail-Anhänge kann durch zentrale Einstellungen an der Firewall bzw. Verwendung eines so genannten Proxys unterbunden werden.

7.4 Faktor Mensch: Kenntnis und Beachtung von Sicherheitserfordernissen

29. Sicherheitsrichtlinien und -anforderungen müssen beachtet werden

Sicherheitsrichtlinien helfen nur dann, wenn sie beachtet werden. Und auch die besten Sicherheitsfunktionen und -programme helfen nicht, wenn sie nicht genutzt werden. Die konsequente Beachtung aller nötigen Sicherheitserfordernisse erfordert einen Lernprozess bei jedem Einzelnen und funktioniert erst dann nachhaltig, wenn sie zur Routine wird. Alle Mitarbeiter sollten ein Grundverständnis für Informationssicherheit haben, stets mitdenken und Gefahren einschätzen können. Denn selbst die ausgefeiltesten Sicherheitsrichtlinien können nie alle Sicherheitsaspekte des täglichen Berufslebens lückenlos abdecken.

30. Am Arbeitsplatz sollte Ordnung herrschen und sensitive Informationen nicht frei zugänglich sein

„Ordnung ist das halbe Leben". Über diesen Spruch mag man geteilter Meinung sein. Im Zusammenhang mit Informationssicherheit ist Ordnung zweifelsfrei ein hervorragendes Mittel zur Vermeidung zahlreicher Risiken. Vertrauliche Akten sollten bei Verlassen des Arbeitsplatzes im Schrank oder Safe verschlossen werden. Datenträger wie Bänder, USB-Sticks und CD-ROMs sollten nie offen herumliegen, wenn sich vertrauliches Material darauf befindet. Im Bedarfsfall sollten sie sachgerecht entsorgt werden, um unbefugtes Rekonstruieren zu verhindern. Vertrauliche Ausdrucke gehören in den Datenvernichter und nicht in den normalen Papierkorb. Datenträger wie Festplatten oder CD-ROMs müssen sicher gelöscht oder zerstört werden.

Die Voraussetzung für die Umsetzung dieser Maßnahme ist natürlich, dass Daten und Akten im Rahmen einer Schutzbedarfsfeststellung als sensitiv eingestuft wurden und die Mitarbeiter mit diesen Vorgaben vertraut sind!

31. Bei Wartungs- und Reparaturarbeiten sind besondere Vorsichtsmaßnahmen zu beachten

Besonders wenn Computer bzw. einzelne Festplatten repariert oder weggeworfen werden, können Unbefugte (in der Regel auch noch auf defekten Datenträgern) vertrauliche Daten einsehen oder rekonstruieren. Servicetechniker sollten daher nie allein ohne Aufsicht an IT-Systemen oder TK-Anlagen arbeiten. Wenn Datenträger das Haus verlassen, müssen vorher alle Daten sorgfältig gelöscht werden.

Achtung:

Dateien, die herkömmlich gelöscht werden, sind anschließend mit speziellen Tools noch immer ganz oder in Teilen lesbar. Wichtige Dateien müssen deshalb „sicher gelöscht" werden. Für die gängigen Betriebssysteme gibt es dazu Zusatzprogramme.

32. Mitarbeiter müssen regelmäßig geschult werden

Viele Fehler entstehen aus Unkenntnis oder aus mangelndem Problembewusstsein. Diese Aussage gilt selbstverständlich auch für Informationssicherheit.

Besonders für Administratoren und Informationssicherheitsverantwortliche sind regelmäßige Weiterbildungen unverzichtbar. Auch in Zeiten geringer

Budgets sollte nicht gänzlich auf Schulungsmaßnahmen verzichtet werden, selbst wenn teure Maßnahmen wie der Besuch von Seminaren nicht möglich sind. Der Kauf guter Fachliteratur lohnt sich immer.

Die Schulungen dürfen sich jedoch nicht nur auf technische Themen beschränken. Das schwächste Glied in der Sicherheitskette ist nämlich fast immer der Mitarbeiter. Vor dem US-Kongress hat einmal ein einschlägig bekannter „Experte" ausgesagt, wie es ihm gelungen sei, illegal in die Netze namhafter Großunternehmen einzudringen, um Informationen zu stehlen. Nur selten sei er zu technischen Angriffen übergegangen, meistens sei es ein Leichtes gewesen, Mitarbeiter dazu zu bringen, ihm die Sicherheitscodes zu verraten.

Es sollten daher regelmäßig Maßnahmen ergriffen werden, um bei allen Beteiligten das Sicherheitsbewusstsein (engl. „Security Awareness") zu erhöhen. Dies kann auf vielen Wegen geschehen: interne Vorträge, Schulungen, Rundschreiben, Plakate, anschauliche Beispiele, Veröffentlichung von Sicherheitsvorkommnissen etc.

Sehr wichtig ist auch, Mitarbeiter darüber zu informieren, in welcher Form eine Kommunikation mit Geschäftspartnern möglich ist: Wer sind die Ansprechpartner? Welche Kompetenzen haben sie? Wie findet eine Autorisierung statt? Welche Informationen dürfen an Externe weitergegeben werden?

Auch Kommunikationswege müssen erklärt werden: Welche Daten dürfen über E-Mail ausgetauscht werden? Wie lauten die korrekten Telefonnummern oder Web-Adressen der Geschäftspartner?

Es kommt immer häufiger vor, dass Betrüger mit E-Mails unter falscher Identität arglose Internetnutzer auf gefälschte Web-Seiten (z. B. von Banken) locken und sie zur Eingabe von geheimen Informationen wie PIN, Passwort oder TAN auffordern („Phishing").

33. Nur eine ehrliche Selbsteinschätzung hilft weiter: Manchmal muss Expertenrat eingeholt werden

Nicht für alle Informationssicherheitsaspekte ist das notwendige Fachwissen in der eigenen Organisation vorhanden. In der Praxis zeigt sich: Qualifizierungsmaßnahmen reichen oftmals nicht aus, da die betreffenden Personen mit den fachlichen Anforderungen rein zeitlich überfordert wären. Hier sollten Zuständigkeiten überdacht und neu festgelegt werden. In vielen Fällen ist es klüger, externe Hilfe in Anspruch zu nehmen oder Fachaufgaben an Dienstleister auszulagern. Überschätzung der eigenen Fähigkeiten oder falsche Sparsamkeit können an dieser Stelle fatale Konsequenzen haben.

34. Für alle bestehenden Sicherheitsvorgaben sollten Kontrollmechanismen aufgebaut werden

Die persönliche Einsicht, Akzeptanz und Freiwilligkeit bei allen geforderten Sicherheitsmaßnahmen ist stets das oberste Ziel. Die Einhaltung von Vorgaben scheitert allerdings aus verschiedenen Gründen. Bewusste Missachtung ist eher die Ausnahme. Vielmehr sind Irrtümer und Nachlässigkeiten die häufigsten Ursachen. Deren Vermeidung durch geeignete Maßnahmen liegt im Interesse aller Beteiligten. Aus diesem Grund sollte für jede bestehende Sicherheitsvorgabe zugleich überlegt werden, wie deren Einhaltung kontrolliert werden kann. Die Kontrolle kann beispielsweise durch technische Prüfwerkzeuge erfolgen oder durch Auditoren bzw. Revisoren, durch Auswertung vorhandener Protokollierungsdaten, anhand von Stichproben durch Vorgesetzte etc. Nicht zuletzt sollte die Möglichkeit der Selbstkontrolle angeboten werden, beispielsweise durch Abarbeitung geeigneter Checklisten. Optional können solche ausgefüllten Checklisten dann unterzeichnet und weiter gereicht werden.

35. Konsequenzen für Sicherheitsverstöße sollten festgelegt und veröffentlicht werden

Es sollte allen Beteiligten bewusst sein, dass die (absichtliche oder versehentliche) Missachtung von Sicherheitsvorgaben Konsequenzen nach sich zieht. Um diesen Sachverhalt zu unterstreichen, sollte jeweils klar vermerkt werden (beispielsweise in der organisationseigenen Sicherheitsrichtlinie), mit welchen Folgen im Ernstfall zu rechen ist.

