TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.

Leitfaden zur Informationssicherheit in der Markt-, Meinungs- und Sozialforschung

TeleTrusT/ADM-Arbeitsgruppe "IT-Sicherheit in der Marktforschung"

Impressum

Herausgeber:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 306
Fax: +49 30 400 54 311
E-Mail: info@teletrust.de
http://www.teletrust.de

Herstellung:

DATEV eG, Nürnberg

1. Auflage

Inhalt

1 Vorwort

2 Einleitung

3 Bestandsaufnahme

4 Rechtliche Aspekte

5 Checkliste zur Informationssicherheit in der Markt-, Meinungs- und Sozialforschung

A. Informationssicherheitsmanagement
B. Sicherheit von IT-Systemen
C. Vernetzung und Internet-Anbindung
D. Beachtung von Sicherheitserfordernissen
E. Wartung von IT-Systemen: Umgang mit Updates
F. Passwörter und Verschlüsselung
G. IT-Notfallvorsorge
H. Datensicherung
I. Infrastruktursicherheit

1 Vorwort

Die Einrichtung der Arbeitsgruppe "IT-Sicherheit in der Markt-, Meinungs- und Sozialforschung" durch den Bundesverband IT-Sicherheit e.V. (TeleTrusT) und den ADM Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V. in Kooperation mit der Deutschen Gesellschaft für Online-Forschung e.V. (DGOF) als jeweilige Branchenvertretungen ist Ausdruck der als gemeinsame Aufgabe empfundenen Verantwortung der drei Verbände für die Sicherheit der in den Markt- und Sozialforschungsinstituten vorhandenen Daten und Informationen.

Die Aktivitäten der gemeinsamen Arbeitsgruppe begannen mit einer Informationsveranstaltung zur IT-Sicherheit in der Markt-, Meinungs- und Sozialforschung im Oktober 2013 in Berlin. Im Sommer 2014 führten ADM und DGOF eine Befragung ihrer Mitgliedsinstitute zum Stand der Informationssicherheit im jeweiligen Institut durch. Die Ergebnisse dieser Mitgliederbefragung wurden erstmals auf der Fachmesse der Marktforschung "Research & Results" im Oktober 2014 in München präsentiert. Selbstverständlich haben die Umfrageergebnisse auch unmittelbar Eingang gefunden in die konkreten Hinweise und Empfehlungen des vorliegenden Leitfadens zur Informationssicherheit in der Markt-, Meinungs- und Sozialforschung.

TeleTrusT, ADM und DGOF sehen die Förderung der Informationssicherheit in der Markt-, Meinungs- und Sozialforschung als eine permanente gemeinsame Aufgabe und Verantwortung an und werden deshalb den gemeinsamen Ausschuss mit vielfältigen Aktivitäten fortführen. Der Dank der drei Verbände geht an die jeweiligen Mitglieder, die durch ihre aktive Mitarbeit in dem Ausschuss das erst möglich machen. Ganz besonderer Dank gilt den Autoren des vorliegenden Leitfadens zur Informationssicherheit in der Markt-, Meinungs- und Sozialforschung: Alexandra Wachenfeld-Schell, Oliver Bauchinger, Uwe Czaia, Mehmet Kus, Dr. Holger Mühlbauer, Dr. Volker Scheidemann, Bernd Uhlmann und Erich Wiegand.

TeleTrusT – Bundesverband IT-Sicherheit e.V.

ADM Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.

DGOF Deutsche Gesellschaft für Online-Forschung e.V.

2 Einleitung

Der verhaltensbedingte Schutz und die technikbedingte Sicherheit von Daten und Informationen sind zwei Aspekte einer Problematik, die mit der fortschreitenden Digitalisierung der Gesellschaft nicht mehr getrennt gesehen werden können. Über Jahrzehnte hinweg stand für die Verbände der Markt- und Sozialforschung der Schutz der Anonymität der Untersuchungsteilnehmer und die Vertraulichkeit ihrer Daten durch die Konkretisierung und Präzisierung der gesetzlichen Bestimmungen des Datenschutzes in den berufsständischen Verhaltensregeln aus guten Gründen ganz eindeutig im Vordergrund ihres Handels. Die Sicherheit der Daten und Informationen durch den Einsatz entsprechender Technologien spielte demgegenüber für die Verbände eine eher untergeordnete Rolle, nicht so natürlich für die einzelnen Forschungsinstitute.

Erst langsam setzte sich in den Verbänden der Markt- und Sozialforschung die Erkenntnis durch, dass neben den - nicht nur personenbezogenen - Daten der Untersuchungsteilnehmer in den Forschungsinstituten eine ganze Reihe verschiedenartiger Daten und Informationen vorliegen, zu deren Schutz berufsständische Verhaltensregeln definiert werden müssen, die die technikbedingten Maßnahmen zur Daten- und Informationssicherheit sichern und verstärken.

Auch im Bereich der Informationssicherheit gibt es, wie für den Forschungsprozess selbst, für Markt- und Sozialforschungsinstitute verschiedene Möglichkeiten, die ganzheitliche Qualität ihrer datenschützenden und informationssichernden Maßnahmen auf der Grundlage objektiver Kriterien und Maßstäbe durch externe Prüfer bewerten und dokumentieren zu lassen. Die Verbände der Markt- und Sozialforschung in Deutschland fordern von ihren Mitgliedsinstituten keine externe Qualitätsbewertung der Informationssicherheit als Voraussetzung der Mitgliedschaft. Es ist aber die Absicht der Verbände, durch verschiedene Maßnahmen zu einer signifikanten Erhöhung des Niveaus der Informationssicherheit beizutragen. Der vorliegende Leitfaden zur Informationssicherheit in der Markt-, Meinungs- und Sozialforschung spielt dabei eine zentrale Rolle.

Die Hinweise und Empfehlungen des vorliegenden Leitfadens sind zu lesen als eine Art Checkliste, die es den Forschungsinstituten ermöglicht, ihr Konzept der Informationssicherheit umfassend auszubauen, effizient zu überprüfen und entdeckte Schwachstellen gegebenenfalls zu beseitigen. Für die Auftraggeber von Forschungsdienstleistungen bietet sie die Möglichkeit, den Schutz und die Sicherheit der an ein Forschungsinstitut übermittelten Unternehmens- und anderen Daten durch die im Institut getroffenen Maßnahmen anhand objektiver Kriterien bewerten zu können.