36. Erkannte Sicherheitsverstöße sollten auch tatsächlich sanktioniert werden

Werden Sicherheitsverstöße aufgedeckt, so stellt sich unmittelbar die Frage, wie Vorgesetzte dem Verursacher gegenüber auftreten sollen. Harte Sanktionen bei leichten Verstößen sind sicherlich unangemessen, besonders falls es sich um das erste Mal handeln sollte. Ebenso falsch ist es jedoch, bei schwereren Verstößen oder hartnäckigen Verweigerern auf Sanktionierung zu verzichten. Dies setzt nicht nur beim Verursacher falsche Signale, sondern auch bei allen anderen, die davon erfahren. Daher muss im Bedarfsfall angemessen reagiert werden. Die Tatsache, dass Verstöße geahndet werden, muss allen anderen kommuniziert werden, soweit die jeweilige Situation dies erlaubt.

7.5 Wartung von IT-Systemen: Umgang mit sicherheitsrelevanten Updates

37. Sicherheits-Updates müssen regelmäßig eingespielt werden

Höchste Priorität bei Sicherheits-Updates haben angesichts der sich manchmal rasend schnell ausbreitenden neuen Viren die Virenschutzprogramme. Updates von Web-Browsern, E-Mail-Programmen und Betriebssystemen sollten ebenfalls regelmäßig durchgeführt werden. Aber auch andere Anwendungssoftware und bestimmte Hardware-Komponenten müssen regelmäßig gewartet werden.

38. Zu den Sicherheitseigenschaften verwendeter Software sollten in regelmäßigen Abständen ausführliche Recherchen durchgeführt werden

Um IT-Systeme abzusichern, ist eine regelmäßige Informationsbeschaffung über neu aufgedeckte Schwachstellen und Hilfsmittel zu deren Beseitigung notwendig. Eigene Recherchen werden durch aktuelle Empfehlungen im Internet sowie Fachartikel erleichtert (siehe z. B. in Kapitel „Weiterführende Informationen“ den Abschnitt über CERTs). In „neueren“ Programmversionen (z. B. von Browsern) wurden sicherheitsrelevante Schwachstellen in der Regel vom Hersteller beseitigt. Dies erspart jedoch nicht eine individuelle Betrachtung, da neue Versionen in der Regel auch neue Funktionen und Fehler beinhalten, die andere Gefahren mit sich bringen.

Jeder Systemverantwortliche sollte in regelmäßigen Abständen die Zeit für entsprechende Suchen im Internet und für den Austausch mit Fachkollegen aufbringen. Nach wie vor gibt es zahlreiche frei erhältliche Informationsdienste, deren Angebot jenes kommerzieller Anbieter oft qualitativ übersteigt.

Die Fülle ständig neu veröffentlichter Updates und Sicherheits-Patches macht zudem einen Auswahlprozess erforderlich. In der Regel können nicht alle installiert werden, insbesondere nicht im Rahmen einer Sofortmaßnahme. Daher sollte bereits im Vorfeld Einvernehmen darüber bestehen, nach welchen Auswahlkriterien bestimmt wird, welche Updates mit wieviel Zeitverzug installiert werden können bzw. müssen.

39. Es sollte ein Aktionsplan zum Einspielen erforderlicher Sicherheits-Updates erstellt werden

Selbst wenn der Systemverantwortliche wichtige Sicherheits-Updates nicht einspielt, bleibt deshalb weder automatisch das System stehen noch erfolgt umgehend ein bösartiger Hackerangriff. Das macht deutlicht: Das Einspielen von Updates erfordert sehr viel Disziplin und muss von vornherein als Prozess verankert sein. Gerade bei Viren-Schutzprogrammen sollte das schnellstmögliche Einspielen von Updates zur Routine werden.

40. Softwareänderungen sollten getestet werden

Theoretisch sollte jede Softwareänderung an Produktivsystemen zuvor ausgiebig in einer Testumgebung überprüft werden, damit nach erfolgter Änderung noch alle Systeme reibungslos funktionieren. Auch Updates von Viren-Schutzprogrammen haben bereits Unternehmensnetze lahmgelegt, da unternehmenseigene Software fälschlich als neuer Virus identifiziert und deaktiviert wurde.

Der Test von wichtigen Sicherheits-Updates erfolgt meistens unter besonderem Zeitdruck, da sie möglichst umgehend eingespielt werden müssen. In der

Praxis müssen Administratoren daher besonders sorgfältig zwischen Sicherheitserfordernissen und den verfügbaren Ressourcen abwägen und vernünftige Kompromisse eingehen.

7.6 Verwendung von Sicherheitsmechanismen: Umgang mit Passwörtern und Verschlüsselung

41. Sicherheitsmechanismen sollten sorgfältig ausgesucht werden

Viele Hersteller haben bereits optional Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung in ihre Produkte integriert. Die Konstruktion sicherer Verschlüsselungsverfahren ist eine äußerst anspruchsvolle Wissenschaft. Produktentwickler, die sich nicht viele Jahre intensiv damit befasst haben, können unmöglich sichere Verfahren entwickeln. Trotzdem gibt es noch immer viele Produkthersteller, deren Produkte selbstentwickelte Verschlüsselungsmechanismen anbieten, die in der Regel unsicher sind. Sofern man auf sichere Verfahren angewiesen ist, sollte man kritisch hinterfragen, welche Verfahren der Hersteller einsetzt. Nach Möglichkeit sollte es sich um standardisierte, allgemein anerkannte Algorithmen handeln.

Auch wenn Zweifel an der Qualität einer bestimmten Sicherheitsfunktionalität bestehen, empfiehlt es sich, diese zu nutzen, wenn wirkungsvollere nicht in Frage kommen: Ein schlechter Schutz ist besser als gar keiner. Die vorhandenen Schutzmechanismen sollten dann aber in der höchsten Schutzstufe betrieben werden. In der Praxis lassen viele Anbieter von Online-Dienstleistungen beispielsweise bei SSL-Verschlüsselung immer noch – aus Rücksicht auf ältere Web-Browser – eine unsichere Schlüssellänge von 40 Bit zu.

42. Es müssen gut gewählte (sichere) Passwörter eingesetzt werden

Schlecht gewählte Passwörter stehen auf einer Hitliste besonders häufiger Sicherheitsdefizite ganz weit oben. Besonders Hacker nutzen diesen Umstand aus. Um sich gegen Hackerwerkzeuge zu schützen, die vollautomatisch alle möglichen Zeichenkombinationen ausprobieren oder ganze Wörterbücher einschließlich gängiger Kombinationen aus Worten und angefügten Zahlen testen, muss ein Passwort bestimmten Qualitätsanforderungen genügen. Es sollte länger als sieben Zeichen sein, nicht in Wörterbüchern vorkommen, nicht aus Namen bestehen (insbesondere nicht von „Lieblingshelden" aus Literatur und Film) und auch Sonderzeichen oder Ziffern enthalten. Im letztgenannten Fall sollten allzu gängige Varianten vermieden werden, wie beispielsweise Anhängen einfacher Ziffern am Ende des Passwortes oder eines der üblichen Sonderzeichen „$, !, ?, #" am Anfang oder Ende eines ansonsten simplen Passwortes.

Die sinnvolle Forderung, dass jedes Passwort in regelmäßigen Zeitabständen geändert werden sollte, macht das Dilemma offenkundig: Es ist schwer, sich alle Passwörter zu merken. Bis auf wenige Ausnahmen in Hochsicherheitsbereichen ist es daher legitim, sich seine Passwörter aufzuschreiben und an einem sicheren Ort aufzubewahren (aber natürlich nicht am Monitor oder in der obersten Schreibtischschublade).

Problematisch ist auch die Gewohnheit, einheitliche Passwörter für viele verschiedene Zwecke bzw. Accounts zu verwenden. Gerät das Passwort einer einzelnen Anwendung in falsche Hände, so wird ein geschickter Angreifer dieses Passwort auch bei anderen Anwendungen derselben Person ausprobieren. Die Vor- und Nachteile solcher „Erleichterungen" sollten daher von Fall zu Fall abgewogen werden.

43. Voreingestellte oder leere Passwörter sollten geändert werden

Manche Softwareprodukte verfügen im Auslieferungszustand über Accounts, deren Passwort leer oder immer gleich und allgemein bekannt ist. Viele Hacker wissen das und probieren bei einem Angriffsversuch zunächst aus, ob vergessen wurde, diese Accounts mit neuen Passwörtern zu versehen. Deshalb sollte bei neu installierten Produkten stets in den Handbüchern nachgelesen werden, ob solche Accounts vorhanden sind. Auch Wartungsfirmen, die für einen externen Wartungszugang schlechte oder gar fest eingestellte Passwörter verwenden, sind ein Sicherheitsproblem. In Einzelfällen wurde bekannt, dass Hersteller nicht dokumentierte „Hintertüren" (engl.: Backdoors) in ihren Programmen installiert haben, beispielsweise um im Supportfall auf einfache Weise Administrationszugang zu erlangen. Hersteller bzw. Wartungsfirma sollten daher explizit zusichern können, dass solche Methoden nicht von ihnen angewandt werden.

Die Warnung bezieht sich nicht nur auf IT-Systeme, sondern auch auf moderne TK-Anlagen.

44. Arbeitsplatzrechner sollten bei Verlassen mit Bildschirmschoner und Kennwort gesichert werden

Jedes gängige Betriebssystem bietet die Möglichkeit, Tastatur und Bildschirm nach einer gewissen Wartezeit zu sperren. Die Entsperrung erfolgt dann erst nach Eingabe eines korrekten Passwortes. Bildschirmschoner sollten benutzt werden, wenn unbefugte Dritte bei vorübergehender Abwesenheit des rechtmäßigen Benutzers Zugang zu dessen PC erlangen könnten. Die Aktivierung

der Sperre sollte nicht zu schnell erfolgen (sonst stört sie den Benutzer nach kurzen Bedienpausen). Ein häufig angewandter Zeitpunkt ist fünf Minuten nach der letzten Benutzereingabe. Zusätzlich sollte die Möglichkeit bestehen, im Bedarfsfall die Sperre sofort zu aktivieren (unter Windows findet sich diese Option nach Eingabe von Strg + Alt + Entf).

45. Sensitive Daten und Systeme müssen geschützt werden

Spätestens dann, wenn jemand direkten Zugriff auf eine Festplatte mit sensitiven Daten erhält, sind unverschlüsselte Daten im Allgemeinen frei auslesbar. Die eingebauten Schutzmechanismen des Betriebssystems oder der jeweiligen Applikation bieten nur ungenügenden Schutz vor dem Zugriff durch Experten. Daher sollte der Einsatz einer Verschlüsselungssoftware für vertrauliche Dateien erwogen werden. Notebooks sollten nach Möglichkeit komplett verschlüsselt werden, weil sie besonders einfach gestohlen werden können. Gute Produkte werden für wenig Geld oder sogar kostenlos angeboten. Bei der Produktauswahl sollte darauf geachtet werden, dass die verwendeten Schutzmechanismen als sicher gelten. Eigenentwicklungen von Herstellern sind selten sicher. Informationen über sichere Algorithmen und Schlüssellängen gibt es in Fachbüchern, beim BSI oder auf einschlägigen Sicherheitsseiten im Internet.

7.7 Schutz vor Katastrophen und Elementarschäden

46. Notfallpläne sollten erstellt werden und jedem Mitarbeiter bekannt sein

Wenn das Bürogebäude abbrennt, ein erheblicher Teil der Mitarbeiter durch eine Grippewelle ausfällt, ein Zulieferer oder Dienstleister infolge einer

Insolvenz ausfällt, oder auch nur ein Datenserver streikt, der Drucker nicht mehr druckt, der Strom ausfällt, das Netz von einem Virus befallen wurde oder Daten versehentlich gelöscht wurden, sollte jeder Mitarbeiter wissen, was zu tun ist. Denkbare Szenarien sollten durchgespielt und Gegenmaßnahmen entworfen werden. Für die Wiederherstellung von Systemen und kritischen Geschäftsprozessen sollten Vorkehrungen getroffen werden und auf einer Liste Verantwortliche und Telefonnummern notiert werden. Beispiele: Wie werden Ausweich-Serverräume in Betrieb genommen? Wo können Ersatzarbeitsplätze geschaffen werden? Wie wird der Notbetrieb gestartet? Wie wird ein Backup zurückgespielt? Wie wird der Druckerserver neu gestartet?

47. Alle wichtigen Daten müssen regelmäßig gesichert werden (Backup)

Für die Datensicherung (Backup) stehen zahlreiche Software- und Hardwarelösungen zur Verfügung. Es ist wichtig, dass wirklich alle relevanten Daten vom eingerichteten Backup erfasst werden. Dies stellt insbesondere bei verteilten heterogenen Umgebungen eine besondere Herausforderung dar. Auch mobile Endgeräte wie Notebooks, unvernetzte Einzelplatzrechner und auch PDAs müssen mit einbezogen werden. Es sollte regelmäßig verifiziert werden, dass das Backup auch tatsächlich funktioniert und die Daten wieder erfolgreich eingespielt werden können.

Die Backup-Medien müssen an sicherem Ort, möglichst außerhalb des Unternehmens bzw. des Dienstgebäudes, aufbewahrt werden. Der Aufbewahrungsort sollte zudem hinreichend gegen Elementarschäden wie Feuer, Wasser und Ähnliches geschützt sein.

Alle Anwender müssen wissen, welche Daten wann und wie lange gesichert werden. In der Regel werden nur bestimmte Verzeichnisse und Dateien gesichert, selten geschieht ein komplettes Backup.

48. IT-Systeme müssen angemessen gegen Feuer, Überhitzung, Wasserschäden und Stromausfall geschützt sein

Nicht nur durch Fehlbedienung oder mutwillige Angriffe können einem Informationsverbund Schäden zugefügt werden. Oftmals entstehen gravierende Schäden infolge physischer Einwirkung von Feuer, Wasser oder Strom. Viele Geräte dürfen nur unter bestimmten Klimabedingungen betrieben werden. Daher sollten besonders wichtige IT-Komponenten (Server, Sicherungsmedien, Router etc.) in ausreichend geschützten Räumen untergebracht werden. Zusätzlich sollten sie an eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz angeschlossen sein. Nützliche Tipps zur Umsetzung erteilen beispielsweise die Feuerwehr sowie das BSI (vgl. auch die Hinweise in den IT-Grundschutz-Katalogen hierzu).

49. Maßnahmen zum Zutrittsschutz und zum Schutz vor Einbrechern müssen umgesetzt werden

Auch kleine Unternehmen und Behörden sollten sich Gedanken über den Schutz vor Einbrechern und anderen ungebetenen Gästen machen. Einige einfache Maßnahmen können bereits einen beträchtlichen Sicherheitsgewinn bringen. Es gilt zu überlegen, wo sich Besucher und Betriebsfremde in der Regel aufhalten und auf welche IT-Systeme sie dabei zugreifen könnten. Besonders Server oder Rechner, mit denen auf sensitive Daten zugegriffen wird, sollten so aufgestellt sein, dass Fremde sich nicht unbemerkt an ihnen zu schaffen machen können. Besucher sollten nicht nur aus Höflichkeit aufmerksam betreut werden.

Unter Umständen ist es sinnvoll, bestimmte Büros bei Abwesenheit der Mitarbeiter abzuschließen oder die Fenster (z. B. während der Mittagspause) nicht gekippt zu lassen. Die Tätigkeit von Handwerkern, Servicetechnikern und Reinigungspersonal sollte bewusst geplant und allen Mitarbeitern bekannt gegeben werden. Notebooks sollten nie unbeaufsichtigt im Auto zurückgelassen werden und ggf. auch im Büro nachts oder bei längerer Abwesenheit eingeschlossen werden. Die hier gegebenen Hinweise sind sicher nicht vollständig – sie sollten im Einzellfall überdacht und ergänzt werden.

Tipp:
Lassen Sie den Einbruchsschutz von Experten oder Beratern der Polizei überprüfen, um es Einbrechern nicht unnötig leicht zu machen.

50. Der gesamte Bestand an Hard- und Software sollte in einer Inventarliste erfasst werden

Empfehlenswert ist eine Inventarliste, die regelmäßig aktualisiert wird. In vielen Fällen können diese Informationen aus den Buchhaltungsdaten entnommen werden. Doch selbst dann besteht oft Unklarheit über den letzten Standort oder darüber, ob ein vermisstes Objekt zu einem gegebenen Zeitpunkt schon länger fehlte oder erst vor kurzem abhanden kam. Auch Versicherungen benötigen Inventarlisten mit Wertangaben, damit im Schadensfall ordnungsgemäß reguliert werden kann. Anhand der Inventarliste kann darüber hinaus regelmäßig überprüft werden, dass keine Unterdeckung bezüglich der Versicherungssumme besteht.