3 Bestandsaufnahme

Die den vorliegenden Leitfaden herausgebenden Verbände sind sich der hohen Relevanz der Informationssicherheit in Bezug auf die Reputation und die Fähigkeit zur Selbstregulierung der Markt- und Sozialforschung bewusst und wollen die Branche bei der Identifizierung von kritischen Handlungsfeldern unterstützen.

Vor diesem Hintergrund wurde im Sommer 2014 die Befragung der Mitglieder von ADM und DGOF zur Informationssicherheit in den Instituten durchgeführt. Sie diente einerseits als empirischer Befund des Status Quo der Branche. Andererseits ist sie ein Wegweiser für das Erkennen von Defiziten. Auf dieser Basis lassen sich exemplarisch relevante Maßnahmen ableiten und Möglichkeiten der effizienten Umsetzung aufzeigen, mit dem Ziel, den Stand der Informationssicherheit im Institut zu optimieren.

Zur Strukturierung einer systematisierten Analyse der Informationssicherheit werden die folgenden Bereiche unterschieden:

A. Informationssicherheitsmanagement
B. Sicherheit von IT-Systemen
C. Vernetzung und Internet-Anbindung
D. Beachtung von Sicherheitserfordernissen
E. Wartung von IT-Systemen: Umgang mit Updates
F. Passwörter und Verschlüsselung
G. IT-Notfallvorsorge
H. Datensicherung
I. Infrastruktursicherheit

Die Mitgliederbefragung zeigt in vielerlei Hinsicht, dass die Branche der notwendigen Informationssicherheit Rechnung trägt und in vielen Bereichen bereits gut aufgestellt ist. Gut aufgestellte Bereiche sind:

- Viren-Schutzprogramme
- Eigene Rollen und Profile für Administratoren
- Zentrale Firewall-Systeme
- Regelmäßige Sicherheits-Updates
- Backupstrategie
- Zutrittskontrolle / Zutrittsschutz

Aber die Befragung legt auch "Baustellen" offen, bei deren Beseitigung die Verbände unter anderem mit Hilfe des vorliegenden Leitfadens zur Informationssicherheit die Branche mit einer Checkliste unterstützen möchten. Vor allem die folgenden Bereiche sind als "Baustellen" zu bezeichnen:

- Zutrittskontrolle / Zutrittsschutz
- Bestimmung von Sicherheitsbeauftragten
- Dokumentation und regelmäßige Überprüfung von Sicherheitskonzepten
- Sensibilisierung und Schulung der Mitarbeiter
- Klassifizierung von Daten und Dokumenten nach Vertraulichkeitsklassen
- Testkonzept für Software-Änderungen
- Notfallmanagement

Die mangelnde Sensibilisierung der Mitarbeiter und eine fehlende nachhaltige Schulung, das Fehlen eines dokumentierten Sicherheitskonzepts sowie eines umfassenden Notfallmanagements konnten als die dringendsten Handlungsfelder identifiziert werden.

Um die Defizite zu beseitigen braucht es auf der Institutsebene:

→ Einen ganzheitlichen Ansatz
→ Eine methodische Vorgehensweise
→ Ein Konzept zur kontinuierlichen Verbesserung
→ Ein verantwortliches Managementsystem für Informationssicherheit
→ Die Mitarbeit jedes Einzelnen
→ Und ein positives Image der Informationssicherheit als Teil der Wertschöpfungskette in der Markt-, Meinungs- und Sozialforschung

Das Ziel ist ein System von Strategien und Verfahren zur Identifizierung, Kontrolle und zum Schutz von Informationen und Geräten, die im Zusammenhang mit der Speicherung, Übermittlung und Verarbeitung von Daten und Informationen genutzt werden.

4 Rechtliche Aspekte

Ganzheitliches Management von Informationssicherheit erfordert technisch-organisatorische Maßnahmen wie Handlungsanweisungen, Verfahrens- und Nutzungsrichtlinien sowie die Einhaltung rechtlicher Rahmenbedingungen. Ergänzt wird dies durch ein Risikomanagement einschließlich Mitarbeiterschulung, das durch die Entscheidungsträger eines Unternehmens bzw. einer Organisation umzusetzen ist. Dies dient auch der Vermeidung von Haftungstatbeständen.

Ganzheitliche Informationssicherheit umfasst:[1]

- Organisatorische Sicherheit (Risikomanagement, Nutzungsrichtlinien, Kontrolle, Schulung);
- Rechtliche Sicherheit (Vertragsgestaltung, AGB, Vermeidung straf- und zivilrechtlicher Haftung bzw. Organisationsverschulden, Betriebsvereinbarungen);
- Technische Sicherheit (Archivierung, Backup, Firewall, Filter, Verschlüsselung, Authentifizierung);
- Wirtschaftliche Sicherheit (Vermeidung wirtschaftlicher Schäden durch IT-Sicherheitsvorfälle).

Der Bundesgerichtshof (BGH) verwendet in Zusammenhang mit dem Haftungsrecht den Begriff "Verkehrssicherungspflichten". Das bedeutet: Wer eine Gefahrenquelle eröffnet oder sich an ihr beteiligt, muss Dritte schützen und hierfür geeignete Schutzmaßnahmen ergreifen. Die IT-gestützten Kommunikationsvorgänge (z.B. in Intranet und Internet) eröffnen vielfältige Gefahren und sind demnach Gefahrenquellen im Sinne der Verkehrssicherungspflichten.

Diese **Verkehrssicherungspflichten** bestehen im Wesentlichen aus:

- Organisationspflichten bezüglich betrieblicher und technischer Abläufe;
- Aufsichtspflichten des Arbeitgebers gegenüber seinen Mitarbeitern.

Vollständige Sicherheit kann im Rahmen der Verkehrssicherungspflichten nicht verlangt werden, jedoch solche Maßnahmen, die wirtschaftlich zumutbar sind.

[1] Zusammengestellt unter Verwendung von: Speichert, Horst: IT-Rechtsleitfaden

Vertragliche Schutzpflichten richten sich nach den Verkehrssicherungspflichten. Solche Verkehrssicherungspflichten ergeben sich aus einer Vielzahl gesetzlicher und vertraglicher Bestimmungen sowie der Rechtsprechung. Hervorzuheben sind insbesondere:

- "Garantenstellung" nach § 13 StGB: Straftaten können auch durch Unterlassen von Sicherungsmaßnahmen, Verletzung von Sorgfaltspflichten begangen werden;
- § 9 BDSG plus Anlage (Diese Vorschrift enthält die Grundsätze ordnungsgemäßer Datenverarbeitung, also Vorgaben für die technisch-organisatorische Datensicherheit);
- bei Amts-, Berufs- und Privatgeheimnissen, § 203 StGB;
- bei Geschäfts- und Betriebsgeheimnissen, § 17 UWG;
- besondere Verschwiegenheitsverpflichtungen und strafbewehrte Garantenpflicht für besonders sensible Daten.