8 Der IT-Grundschutz des BSI

In den vorhergehenden Kapiteln wurden verschiedene Aspekte der Informationssicherheit beleuchtet und erläutert, warum sich eine angemessene Sicherheit nicht allein durch technische Mechanismen und Funktionen erreichen lässt. Vielmehr müssen die technischen Sicherheitsfunktionen durch organisatorische, personelle und baulich-physische Maßnahmen flankiert werden. Wer jetzt systematisch und umfassend seine Informationssicherheit verbessern möchte, steht vor der Herausforderung, eine möglichst optimale Sicherheitsfunktionalität bei vertretbaren Kosten zu erreichen. Dazu kommt: Die umgesetzten Lösungen müssen praxistauglich und ausreichend komfortabel sein, damit sie von den Betroffenen auch in der täglichen Arbeit akzeptiert werden. Dieses Kapitel zeigt prinzipielle Vorgehensweisen bei der Erstellung professioneller Sicherheitskonzepte auf und erklärt Ihnen, wie die IT-Grundschutz-Vorgehensweise des BSI dabei helfen kann.

8.1 Der IT-Grundschutz des BSI als Grundlage eines professionellen Sicherheitskonzeptes

Umfassend aber teuer: Die Risikoanalyse

Eine Möglichkeit, ein Sicherheitskonzept zu erstellen, ist die traditionelle Risikoanalyse. Dabei werden individuelle Sicherheitsmaßnahmen für eine vorliegende IT-Landschaft erarbeitet. Die zu schützenden Werte (IT-Systeme, Daten, Know-how etc.) werden ermittelt und genau untersucht, welchen Bedrohungen sie ausgesetzt sind. Anschließend wird analysiert, wie hoch die Wahrscheinlichkeit eines Sicherheitsvorfalls ist, welches Schadensausmaß zu erwarten ist, welche Sicherheitsmaßnahmen ergriffen werden können und welches Restrisiko nach Umsetzung des Sicherheitskonzeptes verbleibt.

Risikoanalysen liefern wertvolle Informationen, sind aber durch die individuelle Betrachtung mit hohem Arbeitsaufwand verbunden: Es werden Experten mit entsprechendem Know-how benötigt. Die relevanten Eingangsgrößen wie Eintrittswahrscheinlichkeit oder Schadenshöhe sind zudem nur sehr schwer und nur höchst ungenau zu ermitteln. Daher ist eine Risikoanalyse mit hohen Kosten verbunden.

Der IT-Grundschutz des BSI als effektive Alternative

Einen alternativen Weg zur Erstellung eines Sicherheitskonzepts beschreitet der IT-Grundschutz des BSI. Die Methode des IT-Grundschutzes basiert auf zwei Werken: Dem BSI-Standard 100-2, der die IT-Grundschutz-Vorgehensweise beschreibt, und den IT-Grundschutz-Katalogen, welche die Baustein-, Gefährdungs- und Maßnahmenkataloge enthalten. Der IT-Grundschutz nutzt die Tatsache, dass ein Großteil der in der Praxis vorhandenen IT-Systeme und Anwendungen von den Anwendern ähnlich und in vergleichbaren Einsatzumgebungen betrieben wird. Server unter Unix, Client-PCs unter Windows oder Datenbankanwendungen sind hier Beispiele. Durch den Einsatz dieser typischen Komponenten ergeben sich immer wieder ähnliche Gefährdungen für den IT-Betrieb. Wenn nicht besondere Sicherheitsanforderungen vorliegen, sind diese Gefährdungen weitgehend unabhängig vom konkreten Nutzungsszenario. Hieraus ergeben sich zwei Ideen für die Herangehensweise:

- Eine umfassende Risikoanalyse ist nicht immer notwendig: Die Gefährdungen für den IT-Betrieb und die Eintrittswahrscheinlichkeit für Schäden, die sich aus diesen Gefährdungen ergeben, lassen sich unter bestimmten Voraussetzungen pauschalisieren.
- Es ist nicht immer notwendig, Sicherheitsmaßnahmen für jeden Anwendungsfall neu zu entwickeln: Es lassen sich Bündel von Standard-Sicherheitsmaßnahmen ableiten, die bei normalen Sicherheitsanforderungen einen angemessenen und ausreichenden Schutz vor diesen Gefährdungen bieten.

Auf Basis dieser Annahmen schlägt IT-Grundschutz eine Vorgehensweise zur Erstellung und Prüfung von Sicherheitskonzepten vor. Im BSI-Standard 100-2 zur IT-Grundschutz-Vorgehensweise ist Schritt für Schritt beschrieben, wie ein Informationssicherheitsmanagement in der Praxis aufgebaut und betrieben werden kann. Die IT-Grundschutz-Vorgehensweise geht sehr ausführlich darauf ein, wie ein Sicherheitskonzept in der Praxis erstellt und wie angemessene Sicherheitsmaßnahmen identifiziert und umgesetzt werden können. IT-Grundschutz interpretiert damit die sehr allgemein gehaltenen Anforderungen der ISO-Standards 27001 und 27002 und hilft Anwendern in der Praxis bei der Umsetzung mit vielen Hinweisen, Hintergrundwissen und Beispielen. Ergänzt wird der IT-Grundschutz durch den BSI-Standard 100-4 Notfallmanagement, der hilfreiche Tipps für den Ausbau eines betrieblichen Kontinuitätsmanagements liefert und die Anforderungen der britischen Standards BS 25999-1:2006 und BS 25999-2:2007 konkretisiert.

Eines der wichtigsten Ziele des IT-Grundschutzes ist es, den Aufwand im Informationssicherheitsprozess zu reduzieren, indem bekannte Vorgehensweisen zur Verbesserung der Informationssicherheit gebündelt und zur Wiederverwendung angeboten werden. So enthalten die IT-Grundschutz-Kataloge Standard-Gefährdungen und -Sicherheitsmaßnahmen für typische IT-Systeme, die nach Bedarf im Unternehmen eingesetzt werden können. Hier finden sich praxiserprobte Standard-Sicherheitsmaßnahmen für typische IT-Systeme, die nach dem aktuellen Stand der Technik umzusetzen sind, um ein angemessenes Sicherheitsniveau zu erreichen. Dabei werden die Bereiche Infrastruktur, Organisation, Personal, Technik und Notfallvorsorge berücksichtigt und so eine ganzheitliche Vorgehensweise unterstützt. Besonderer Wert wird auf die Vermittlung des nötigen technischen Wissens gelegt. Damit eignen sich die IT-Grundschutz-Kataloge auch als Referenz- und Nachschlagewerk.

IT-Grundschutz-Benutzer genießen Vorteile

Mit Hilfe des IT-Grundschutzes lassen sich Sicherheitskonzepte einfach und arbeitsökonomisch realisieren. Das erreichbare Sicherheitsniveau ist für den normalen Schutzbedarf ausreichend und angemessen und kann als Basis für hochschutzbedürftige IT-Systeme und Anwendungen dienen. Erst bei einem signifikant höheren Schutzbedarf oder für IT-Systeme, die nicht in den IT-Grundschutz-Katalogen behandelt werden, muss eine ergänzende Sicherheitsanalyse durchgeführt werden. Zusammenfassend ergeben sich folgende **Vorteile durch eine Orientierung am IT-Grundschutz:**

- Standard-Sicherheitsmaßnahmen werden konkret und detailliert beschrieben.
- Die resultierenden Sicherheitskonzepte sind erweiterbar, aktualisierbar und kompakt, da sie auf eine existierende Referenzquelle verweisen.
- Die umzusetzenden Sicherheitsmaßnahmen sind praxiserprobt und so ausgewählt, dass ihre Umsetzung möglichst kostengünstig möglich ist.
- Selbst wer kein komplettes Sicherheitskonzept erstellen möchte, kann den IT-Grundschutz durch den modularen Aufbau als technischen Leitfaden und Ratgeber für verschiedenste Sicherheitsfragestellungen nutzen und dadurch profitieren.

IT-Grundschutz hat sich in Deutschland als Quasi-Standard durchgesetzt und wird von verschiedenen Institutionen wie z. B. dem Bundesbeauftragten für den Datenschutz als Methode zur Erstellung von Sicherheitskonzepten empfohlen.

GSTOOL, der professionelle Begleiter



Zusätzlich zu den Werken rund um IT-Grundschutz stellt das BSI mit dem GSTOOL (Grundschutz-Tool) eine spezielle Software bereit. Sie unterstützt den Anwender bei der Erstellung, Verwaltung und Fortschreibung von Sicherheitskonzepten auf der Basis von IT-Grundschutz. Nach Erfassung der benötigten Informationen steht dem Anwender ein

umfangreiches Berichtssystem zur Verfügung, das strukturierte Auswertungen über alle erfassten Daten ermöglicht. Eine voll funktionsfähige Testversion ist kostenlos erhältlich. Informationen zum GSTOOL erhalten sie auf der Internetseite www.bsi.bund.de/gstool.

Bezugsquelle

Die IT-Grundschutz-Kataloge werden vom BSI regelmäßig fortgeschrieben. Sowohl die IT-Grundschutz-Vorgehensweise als auch die IT-Grundschutz-Kataloge werden im Internet kostenlos in deutscher und englischer Sprache bereitgestellt. Sie können außerdem zusammen mit anderen BSI-Empfehlungen als DVD bezogen werden. Als gedruckte Version sind sie zusätzlich vom Bundesanzeiger Verlag verlegt worden und über den Buchhandel erhältlich.



Alle Veröffentlichungen rund um den IT-Grundschutz und das darauf basierende ISO 27001-Zertifikat auf der Basis von IT-Grundschutz sind grundsätzlich jedem Interessenten frei und kostenlos zugänglich. Solange die Inhalte nicht verändert oder kommerziell genutzt werden, dürfen sie auch zum Beispiel im Intranet eines Unternehmens verbreitet werden.

Die Mitarbeiter des BSI sind für Fragen und Anregungen über E-Mail (grundschutz@bsi.bund.de) und eine telefonische Hotline 0228 99 9582 - 5369 für Bürger, Unternehmen und Behörden erreichbar.

Alle Informationen rund um IT-Grundschutz stehen im Internet unter

- www.bsi.bund.de/grundschutz oder
- www.it-grundschutz.de

8.2 Struktur der IT-Grundschutz-Kataloge

Die Bausteine der IT-Grundschutz-Kataloge lassen sich entsprechend ihrem jeweiligen Fokus in fünf Bereiche einteilen:

1. Übergreifende Aspekte

Hier finden sich Bausteine wie Personal, Informationssicherheitsmanagement und Datensicherungskonzept.

2. Baulich-technische Gegebenheiten (Infrastruktur)

In diese Gruppe gehören die Bausteine für Gebäude, Serverraum und häuslicher Arbeitsplatz.

3. IT-Systeme

Für typische IT-Systeme wie Unix-System, Tragbarer PC und TK-Anlage gibt es entsprechende Bausteine in den IT-Grundschutz-Katalogen.

4. Vernetzungsaspekte der IT-Systeme

Vernetzungsaspekte wie Heterogene Netze oder Netz- und Systemmanagement werden hier behandelt.

5. Anwendungen

Für einige Anwendungen wie E-Mail, Webserver und Datenbanken sind hier spezielle Bausteine zu finden.

Jeder Baustein der IT-Grundschutz-Kataloge enthält eine kurze Beschreibung der Thematik und eine Liste mit Verweisen auf die jeweils relevanten Gefährdungen und auf die jeweils relevanten Standard-Sicherheitsmaßnahmen.

8.3 Durchführung einer IT-Grundschutzanalyse

Die IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2) beschreibt eine Methodik, wie Sicherheitskonzepte auf der Basis von Standard-Sicherheitsmaßnahmen für IT-Lösungen erstellt oder geprüft werden können. Auch zur Realisierung von Sicherheitsmaßnahmen und zur Aufrechterhaltung der Informationssicherheit im laufenden Betrieb werden umfangreiche Hinweise gegeben. Die Standard-Sicherheitsmaßnahmen der IT-Grundschutz-Kataloge bilden eine Basis -Sicherheit, die für normale Sicherheitsanforderungen angemessen und ausreichend ist. Aber auch für den höheren Schutzbedarf enthalten die IT-Grundschutz-Kataloge Empfehlungen. Unter Umständen müssen diese durch zusätzliche, weitergehende Sicherheitsmaßnahmen ergänzt werden. Ergänzende Sicherheitsmaßnahmen können beispielsweise auch dann erforderlich sein, wenn spezielle Komponenten verwendet werden, die in den IT-Grundschutz-Katalogen nicht behandelt werden, die aber eine wichtige Rolle für die Gesamtsicherheit des Informationsverbundes spielen.

Die wesentlichen Schritte der IT-Grundschutz-Methodik im Überblick:

1. IT-Strukturanalyse

Dieser Arbeitsschritt dient dazu, Informationen über die Informationstechnik des betrachteten Bereichs („Informationsverbund“) zusammenzutragen. Wichtig ist es, Anwendungen, IT-Systeme und IT-Räume zu erfassen und Abhängigkeiten aufzuzeigen. Dabei sollte man sich auf die wichtigsten Komponenten beschränken und die Ergebnisse übersichtlich darstellen.

2. Schutzbedarfsfeststellung

Das Ziel der Schutzbedarfsfeststellung ist es zu ermitteln, mit welchem Aufwand Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume vor Beeinträchtigungen der Vertraulichkeit, Integrität und Verfügbarkeit geschützt werden müssen. Nur so kann es gelingen, ein ausreichendes Schutzniveau bei möglichst geringen Kosten zu erreichen.

3. Modellierung

Die Modellierung ist der zentrale Arbeitsschritt bei der Anwendung von IT-Grundschutz. Die Bausteine der IT-Grundschutz-Kataloge werden bei der Modellierung den existierenden Prozessen und Komponenten („Zielobjekten") zugeordnet. Die IT-Grundschutz-Kataloge enthalten eine genaue Beschreibung, wie mit den vorhandenen Bausteinen ein realer Informationsverbund möglichst genau nachgebildet werden kann.

So wird beispielsweise der Baustein „Sicherheitsmanagement" einmal auf den gesamten Informationsverbund angewendet, der Baustein „Faxgerät" auf jedes Faxgerät. Jeder Baustein enthält eine Beschreibung der relevanten Gefährdungen und Sicherheitsmaßnahmen für das entsprechende Zielobjekt. Das Ergebnis der Modellierung ist eine umfangreiche Liste mit Sicherheitsmaßnahmen.

Mit Hilfe dieses Maßnahmenkatalogs kann im nächsten Schritt geprüft werden, welche Sicherheitsmaßnahmen in der Realität bereits umgesetzt sind oder wo noch Schwachstellen bestehen (Soll-Ist-Vergleich). Bei der Planung eines Informationsverbundes kann der Maßnahmenkatalog als Grundlage eines Pflichtenheftes benutzt werden.

4. Basis-Sicherheitscheck

Falls die IT-Grundschutz-Vorgehensweise auf einen existierenden Informationsverbund angewandt wird, muss geprüft werden, welche Standard-Sicherheitsmaßnahmen, die in der Modellierung als erforderlich identifiziert wurden, bereits umgesetzt sind und wo noch Defizite bestehen. Hierzu werden Interviews mit den Verantwortlichen und stichprobenartige Kontrollen durchgeführt. Dieser Arbeitsschritt wird als Basis-Sicherheitscheck bezeichnet.

9 Standards und Zertifizierung der eigenen Informationssicherheit

Möchte eine Organisation den Nachweis erbringen, dass sie definierte Sicherheitsstandards erfüllt, bietet sich eine Zertifizierung an. Der folgende Überblick zeigt die Ausrichtungen der verschiedenen Verfahren auf. Dabei werden auch bekannte Standards erwähnt, nach denen keine offizielle Zertifizierung möglich ist, da es hier immer wieder zu Missverständnissen kommt.