Es ist ein **technisches Sicherheitskonzept** zu entwickeln, das unbefugten Zugriff auf personenbezogene Daten verhindert. Im Einzelnen bedeutet dies:

- Verfügbarkeitskontrolle (Virenschutz, Backup, sichere Archivierung);
- Weitergabekontrolle (Datensicherung, Verschlüsselung);
- Zugangskontrolle (Passwort, Firewall);
- Zugriffskontrolle (effektive, rollenbasierte Rechteverwaltung);
- Zutrittskontrolle (räumliche, physische Sicherung).

Die Vermeidung **persönlicher Eigenhaftung** ist für die handelnden Mitarbeiter, wie Leiter von IT-Abteilungen, Sicherheitsbeauftragte, Administratoren und sonstige IT-Verantwortliche entscheidend. Hierbei ist zu unterscheiden zwischen:

- arbeitsrechtlicher Haftung (Abmahnung, Kündigung);
- strafrechtlicher Haftung (Geld- oder Freiheitsstrafe);
- zivilrechtlicher Haftung (Schadensersatz).

Abgeleitet aus dem Arbeitsvertragsverhältnis hat jeder Mitarbeiter arbeitsvertragliche Nebenpflichten (Schutz-, Mitwirkungs-, Geheimhaltungs- und Aufklärungspflichten). Bei leitenden Mitarbeitern gelten höhere Sorgfaltsanforderungen.

Schadensersatzansprüche des Arbeitgebers wegen Verletzung arbeitsvertraglicher Nebenpflichten sind in der Praxis in seltenen Fällen zwar möglich, aber wegen der Fremdbestimmtheit der Arbeitsleistung trägt der Arbeitgeber grundsätzlich das **Unternehmerrisiko**. Für Arbeitnehmertätigkeiten mit erhöhtem Risiko gelten deshalb (Rechtsprechung des BAG) die Grundsätze zur sog. "schadensgeneigten Tätigkeit":

- für vorsätzliches und grob fahrlässiges Verhalten: volle Haftung des Mitarbeiters;
- mittlere Fahrlässigkeit: Schadensteilung zwischen Arbeitgeber und Mitarbeiter;
- leichte Fahrlässigkeit: keine Haftung des Mitarbeiters.

Diese Haftungserleichterung für den Mitarbeiter gilt grundsätzlich nur im Innenverhältnis zum Arbeitgeber. Im Außenverhältnis zu geschädigten Dritten besteht ein Freistellungsanspruch des Arbeitnehmers gegen den Arbeitgeber. Für eine mögliche Strafbarkeit gilt dagegen der Grundsatz der vollständigen Eigenverantwortung. Ein Arbeitnehmer macht sich also selbst strafbar, die arbeitsvertragliche Haftungserleichterung ist nicht anwendbar. Auch ein "Befehlsnotstand" kann im Regelfall nicht angeführt werden.

Zur **Vermeidung von Eigenhaftung** kann ein verantwortlicher Mitarbeiter nachfolgende Maßnahmen zum Selbstschutz ergreifen:

- Gewissenhafte Aufgabenerfüllung;
- Lösungsvorschläge für Sicherheitsmängel erarbeiten, Projekte vorschlagen, angemessenes Budget beantragen;
- Regelmäßige Information der Geschäftsleitung über mögliche Risiken;
- gegebenenfalls Hinzuziehung externer Berater.

Als Reaktion bei Ablehnung vorgeschlagener Maßnahmen durch die Geschäftsleitung ist zu empfehlen:

- Risiken erneut aufzeigen;
- Vorgang des Vorschlags und der Ablehnung "protokollieren" bzw. dokumentieren;
- "Mitwisser" schaffen, z.B. durch E-Mail mit 'cc';
- schriftliche Bestätigung als Risikoakzeptanz einfordern.

In erster Linie ist aber die Unternehmensleitung für ein effektives Risikomanagement verantwortlich, wozu auch das Informationssicherheitsmanagement zählt. Insbesondere müssen Gefahrenpotenziale erfasst, abgeschätzt und überwacht werden, damit Gefahren frühzeitig erkannt werden.

Der Umfang der Managementpflichten variiert je nach Gefahrenlage und Schadenspotenzial. Kommt die Unternehmensleitung ihren Pflichten nicht mit der gebotenen Sorgfalt nach, ergeben sich persönliche Haftungsrisiken der Verantwortlichen gegenüber dem Unternehmen oder gegenüber Dritten. Daher empfiehlt es sich, alle einschlägigen Veranlassungen zu dokumentieren.

5 Checkliste zur Informationssicherheit in der Markt-, Meinungs- und Sozialforschung

A. Informationssicherheitsmanagement

01. Hat das Management die Informationssicherheitsziele festgelegt und die Verantwortung für die Informationssicherheit übernommen?

Auf höchster Ebene sollte eine Informationssicherheitsleitlinie definiert werden, die vom Management genehmigt ist und einen Ansatz zur Bewältigung der Informationssicherheitsziele festlegt.

Leitlinien sollten Mitarbeitern und allen maßgeblichen internen und externen Stellen in einer Form mitgeteilt werden, die für die Zielgruppe relevant, zugänglich und verständlich ist, z.B. im Rahmen eines "Schulungsprogramms zur Sensibilisierung für Informationssicherheit".

02. Sind gesetzliche oder vertragsrechtliche Gesichtspunkte berücksichtigt worden?

Unternehmen müssen im Rahmen der "Compliance" zahlreiche rechtliche Bestimmungen beachten. Hierfür ist vor allem die anzuwendende Sorgfaltspflicht ausschlaggebend. Des Weiteren existieren Anforderungen durch Buchführungs- und Aufbewahrungspflichten (z.B. SOX) sowie beim Umgang mit personenbezogenen Daten (BDSG) und Fernmeldedaten (TKG).

Das Management sollte alle für ihr Institut geltenden Gesetze und vertraglichen Anforderungen ermitteln, um die entsprechende Compliance herstellen zu können.