Zertifizierung nach Common Criteria (ISO/IEC 15408)

Die Common Criteria (CC) sind ein international anerkannter Standard zur Zertifizierung von Hardware- oder Software-Produkten. Ziel ist der Nachweis, dass die Sicherheitsanforderungen eines IT-Produktes oder IT-Systems vollständig und korrekt realisiert worden sind. Insbesondere wird nachgewiesen, dass die Sicherheitsfunktionen nicht durch Schwachstellen umgehbar sind. Der Aufwand der Prüfung – und daraus resultierend das Vertrauen in die Wirksamkeit der Sicherheitsleistungen des zertifizierten Produktes – hängt von der Prüftiefe ab. Die CC unterscheiden sieben Stufen (EAL-Stufen 1 bis 7), die sich am angenommenen Täterprofil, der Motivation des Täters, dessen Know-how und dem erforderlichen Zeit- und Ausstattungsaufwand zur Durchführung eines Angriffes orientieren.

COBIT

COBIT (Control Objectives for Information and related Technology) beschreibt eine Methode zur Kontrolle von Risiken, die sich durch den IT-Einsatz zur Unterstützung geschäftsrelevanter Abläufe ergeben.

Die COBIT-Dokumente werden herausgegeben vom „IT Governance Institute“ (ITGI) der „Information Systems Audit and Control Association“ (ISACA). Bei der Entwicklung von COBIT orientierten sich die Autoren an bestehenden Stan-

dards zum Thema Informationssicherheitsmanagement wie NIST Security Handbook und ISO 27002 (früher ISO 17799).

Nach COBIT ist keine Zertifizierung im engeren Sinne möglich, die Kriterien werden von vielen Wirtschaftsprüfern im Rahmen der Jahresabschlussprüfung zur Prüfung des IT-Kontrollumfeldes eingesetzt.

ITIL

Die IT Infrastructure Library (ITIL) ist eine Sammlung mehrerer Bücher zum Thema IT-Service-Management. Sie wurde vom United Kingdom's Office Of Government Commerce (OGC) gemäß ISO 9001 unter Mitarbeit vieler verschiedener Unternehmen und externer Experten entwickelt.

ITIL befasst sich mit dem Management von IT Services aus Sicht des IT-Dienstleisters. Der IT-Dienstleister kann dabei sowohl eine interne IT-Abteilung als auch ein externer Service-Provider sein. Übergreifendes Ziel ist die Optimierung bzw. Verbesserung der Qualität von IT-Services und der Kosteneffizienz. Der ITIL-Ansatz ist durchgängig prozessbasiert und orientiert sich an „best practices".

ISO 27000

Aufgrund der Komplexität von Informationstechnik und der Nachfrage nach Zertifizierung sind in den letzten Jahren zahlreiche Anleitungen, Standards und nationale Normen zur Informationssicherheit entstanden.

Der internationale Standard ISO 27000 gibt einen allgemeinen Überblick über Managementsysteme für Informationssicherheit (ISMS) und über die Zusammenhänge der verschiedenen Standards der ISO 2700x-Familie. Hier finden sich außerdem die grundlegenden Prinzipien, Konzepte, Begriffe und Definitionen für solche Managementsysteme.

ISO 27001

Der ISO-Standard 27001 „Information technology – Security techniques – Information security management systems requirements specification" ist der erste internationale Standard zum Informationssicherheitsmanagement, der auch eine Zertifizierung ermöglicht. ISO 27001 gibt auf ca. 10 Seiten allgemeine Empfehlungen. In einem normativen Anhang wird auf die Controls aus ISO 27002 verwiesen. Die Leser erhalten aber keine Hilfe für die praktische Umsetzung.

ISO 27002 (vorher ISO 17799)

Das Ziel von ISO 27002 „Information technology - Code of practice for information security management" ist es, ein Rahmenwerk für das Informationssicherheitsmanagement zu definieren. ISO 27002 befasst sich daher hauptsächlich mit den erforderlichen Schritten, um ein funktionierendes Informationssicherheitsmanagement aufzubauen und in der Organisation zu verankern. Die erforderlichen Informationssicherheitsmaßnahmen werden kurz auf den ca. 100 Seiten des ISO-Standards angerissen. Die Empfehlungen sind auf Management-Ebene und enthalten kaum konkrete technische Hinweise. Ihre Umsetzung ist eine von vielen Möglichkeiten, die Anforderungen des ISO-Standards 27001 zu erfüllen.

ISO 27005

Dieser ISO-Standard „Information security risk management" enthält Rahmenempfehlungen zum Risikomanagement für Informationssicherheit. Unter anderem unterstützt er bei der Umsetzung der Anforderungen aus ISO 27001. Hierbei wird allerdings keine spezifische Methode für das Risikomanagement vorgegeben. ISO 27005 löst den bisherigen Standard ISO 13335-2 ab. Dieser Standard, ISO 13335 „Management of information and communications technology security, Part 2: Techniques for information security risk management", gab Anleitungen zum Management von Informationssicherheit.

Weitere Standards der ISO 2700x Reihe

Die Normenreihe ISO 2700x wird voraussichtlich langfristig aus den ISO-Standards 27000-27019 und 27030-27044 bestehen. Alle Standards dieser Reihe behandeln verschiedene Aspekte des Sicherheitsmanagements und beziehen sich auf die Anforderungen der ISO 27001. Die weiteren Standards sollen zum besseren Verständnis und zur praktischen Anwendbarkeit der ISO 27001 beitragen. Diese beschäftigen sich beispielsweise mit der praktischen Umsetzung der ISO 27001, also der Messbarkeit von Risiken oder mit Methoden zum Risikomanagement.

Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz

Das Bundesamt für Sicherheit in der Informationstechnik bietet seit Januar 2006 die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz an. Hierüber kann nachgewiesen werden, dass in einem Informationsverbund die wesentlichen Anforderungen nach ISO 27001 unter Anwendung der IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2) und gegebenenfalls einer ergänzenden Risikoanalyse (BSI-Standard 100-3) umgesetzt wurden. Das BSI bietet weiterhin zwei Vorstufen vor dem Zertifikat an, diese dienen als Migrationspfad zur eigentlichen Zertifizierung: das „Auditor-Testat Einstiegsstufe“ und das „Audior-Testat Aufbaustufe“. Hierbei unterscheiden sich die einzelnen Stufen durch die Anzahl der umzusetzenden Maßnahmen. Jeder Maßnahme eines IT-Grundschutz-Bausteines ist eine dieser drei Stufen zugeordnet, so dass transparent ist, welche konkreten Sicherheitsempfehlungen aus den IT-Grundschutz-Katalogen umzusetzen sind.

Einen Antrag auf ein Auditor-Testat kann die Institution nach Umsetzung aller für die jeweilige Stufe relevanten Maßnahmen und einer Überprüfung der Umsetzung von einem beim BSI lizenzierten Auditor stellen. Ein Auditor-Testat hat eine Gültigkeit von zwei Jahren und kann nicht verlängert werden, da es als Vorstufe für die Zertifizierung dient.

Nach Umsetzung aller für die Zertifizierung relevanten Maßnahmen kann die Institution einen beim BSI lizenzierten ISO 27001-Auditor beauftragen, den Informationsverbund gemäß dem Prüfschema des BSI zu überprüfen. Die Ergebnisse dieser unabhängigen Prüfung werden in einem Auditreport festgehalten. Ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz kann zusammen mit der Einreichung des Auditreports beim BSI beantragt werden. Nach Prüfung des Reportes durch Experten des BSI erteilt die Zertifizierungsstelle das Zertifikat, das ebenso wie die Auditor-Testate vom BSI veröffentlicht wird. Alle zertifizierungsrelevanten Informationen wie das Zertifizierungsschema und die Namen der lizenzierten Auditoren sind öffentlich verfügbar und können unter www.bsi.bund.de/grundschutz/zert eingesehen werden.

10 Anhang

10.1 Checklisten

Die Fragen in diesem Kapitel fassen den Inhalt der 50 Sicherheitsmaßnahmen kurz zusammen und ermöglichen einen schnellen Überblick über die Schwachstellen im eigenen Unternehmen oder in der Behörde.