Alle relevanten gesetzlichen und vertraglichen Anforderungen sollten für jedes relevante Informationssystem sowie für das gesamte Institut ermittelt, dokumentiert und aktuell gehalten werden.

Die Maßnahmen und die einzelnen Zuständigkeiten zur Erfüllung dieser Anforderungen sollten ebenfalls festgelegt und dokumentiert werden.

03. Werden Sicherheitserfordernisse bei Entscheidungen frühzeitig berücksichtigt (z.B. bei Planung eines neuen Netzes, Neuanschaffungen von IT-Systemen & Anwendungen, Outsourcing- & Dienstleistungsverträgen)?

Um Sicherheitserfordernisse bei Entscheidungen frühzeitig berücksichtigen zu können, ist es erforderlich, Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit festzulegen.

Um Verantwortungen im Bereich der Informationssicherheit gerecht zu werden, sollten ernannte Personen in diesem Bereich fachkundig sein und die Möglichkeit erhalten, mit Entwicklungen Schritt halten zu können. Eine Koordination und Kontrolle der Informationssicherheitsaspekte bei Neuanschaffungen oder bei Änderungen in Lieferantenbeziehungen sollten ermittelt und dokumentiert werden.

Im Change und Release Management sollten Informationssicherheitsaspekte prozessual verankert werden, d.h. es muss u.a. nachvollziehbar sein, warum wer was wann geändert hat.

04. Besteht ein Überblick über die wichtigsten Anwendungen und IT-Systeme und deren Schutzbedarf?

Informationen verarbeitende Systeme sollten nach ihrem Wert, gesetzlichen Vorschriften, Betriebswichtigkeit und Sensibilität im Hinblick auf unbefugte Offenlegung oder Veränderung klassifiziert werden (Asset-Register). Verfahren für den Umgang mit Werten bzw. Informationen sind entsprechend dem von dem Institut übernommenen Klassifizierungsschema für Informationen zu entwickeln und zu implementieren. Eine Schutzbedarfsanalyse sollte durchgeführt werden (mindestens der Kernprozesse, der dabei beteiligten Systeme und Applikationen).

05. Sind die Sicherheitsziele priorisiert und die Umsetzung der beschlossenen Sicherheitsmaßnahmen geregelt?

Die Ergebnisse einer Risikobewertung helfen dabei, geeignete betriebliche Maßnahmen und Prioritäten zur Bewältigung von Risiken der Informationssicherheit festzulegen, zu betreuen und ausgewählte Sicherheitsmaßnahmen zum Schutz gegen diese Risiken einzuführen. Ein Risikobehandlungsplan sollte erstellt und gemeinsam mit dem Management geregelt und priorisiert werden.

06. Ist bei den Sicherheitsmaßnahmen festgelegt, ob sie einmalig oder in regelmäßigen Intervallen ausgeführt werden müssen (z.B. Update des Viren-Schutzprogramms)?

Angemessene Festlegungen je nach Risikohöhe sind zu treffen und zu dokumentieren. Die Ausführung der Sicherheitsmaßnahmen ist regelmäßig zu kontrollieren. Bei Änderung der Bedrohungslage sind die Intervalle der Sicherheitsmaßnahmen entsprechend anzupassen.

07. Sind für die Sicherheitsmaßnahmen Zuständigkeiten und Verantwortlichkeiten festgelegt?

Für umzusetzende Ziele und regelmäßig wiederkehrende Maßnahmen hat sich eine Taskliste oder aber eine KVP-Liste (Kontinuierlicher-Verbesserungs-Prozess) mit Verantwortlichkeiten und einzuhaltenden Terminen zur jeweiligen Umsetzung bewährt. Es sollten regelmäßige unterjährige Reviews durchgeführt werden.

08. Gibt es Vertretungsregelungen für Verantwortliche und sind die Vertreter mit Ihren Aufgaben vertraut?

Vertretungsregelungen sind zu treffen und es ist dafür Sorge zu tragen, dass die Vertreter mit den jeweiligen Aufgaben auch vertraut sind und Zugangsberechtigungen haben. Entsprechende Ausbildungs- und Trainingsmaßnahmen sollten durchgeführt werden.

09. Sind wichtige Passwörter für Notfälle sicher hinterlegt?

Wichtige Passwörter sollten immer sicher verwahrt werden (Verschlüsselung, z.B. mittels KeePass - Password Safe). Eine Auslagerung der wichtigsten Passwörter (z.B. im Tresor außerhalb des Bürogebäudes) sollte in Erwägung gezogen werden.

10. Sind die Richtlinien zur Informationssicherheit und die entsprechenden Zuständigkeiten im Institut bekannt?

Durch interne Schulungen sollten die Richtlinien und die verantwortliche Sicherheitsorganisation bekannt gemacht werden. Auch die regelmäßige Durchführung von E-Learning-Maßnahmen für alle Mitarbeiter ist geeignet, das notwendige Wissen bei den Mitarbeitern aufzubauen.

Das Management sollte alle Mitarbeiter und Auftragnehmer dazu anhalten, Sicherheitsmaßnahmen entsprechend den festgelegten Leitlinien und Verfahren des Instituts anzuwenden.

11. Gibt es dokumentierte Prozesse, die beim Eintritt und Austritt von Mitarbeitern zu beachten sind?

Der Ein- und Austrittsprozess der Mitarbeiter sollte Berechtigungen, Schlüssel, Unterweisung etc. regeln.

Die vertraglichen Verpflichtungen der Mitarbeiter oder Auftragnehmer sollten die Inhalte der Leitlinie für Informationssicherheit des Instituts widerspiegeln.

Die Personalabteilung ist im Allgemeinen zuständig für den gesamten Einstellungs- und Beendigungsprozess und arbeitet mit dem Vorgesetzten der einzustellenden oder ausscheidenden Person zusammen, um Aspekte der Informationssicherheit im Zusammenhang mit den entsprechenden Verfahren zu regeln.

12. Wird die Wirksamkeit von Sicherheitsmaßnahmen regelmäßig überprüft?

Ein Auditprogramm sollte erstellt und umgesetzt werden. Die Durchführung von internen und externen Audits dient der regelmäßigen Überprüfung der Wirksamkeit von Sicherheitsmaßnahmen. Es sollten auch unangemeldete interne Begehungen und Audits durchgeführt werden.

13. Gibt es ein dokumentiertes Sicherheitskonzept?

Die Security Policy des Instituts, die allen Mitarbeitern bekannt gemacht werden sollte, muss das Sicherheitskonzept beinhalten. Es sollten außerdem Regelungen im Rahmen des Risikomanagements etabliert werden.

B. Sicherheit von IT-Systemen

14. Werden vorhandene Schutzmechanismen in Applikationen genutzt?

Applikationen, insbesondere Webbrowser, bieten integrierte Schutzmechanismen zum Selbstschutz, welche sich in den Sicherheitseinstellungen der jeweiligen Applikation konfigurieren lassen. Diese vorhandenen Sicherheitsfunktionalitäten (insbesondere die Rückfrage vor dem Ausführen von Programmen) sollten genutzt werden. Passwortschutz, verschlüsselte Kommunikation oder der Einsatz von Zertifikaten sind einige Beispiele von Schutzmechanismen in Applikationen - insbesondere in Mailprogrammen - die verwendet werden sollten. Es sollte auch sichergestellt werden, dass Anwender (und mit Anwender-Rechten gestartete Programme) möglichst keine sicherheitsrelevanten Änderungen an den Systemeinstellungen durchführen können, sondern dass dies nur durch die Rolle des Administrators erfolgen kann.

15. Werden Viren-Schutzprogramme eingesetzt?

Viren-Schutzprogramme sind wirksame Mittel in der Prävention von Schadsoftware (z.B. Viren, Trojaner, Würmer). Sowohl die Software als auch Signaturen sollten stets auf dem aktuellen Stand gehalten werden. Viren-Schutzprogramme sollten auch ein- und ausgehende E-Mails überprüfen.

16. Werden den Systembenutzern Rollen und Profile zugeordnet?

Um die Sicherheit der Systemlandschaft zu erhöhen ist es notwendig, den Systembenutzern adäquate Rollen und Profile zuzuordnen. Hierbei ist zu beachten, dass nur notwendige Berechtigungen den entsprechenden Systembenutzern zugeordnet werden. Reine Anwender (und Programme mit Anwenderrechten) sollten nicht berechtigt sein, sicherheitsrelevante Änderungen an den Systemeinstellungen durchzuführen.

17. Ist geregelt, auf welche Datenbestände jeder Mitarbeiter zugreifen darf?

Der Zugriff auf die Datenbestände sollte ausschließlich zweckgebunden sein und nur von autorisierten Mitarbeitern erfolgen. Hierfür sind entsprechende organisatorische und technische Vorkehrungen zu treffen. Es muss sichergestellt sein, dass Benutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind und dass Daten bei der Verarbeitung, Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können.

18. Gibt es eigene Rollen und Profile für Administratoren?

Administrator im Allgemeinen ist ein Benutzer mit erweiterten Berechtigungen zur Verwaltung von IT-Systemen, Netzwerken, Programmen, Mailboxen, Webseiten, Foren oder Datenbanken. Jeder Administrator sollte abhängig von seinen Aufgaben nur über hieran angepasste Rechte verfügen. Administratoren dürfen ihre erweiterten Rechte nur bei Verwendung der Administratorenprofile nutzen.

19. Ist bekannt und geregelt, welche Privilegien und Rechte Applikationen (Software) haben?

Einer Applikation können verschiedene Privilegien und Rechte zugewiesen werden. Es ist zu regeln, auf welche Verzeichnisse, Dateien und Dienste eine Applikation zugreifen darf. Mit erweiterten Rechten können Applikationen auch private Informationen anderer Nutzer abrufen und auch verändern.

20. Werden sicherheitsrelevante Standardeinstellungen von Applikationen und IT-Systemen geeignet angepasst?

Die vorhandenen Sicherheitsfunktionalitäten von Applikationen sollten auf jeden Fall angepasst werden. Die Priorität bei der Auslieferung von Applikationen und Systemen liegt bei den meisten Herstellern in der Funktionalität und einfachen Handhabung der Lösung und weniger beim Thema Informationssicherheit und Datenschutz. Der Softwarehersteller hat ein primäres Interesse daran, dass die Software installiert werden kann, ohne Kosten zu verursachen und auf einer großen Bandbreite von verschiedenen Systemkonfigurationen funktioniert. Daher sind die sicherheitsrelevanten Standardeinstellungen zumeist auf dem Stand des kleinsten gemeinsamen Nenners der IT-Landschaft und sollten nach der Installation auf dem sicherheitskritischen System auf die jeweilige Infrastruktur angepasst werden.

21. Werden nicht benötigte sicherheitsrelevante Applikationen und Funktionen deinstalliert bzw. deaktiviert?

Sicherheitsrelevante Applikationen und Funktionen, die nicht benötigt werden, können zu einem Sicherheitsrisiko werden und sollten daher deinstalliert oder deaktiviert werden. Standardpasswörter und Standard-Benutzer-Accounts sollten geändert werden.

22. Werden Installations- und Systemdokumentationen erstellt und regelmäßig aktualisiert?

Es wird empfohlen, alle Schritte vor, während und nach einer Installation schriftlich zu dokumentieren. Dies spart im Wiederholungsfall nicht nur Zeit und Kosten, sondern hilft auch in Problemfällen die Ursachen schneller zu finden. Dokumentationen sollten so erstellt werden, dass auch Anwender ohne systemisches Vorwissen die entsprechenden Anwendungen bedienen können. Zur Reduzierung von Ausfällen und zur Sicherstellung der Nutzbarkeit sollten Systemdokumentationen von Dritten evaluiert werden.

C. Vernetzung und Internet-Anbindung

23. Werden zentrale Firewall-Systeme eingesetzt?

Firewall-Systeme sind ein Bestandteil eines ganzheitlichen Sicherheitskonzeptes und sollten immer eingesetzt werden. Weiterführende Hinweise zu Firewall-Systemen sind auch in den IT-Grundschutz-Katalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) enthalten.

24. Werden Konfiguration und Funktionsfähigkeit der Firewall-Systeme regelmäßig überprüft?

Die regelmäßige Überprüfung der Funktionsfähigkeit und Konfiguration eines Firewall-Systems ist notwendig. Die Wartung eines Firewall-Systems sollte regelmäßig erfolgen. Filterregeln eines Firewall-Systems sollten so restriktiv wie möglich eingestellt sein. Die Filterregeln sollten regelmäßig überprüft werden. Im Anschluss an einer Änderung der Firewall-Konfiguration sollte ein Funktionstest durchgeführt werden. Neben einer regelmäßigen Überprüfung wird auch eine anlass- bzw. ereignisbasierte Überprüfung empfohlen. Der Einsatz eines Firewall-Systems, die Wartung wie auch die Auswertung der Protokollierung sollten ein Bestandteil des Sicherheitskonzeptes sein.