Informationssicherheitsmanagement

- ☐ Hat die Unternehmens- bzw. Behördenleitung die Informationssicherheitsziele festgelegt und sich zu ihrer Verantwortung für die Informationssicherheit bekannt? Sind alle gesetzlichen oder vertragsrechtlichen Gesichtspunkte berücksichtigt worden?
- ☐ Gibt es einen IT-Sicherheitsbeauftragten?
- ☐ Werden Sicherheitserfordernisse bei allen Projekten frühzeitig berücksichtigt (z. B. bei Planung eines neuen Netzes, Neuanschaffungen von IT-Systemen und Anwendungen, Outsourcing- und Dienstleistungsverträgen)?
- ☐ Besteht ein Überblick über die wichtigsten Anwendungen und IT-Systeme und deren Schutzbedarf?
- ☐ Gibt es einen Handlungsplan, der Sicherheitsziele priorisiert und die Umsetzung der beschlossenen Sicherheitsmaßnahmen regelt?
- ☐ Ist bei allen Sicherheitsmaßnahmen festgelegt, ob sie einmalig oder in regelmäßigen Intervallen ausgeführt werden müssen (z. B. Update des Viren-Schutzprogramms)?
- ☐ Sind für alle Sicherheitsmaßnahmen Zuständigkeiten und Verantwortlichkeiten festgelegt?
- ☐ Gibt es geeignete Vertretungsregelungen für Verantwortliche und sind die Vertreter mit ihren Aufgaben vertraut? Sind die wichtigsten Passwörter für Notfälle sicher hinterlegt?

(Fortsetzung) IT-Sicherheitsmanagement

- ☐ Sind die bestehenden Richtlinien und Zuständigkeiten allen Zielpersonen bekannt?
- ☐ Gibt es Checklisten, was beim Eintritt neuer Mitarbeiter und beim Austritt von Mitarbeitern zu beachten ist (Berechtigungen, Schlüssel, Unterweisung etc.)?
- ☐ Wird die Wirksamkeit von Sicherheitsmaßnahmen regelmäßig überprüft?
- ☐ Gibt es ein dokumentiertes Sicherheitskonzept?

Sicherheit von IT-Systemen

- ☐ Werden vorhandene Schutzmechanismen in Anwendungen und Programmen genutzt?
- ☐ Werden flächendeckend Viren-Schutzprogramme eingesetzt?
- ☐ Sind allen Systembenutzern Rollen und Profile zugeordnet worden?
- ☐ Ist geregelt, auf welche Datenbestände jeder Mitarbeiter zugreifen darf? Gibt es sinnvolle Beschränkungen?
- ☐ Gibt es verschiedene Rollen und Profile für Administratoren oder darf jeder Administrator alles?
- ☐ 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?

(Fortsetzung) Sicherheit von IT-Systemen

- ☐ Werden nicht benötigte sicherheitsrelevante Programme und Funktionen konsequent deinstalliert bzw. deaktiviert?
- ☐ Werden Handbücher und Produktdokumentationen frühzeitig gelesen?
- ☐ Werden ausführliche Installations- und Systemdokumentationen erstellt und regelmäßig aktualisiert?

Vernetzung und Internet-Anbindung

- ☐ Gibt es eine Firewall?
- ☐ Werden Konfiguration und Funktionsfähigkeit der Firewall regelmäßig kritisch überprüft und kontrolliert?
- ☐ Gibt es ein Konzept, welche Daten nach außen angeboten werden müssen?
- ☐ Ist festgelegt, wie mit gefährlichen Zusatzprogrammen (PlugIns) und aktiven Inhalten umgegangen wird?
- ☐ Sind alle unnötigen Dienste und Programmfunktionen deaktiviert?
- ☐ Sind Web-Browser und E-Mail-Programm sicher konfiguriert?
- ☐ Sind die Mitarbeiter ausreichend geschult?

Beachtung von Sicherheitserfordernissen

- ☐ Werden vertrauliche Informationen und Datenträger sorgfältig aufbewahrt?
- ☐ Werden vertrauliche Informationen vor Wartungs- oder Reparaturarbeiten von Datenträgern oder IT-Systemen gelöscht?
- ☐ Werden Mitarbeiter regelmäßig in sicherheitsrelevanten Themen geschult?
- ☐ Gibt es Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter?
- ☐ Werden bestehende Sicherheitsvorgaben kontrolliert und Verstöße geahndet?

Wartung von IT-Systemen: Umgang mit Updates

- ☐ Werden Sicherheits-Updates regelmäßig eingespielt?
- ☐ Gibt es einen Verantwortlichen, der sich regelmäßig über Sicherheitseigenschaften der verwendeten Software und relevanter Sicherheits-Updates informiert?
- ☐ Gibt es ein Testkonzept für Softwareänderungen?

Passwörter und Verschlüsselung

- ☐ Bieten Programme und Anwendungen Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung? Sind die Sicherheitsmechanismen aktiviert?
- ☐ Wurden voreingestellte oder leere Passwörter geändert?
- ☐ Sind alle Mitarbeiter in der Wahl sicherer Passwörter geschult?
- ☐ Werden Arbeitsplatzrechner bei Verlassen mit Bildschirmschoner und Kennwort gesichert?
- ☐ Werden vertrauliche Daten und besonders gefährdete Systeme wie Notebooks ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt?

Notfallvorsorge

- ☐ Gibt es einen Notfallplan mit Anweisungen und Kontaktadressen?
- ☐ Werden alle notwendigen Notfallsituationen behandelt?
- ☐ Kennt jeder Mitarbeiter den Notfallplan und ist dieser gut zugänglich?

Datensicherung

- ☐ Gibt es eine Backupstrategie?
- ☐ Ist festgelegt, welche Daten wie lange gesichert werden?
- ☐ Bezieht die Sicherung auch tragbare Computer und nicht vernetzte Systeme mit ein?
- ☐ Werden die Sicherungsbänder regelmäßig kontrolliert?
- ☐ Sind die Sicherungs- und Rücksicherungsverfahren dokumentiert?

Infrastruktursicherheit

- ☐ Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall?
- ☐ Ist der Zutritt zu wichtigen IT-Systemen und Räumen geregelt? Müssen Besucher, Handwerker, Servicekräfte etc. begleitet bzw. beaufsichtigt werden?
- ☐ Besteht ein ausreichender Schutz vor Einbrechern?
- ☐ Ist der Bestand an Hard- und Software in einer Inventarliste erfasst?

10.2 Beispiel: Was im Sicherheitskonzept für eine TK-Anlage geregelt sein sollte

- Ein TK-Verantwortlicher und ein Vertreter sollten benannt werden.
- Nicht benötigte Leistungsmerkmale sollten erkannt und gesperrt werden.
- Werkseitig eingestellte Passwörter sollten geändert werden.
- Passwörter, die zur Konfiguration und Wartung benötigt werden, sollten für Notfälle sicher hinterlegt werden.
- Richtlinien zu Service-Rufnummern und Auslandsverbindungen sollten erlassen werden (z. B. Sperrung von 0190- und 0900-Rufnummern).
- Protokolldateien sollten regelmäßig ausgewertet werden, um Auffälligkeiten festzustellen. Dies sind z. B. unzulässige Einwahlen über Wartungszugänge, Verbindungen nach Feierabend, wiederholte Anrufe zum systematischen Durchprobieren von PINs, Aktivierung der Raumüberwachung etc.
- Die Konfiguration der TK-Anlage sollte regelmäßig gesichert werden.
- Eine technische Dokumentation sowie ein kurzer Leitfaden für die tägliche Benutzung sollten erstellt bzw. vom Hersteller besorgt werden.
- Die TK-Anlage sollte im Notfallhandbuch aufgeführt werden (z. B. Möglichkeiten der Fehlersuche, Telefonnummer eines Servicetechnikers etc.).
- Mitarbeiter sollten über Gefahren aufgeklärt werden (z. B. über die Möglichkeit, die Raumüberwachungsfunktion bei Mobiltelefonen, Festnetzgeräten und Anrufbeantwortern zum Abhören geheimer Besprechungen zu missbrauchen).
- Nach Möglichkeit sollte die Sicherheit der TK-Anlage regelmäßig von externen Experten geprüft werden.