25. Gibt es ein Konzept, wenn Services nach außen durch die Firewall-Systeme angeboten werden?

Dienste, die nach außen angeboten werden, erhöhen das potenzielle Angriffsrisiko auf die IT-Infrastruktur. Die Verfügbarkeit nach außen sichtbarer Dienste sollte daher auf das erforderliche Mindestmaß beschränkt sein, welches im Rahmen eines Sicherheitskonzeptes geregelt ist. Das Konzept sollte u.a. regeln welche Ports, Dienste bzw. Funktionen wie und in welchem Zeitrahmen erreichbar sind. Es sollte regelmäßig überprüft werden, welche Dienste bzw. Funktionen nach außen erreichbar sind und ob diese auch wirklich notwendig sind. Kontrollierte Penetrationstests auf Firewall-Systeme sollten nach einem Vier-Augen-Prinzip erfolgen. Zudem sollten die Dienste auch nach innen abgesichert sein, um im Angriffsfall den möglichen Schaden so weit wie möglich zu reduzieren. So sollten diese Dienste (wenn möglich) auf einem speziell abgesicherten Teil der Infrastruktur betrieben werden und über möglichst minimale Nutzungsrechte verfügen. Zudem sollten alle Zugriffe auf die Dienste protokolliert werden, um ggf. Angriffsszenarien nachvollziehen und so besser abwehren zu können.

26. Werden Intrusion Detection Systeme und Intrusion Prevention Systeme eingesetzt?

Als Intrusion Detection Systeme (IDS) werden Lösungen bezeichnet, die Angriffe, welche sich gegen Computersysteme oder Rechnernetze richten, erkennen können. Sie dienen der Alarmierung und Dokumentation dieser Ereignisse. Intrusion Prevention Systeme (IPS) können darüber hinaus die entdeckten Angriffe abwehren. IDS/IPS Lösungen sind wichtige Ergänzungen zu einer Firewall und erhöhen die Sicherheit von IT-Infrastrukturen und Systemen. Zusätzlich dienen diese Systeme der Protokollierung und erhöhen gegebenenfalls die Chancen einer Strafverfolgung und sollten deshalb eingesetzt werden.

27. Ist festgelegt, wie Webbrowser mit Zusatzprogrammen (Plug-ins, Add-ons) und aktiven Inhalten (z.B. ActiveX, Java) umgehen?

Webbrowser sind Softwareprogramme zum Betrachten von Webseiten. Viele Webbrowser ermöglichen die zusätzliche Installation von Zusatzprogrammen zur Darstellung von verschiedenen Medienformaten oder auch aktiven Inhalten. Die meisten Sicherheitsprobleme bei der Internet-Nutzung tauchen im Zusammenhang mit aktiven Inhalten wie JavaScript, ActiveX, Flash oder Java, aber auch im Zusammenhang mit anderen Plug-ins und Add-ons auf.

Es sollte daher festgelegt sein, auf welche aktiven Inhalte zugegriffen werden darf und welche Plug-ins bzw. Add-ons installiert werden dürfen. Hierbei sollten Warnungen wie z.B. vom BSI beachtet werden. Auch Plug-ins und Add-ons sollten im Rahmen der Wartung regelmäßig überprüft und aktualisiert werden. Die integrierten Sicherheitsfunktionalitäten der Browser (insbesondere die Rückfrage vor dem Ausführen von Programmen) sollten auf jeden Fall genutzt werden.

28. Sind die Mitarbeiter im Hinblick auf die Risiken des Internets ausreichend geschult?

Mitarbeiter, die nicht regelmäßig geschult und entsprechend sensibilisiert werden, sind oft das größte Risiko im Hinblick auf die Informationssicherheit im Unternehmen. Die Sensibilisierung und die Vermittlung von Kenntnissen zur Informationssicherheit durch regelmäßige Schulungen sollte im Rahmen eines ganzheitlichen Sicherheitskonzepts erfolgen.

Die Mitarbeiter sollten bezüglich der Risiken des Internets ausreichend geschult werden und dazu angehalten werden, den Vorgaben hinsichtlich Informationssicherheit und Verwendung des Internets und den damit verbundenen Applikationen (Browser, Plug-ins, besuchte Webseiten) strikt Folge zu leisten. Die private Verwendung des Internets am Arbeitsplatz ist in jedem Unternehmen individuell geregelt, doch sollte darauf geachtet werden, dass auch dann die sicherheitsrelevanten Vorgaben einzuhalten sind.

D. Beachtung von Sicherheitserfordernissen

29. Werden Informationen und Datenträger vor unbefugtem Zugriff geschützt?

Informationen und Datenträger sollten nur nach dem so genannten "Need-to-know"-Prinzip zugänglich gemacht werden. Das bedeutet, dass Informationen nur Personen zugänglich gemacht werden sollten, die diese Informationen zur Erledigung ihrer Arbeit tatsächlich benötigen. Für schriftliche Informationen oder physische Datenträger empfehlen sich abschließbare Aktenschränke mit einem kontrollierten Zugriff auf die zugehörigen Schlüssel. Für den Zugriff auf elektronisch gespeicherte Informationen sollte ein Zugriffsrechte-Management eingeführt werden, z.B. über Microsoft Active Directory oder über gruppenrechtsfähige Verschlüsselungsverfahren.

30. Werden vertrauliche Informationen auch bei Wartungs- und Reparaturarbeiten von Datenträgern oder IT-Systemen geschützt?

Wartungspersonal sollte nur unter Aufsicht eigener vertrauensvoller Mitarbeiter der Zugang zu IT-Systemen und der Zugriff auf Datenträger gewährt werden. Für den Fall, dass IT-Systeme oder Datenträger außerhalb des eigenen Unternehmens gewartet oder verwahrt werden, empfiehlt es sich, vertrauliche Daten durch Verschlüsselung zu schützen, da diese auch dann noch Informationen schützt, wenn Zugriffsrechte-Managementsysteme nicht aktiv sind.