10.3 Weiterführende Informationen

Das im Internet frei verfügbare Angebot an verschiedensten, oft sehr guten Informationsquellen zu Fragen der Informationssicherheit ist schier unerschöpflich. Verschaffen Sie sich mit Suchmaschinen einen eigenen Eindruck! Sie werden feststellen, dass Sie das Rad nicht neu erfinden müssen, sondern dass es bereits viele Dokumente gibt, die für den eigenen Anwendungszweck eine gute Grundlage bieten. Im Folgenden finden Sie einige interessante Adressen, unter denen Sie auch Informationen zu den dargestellten Zertifizierungen und Standards nachlesen können.

Allgemeine Informationen zur Informationssicherheit

- **www.bsi.bund.de**
  Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** bietet auf seinen Internetseiten aktuelle Informationen und Ratschläge zu Fragen der Informationssicherheit, technische Analysen und Studien zum kostenlosen Download. Außerdem finden sich dort Hinweise zur Bestellung der DVD-Version der IT-Grundschutz-Materialien sowie zahlreiche nützliche Links zu interessanten Internetseiten.
- **www.bsi-fuer-buerger.de**
  Für Einsteiger in das Thema Informationssicherheit bietet das BSI eine eigene Informationsseite an. Diese vermittelt auf unterhaltsame Weise die wichtigsten Grundkenntnisse rund um das Thema Informationssicherheit ohne auf technische Details einzugehen.
- **www.a-sit.at**
  Das Zentrum für sichere Informationstechnologie – Austria (A-SIT) in Österreich wurde als gemeinnütziger Verein vom Bundesministerium für Finanzen, der Österreichischen Nationalbank und der Technischen Universität Graz gegründet. Auf seinen Internetseiten finden Sie viele interessante Themen rund um Informationssicherheit, u. a. das Österreichische Informationssicherheitshandbuch (ITSHB).

- **www.isb.admin.ch**
  In der Schweiz beschäftigt sich das „Informatikstrategieorgan Bund“ (ISB) mit Informationssicherheit und unterstützt die Bundesverwaltung. Viele interessante Maßnahmenkataloge und Leitlinien (in Deutsch) sind frei zugänglich.
- **www.bitkom.org**
  Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien hat verschiedene Publikationen zu Informationssicherheitsthemen veröffentlicht, darunter Leitfäden zu folgenden Themen: E-Mail- und Internetnutzung im Unternehmen, Sicherheit für Systeme und Netze in Unternehmen, Kompass der Informationssicherheitsstandards, Matrix der Haftungsrisiken.
- **www.bankenverband.de**
  Der Bundesverband deutscher Banken veröffentlicht regelmäßig Hinweise zum sicheren Online-Banking (siehe z. B. unter „Broschüren“).

Informationen zum IT-Grundschutz des BSI

- **www.bsi.bund.de/grundschutz**
  Hier finden Sie alle Informationen zur IT-Grundschutz-Vorgehensweise, den IT-Grundschutz-Katalogen, zum GSTOOL und zur Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz.

CERT (Computer Emergency Response Teams)

Hinweise zu Computer-Viren und neu bekannt gewordenen Sicherheitsproblemen in Soft- und Hardware werden auf den Informationsseiten so genannter CERTs (Computer Emergency Response Teams) veröffentlicht. CERTs beantworten präventiv Anfragen zu Themen der Informationssicherheit, sie warnen vor Schwachstellen und informieren über sicherheitsrelevante Ereignisse. Aufgrund dieser Informationen können zeitnahe konkrete Schritte seitens der verantwortlichen Systembetreuer oder Endnutzer zur Gefahrenabwehr ergriffen werden. So werden schon im Vorfeld mögliche Schäden vermieden. Treten Sicherheitsvorfäl-

le auf, so bieten die CERTs je nach individueller Ausprägung auch reaktive Dienstleistungen an, um die Auswirkungen von Vorfällen zu mildern, deren Beseitigung zu unterstützen oder um sie unmittelbar aufzuklären und zu bereinigen.

- **www.bsi.bund.de/CERT-Bund**
  Das BSI betreibt das CERT-Bund und bietet u. a. im Rahmen des Warn- und Informationsdienstes (WID) aktuelle E-Mail-Newsletter zu verschiedenen Sicherheitsthemen an. Die reaktiven Dienstleistungen
  von CERT-Bund stehen insbesondere der primären Zielgruppe in der Bunderverwaltung zur Verfügung.
- **www.buerger-cert.de**
  Das Bürger-CERT informiert und warnt Bürger und Unternehmen schnell und kompetent vor Viren, Würmern und Sicherheitslücken in Computeranwendungen – kostenfrei und absolut neutral. Experten analysieren rund um die Uhr die Sicherheitslage im Internet und verschicken bei Handlungsbedarf Warnmeldungen und Sicherheitshinweise per E-Mail. Zusätzlich besteht die Möglichkeit, neben den Sicherheits- und Virenwarnungen, dort auch den Newsletter „Sicher informiert“ des BSI zu abonnieren.
- **www.CERT-Verbund.de**
  Der CERT-Verbund ist ein Zusammenschluss deutscher CERTs, die
  sich auf der Basis eines „Code of Conduct“ zu einer verbindlichen Zusammenarbeit verpflichtet haben. Der CERT-Verbund ist offen für alle interessierten deutschen CERTs.
- **www.cert.dfn.de**
  Das Deutsche Forschungsnetz betreibt traditionell das CERT für den Bereich der Wissenschaft und der Forschung und bietet öffentlich zugängliche Mailing-Listen an.
- **www.cert.org**
  Hier findet sich ein seit vielen Jahren betriebenes und angesehenes CERT, das zudem das erste seiner Art war. Die Seiten sind in englischer Sprache.

Standards und Zertifizierung

- **www.bitkom.org**
  Im Bereich Publikationen hat die BITKOM im Leitfaden „Kompass IT-Sicherheitsstandards“ die wichtigsten Standards rund um Informationssicherheit zusammengetragen und gegenübergestellt.
- **www.isaca.org**
  Auf der Seite der „Information Systems Audit and Control Association & Foundation“ ist COBIT erhältlich.
- **www.iso.org**
  Auf der Seite der ISO werden die ISO-Standards zum Kauf angeboten. Die Preise sind im Allgemeinen leider nicht niedrig.
- **www.commoncriteria.org**
  Die ebenfalls erwähnten Common Criteria können von der zugehörigen Homepage frei heruntergeladen werden. Dort finden sich zugleich zahlreiche Zusatzinformationen für alle, die nähere Einzelheiten zu diesem Thema erfahren möchten.
- **www.isfsecuritystandard.com**
  Im Information Security Forum (ISF) haben sich einige große Unternehmen zusammengeschlossen, um gemeinsam an Themen der Informationssicherheit zu arbeiten. Öffentlich verfügbar (in Englisch) ist ein sehr guter Leitfaden zur Erstellung eines Sicherheitskonzeptes – „The Standard of Good Practice“.

Datenschutz und Recht

- **www.bfdi.bund.de**
  Wertvolle Informationen rund um den Datenschutz stellt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit auf seinen Web-Seiten bereit. Hier sind auch die Adressen und Links zu den Datenschutzbeauftragten der Länder zusammengestellt, die ebenfalls ein umfangreiches Informationsangebot auch zu Themen der Informationssicherheit bieten.
- **www.datenschutz.de**
  Das „Virtuelle Datenschutzbüro“ ist ein Projekt, an dem u. a. die Datenschutzbeauftragten des Bundes und der Länder beteiligt sind. Es soll vor allem ein einheitliches Portal zum (vornehmlich deutschsprachigen) Datenschutzwissen im Internet sein und enthält eine große Zahl von Beiträgen oder Artikeln.
- **www.bsi.bund.de/Studien**
  Unter dieser Adresse findet sich ein Artikel zur BSI-Studie „IT-Sicherheit und Recht“.

Herausgeber und Redaktion:
Bundesamt für Sicherheit
in der Informationstechnik
Referat 114 Sicherheitsmanagement und IT-Grundschutz
Postfach 20 03 63
53133 Bonn

Telefon: +49 (0) 22899 9582 - 5369
Telefax: +49 (0) 22899 9582 - 5400

Internet: www.bsi.bund.de/grundschutz
E-Mail: grundschutz@bsi.bund.de

Art.- Nr.: BSI-Bro10/311

Herstellung:
Das Druckhaus Bernd Brümmer
53347 Alfter/Bonn
www.druckhaus-bonn.de