31. Sind die Informationen nach Vertraulichkeit klassifiziert?

Informationen sollten nach Vertraulichkeit klassifiziert werden. Es empfiehlt sich, mindestens die Klassifizierungen "öffentlich" und "vertraulich" zu verwenden. Während für öffentliche Informationen keine besonderen Schutzmaßnahmen erforderlich sind, sollten für vertrauliche Informationen, z.B. personenbezogene Daten, Schutzmaßnahmen und die Festlegung von Zugriffsberechtigungen vorgesehen werden. Je nach Relevanz der verarbeiteten Informationen kann die Einführung weiterer Vertraulichkeitsklassen wie "geheim" und "streng geheim" angeraten sein, verbunden mit entsprechenden Kontrollfunktionen, beispielsweise einer Weitergabekontrolle.

32. Wird die Einhaltung bestehender Sicherheitsvorgaben kontrolliert?

Für die Einhaltung bestehender Sicherheitsvorgaben ist es wichtig, die Vorgaben schriftlich festzuhalten und allen Mitarbeitern zugänglich zu machen. Mitarbeiter sollten auf die Einhaltung der Vorgaben verpflichtet werden. Die Einhaltung der Vorgaben sollte, soweit möglich, durch technische Maßnahmen unterstützt werden. Die Umsetzung der technischen Maßnahmen und die Einhaltung der organisatorischen Maßnahmen sollten in regelmäßigen Audits überprüft werden. Hiermit können externe sachkundige Prüfer oder auch hierfür verantwortliche eigene Mitarbeiter beauftragt werden.

33. Werden die Mitarbeiter regelmäßig in sicherheitsrelevanten Themen geschult?

Schulungen zu sicherheitsrelevanten Themen sollten regelmäßig stattfinden. Turnus und Detailtiefe der Schulungen können von der Relevanz der Themen und den Aufgabenbereichen der Mitarbeiter abhängen. Die Minimalanforderung sollte sein, die allgemeinen Sicherheitsvorgaben des Unternehmens vorzustellen und zu erläutern. Für tiefergehende Schulungen und Spezialthemen kann gegebenenfalls auf die Hilfe von externen Spezialisten für Informationssicherheit zurückgegriffen werden.

34. Gibt es Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter?

Mangelndes Sicherheitsbewusstsein von Mitarbeitern ist eine Hauptgefahrenquelle bei der Informationssicherheit. Daher sollten Maßnahmen zur Erhöhung des Sicherheitsbewusstseins regelmäßig ergriffen werden. Dazu zählen beispielsweise Schulungen, Informationsblätter, aufklärende Plakate, informative Videos und, nicht zuletzt, das Vorleben von sicherheitsbewusstem Handeln durch das Management.

E. Wartung von IT-Systemen: Umgang mit Updates

35. Werden Sicherheits-Updates zeitnah eingespielt?

Anbietersoftware, die in den betrieblichen Systemen verwendet wird, sollte die vom Lieferanten angebotene Wartung erfahren. Softwareanbieter stellen den Support für ältere Software-Versionen nach einiger Zeit ein. Das Institut sollte sich mit den Risiken beschäftigen, die mit dem Einsatz einer nicht unterstützten Software verbunden sind.

Bei jeder Entscheidung zur Aktualisierung auf eine neue Version sollten die geschäftlichen Anforderungen für die Änderung und die Sicherheit der Version berücksichtigt werden, z.B. die Einführung neuer Funktionen zur Verbesserung der Informationssicherheit oder Anzahl und Schweregrad der Probleme hinsichtlich der Informationssicherheit, von der diese Version betroffen ist.

Software-Patches/-Updates sollten zeitnah angewendet werden, wenn sie dazu beitragen, Schwächen hinsichtlich der Informationssicherheit zu beheben oder zu mindern.

Es sollte ein dokumentiertes Change- und Release Management eingesetzt werden.

36. Gibt es Verantwortliche, die sich regelmäßig über Sicherheitseigenschaften der verwendeten Software und relevanter Sicherheits-Updates informieren?

Das Institut sollte die mit dem technischen Schwachstellenmanagement verbundenen Aufgaben und Zuständigkeiten festlegen und einrichten, die die Überwachung von Schwachstellen, die Risikobeurteilung von Schwachstellen, das Einspielen von Patches und sämtliche erforderlichen Koordinationsaufgaben umfassen.

Informationen über technische Schwachstellen von verwendeten Informationssystemen sollten rechtzeitig eingeholt, die Anfälligkeit des Instituts für eine Ausnutzung solcher Schwachstellen sollte bewertet und angemessene Maßnahmen für den Umgang mit dem damit einhergehenden Risiko sollten ergriffen werden.

Es sollte ein dokumentiertes Change- und Release Management eingesetzt werden.

37. Gibt es ein Testkonzept für Software-Änderungen?

Entwicklungs-, Test- und Betriebsumgebungen sollten getrennt werden, um das Risiko nicht-autorisierter Zugriffe oder nicht-autorisierter Änderungen an der Betriebsumgebung zu verringern.

Änderungen an betrieblichen Systemen und Anwendungen sollten vor der Freigabe in einer Testumgebung unter Realbedingungen getestet werden.

F. Passwörter und Verschlüsselung

38. Gibt es eine Passwort-Richtlinie?

Eine Passwortrichtlinie sollte definiert und den Mitarbeitern transparent gemacht werden. Hierbei ist darauf zu achten, dass die Umsetzbarkeit der Passwort-Richtlinie durch die IT-Systeme unterstützt wird. Die in der Richtlinie festgelegten Regeln sollten neben dem Aspekt der Sicherheit auf jeden Fall auch den Aspekt der Praktikabilität berücksichtigen. Für Notfälle sollte es Master-Passwörter zu allen kritischen Systemen und Informationen geben. Der Zugriff auf die Master-Passwörter sollte ebenfalls in der Passwort-Richtlinie geregelt sein.

39. Werden Arbeitsplatzrechner bei Verlassen durch entsprechende Maßnahmen gesichert?

Arbeitsplatzrechner sollten bei Verlassen immer durch Bildschirmschoner und Kennwort gesichert werden. Für den Fall, dass ein Mitarbeiter die Abmeldung einmal vergisst, kann ein automatisches Sperren durch das System nach einigen Minuten Inaktivität erzwungen werden. Für Mitarbeiter, die Zugang zu besonders vertraulichen Informationen haben, sollten weitere Schutzmaßnahmen wie beispielsweise die Anmeldung über eine Zwei-Faktor-Authentifizierung per Smartcard oder ähnlicher Token ergriffen werden.

40. Wird die Passwort-Richtlinie systemseitig umgesetzt?

Die Passwort-Richtlinie sollte von den IT-Systemen umgesetzt werden, sodass Passwörter, die der Richtlinie widersprechen, nicht verwendet werden können. Passwörter sollten regelmäßig gewechselt werden.

41. Sind die Mitarbeiter in der Wahl sicherer Passwörter geschult?

Mitarbeiter sollten in der Wahl sicherer und der Passwort-Richtlinie entsprechender Passwörter geschult werden. Insbesondere sollte ihnen erklärt werden, warum gewisse Regeln wie Mindestlänge, Passwortgültigkeit und Passwortkomplexität einzuhalten sind und es sollten ihnen einfache Regeln zur Erstellung ausreichend komplexer, aber trotzdem einfach zu merkender Passwörter bereitgestellt werden. Gegebenenfalls ist auch der Einsatz von sicheren Passwortspeicher-Apps ratsam.

42. Werden vertrauliche Daten und besonders gefährdete Systeme wie Notebooks oder Datensicherungsträger ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt?

Notebooks und Datensicherungsträger sollten mit einem besonderen Schutz versehen werden, welcher die Daten auch dann noch schützt, wenn ein Unbefugter physischen Zugriff auf das Gerät hat. Am besten schützt man die gespeicherten Daten durch Verschlüsselung. Speziell bei Notebooks beachte man, dass eine (integrierte) Festplattenverschlüsselung das Gerät nur im ausgeschalteten Zustand schützt. Tiefergehenden Schutz auch gegen ausgeklügelte Angriffe wie beispielsweise die so genannte "Cold-Boot-Attacke" bieten Datei- und Ordnerverschlüsselungsprogramme.

G. IT-Notfallvorsorge

43. Gibt es einen Notfallplan mit Anweisungen und Kontaktadressen?

Für Notfälle, welche den Ausfall eines oder mehrerer kritischer IT-Systeme zur Folge haben, sollte es einen Notfallplan geben. In diesem sollten alle Prozeduren beschrieben sein, um die negativen Folgen des Systemausfalls so gering wie möglich zu halten. Insbesondere sollten in dem Plan alle Personen mit Kontaktadressen verzeichnet sein, die in einem Notfall informiert werden müssen und die für die Durchführung von Notfallmaßnahmen verantwortlich sind. Die Verantwortung zur Erstellung und Pflege des Notfallplans sollte eindeutig definiert sein. Falls im eigenen Unternehmen keine Erfahrung bei der Erstellung von Notfallplänen vorliegt, sollte die Hilfe von externen Experten in Anspruch genommen werden.

44. Kennen die Verantwortlichen den Notfallplan?

Alle im Notfallplan verzeichneten verantwortlichen Personen, sowie alle Personen, welche im Notfall die Information der Verantwortlichen übernehmen sollen, müssen den Notfallplan kennen bzw. müssen auf den Notfallplan jederzeit Zugriff haben und müssen schnell darin die notwendigen Informationen finden und umsetzen können.

45. Ist der Notfallplan gut zugänglich?

Der Notfallplan sollte jederzeit für alle verantwortlichen Personen gut zugänglich sein. Dabei ist darauf zu achten, dass die Verfügbarkeit des Notfallplans nicht selbst vom Ausfall eines IT-Systems gefährdet sein darf. Mehrfache Aufbewahrung des Plans empfiehlt sich. Alle verantwortlichen Personen müssen über den Aufbewahrungsort des Notfallplans informiert und mit dem Umgang mit dem Notfallplan vertraut sein.

46. Werden die relevanten Notfallsituationen behandelt?

Der Notfallplan muss alle kritischen IT-gestützten Geschäftsprozesse behandeln. Beim Aufstellen des Notfallplans sollten die Notfallsituationen mit einer Risikobewertung versehen werden, in der die Eintrittswahrscheinlichkeiten der Notfälle und die Auswirkungen im Falle des Eintretens abgeschätzt werden. Zur Analyse der Kritikalität der Geschäftsprozesse und zur Risikobewertung kann es sich empfehlen, externe Hilfe in Anspruch zu nehmen.

47. Wird der Notfallplan regelmäßig getestet?

Ein Notfallplan sollte regelmäßig, beispielsweise jährlich, anhand gezielter Systemabschaltungen, getestet und die Ergebnisse der Wiederanlaufprozeduren bewertet werden. Anhand der Ergebnisse sollte der Notfallplan auf sich ändernde Geschäftsprozesse oder auf sich ändernde Risikosituationen angepasst werden. Bei wesentlichen Änderungen in den Geschäftsprozessen oder der Risikobewertung sollte der Notfallplan auch außerhalb der Notfallübungen auf den aktuellen Stand gebracht werden.

H. Datensicherung

48. Gibt es eine Backup-Strategie?

Es sollte eine Sicherungs-/Backup-Leitlinie erstellt werden, in der die Anforderungen des Instituts in Bezug auf die Sicherung von Daten, Software und Systemen festgelegt sind. Im Rahmen der Betriebsverfahren sollten die Durchführung von Sicherungen überwacht und Maßnahmen bei fehlgeschlagenen geplanten Sicherungen festgelegt werden, um die Vollständigkeit der Backups nach der Sicherungsrichtlinie zu gewährleisten.

49. Ist festgelegt, welche Daten wie lange gesichert werden?

In der Sicherungs-/Backup-Leitlinie sind außerdem die Aufbewahrungs- und Schutzanforderungen dargelegt.

Der Aufbewahrungszeitraum für wichtige geschäftliche Informationen sollte unter Berücksichtigung von betrieblichen oder gesetzlichen Anforderungen zur dauerhaften Aufbewahrung von Archivkopien bestimmt werden.

50. Bezieht die Sicherung auch tragbare Computer und nicht vernetzte Systeme mit ein?

Entsprechende Regelungen sollten in der Sicherungs-/Backup-Leitlinie definiert werden.

51. Werden Datensicherungen regelmäßig kontrolliert?

Die Sicherungsmedien sollten regelmäßig überprüft werden, um sicherzustellen, dass auf sie im Notfall Verlass ist. Dies sollte zusammen mit einer Überprüfung der Wiederherstellungsverfahren in Verbindung mit einer Überprüfung der für die Wiederherstellung benötigten Zeit erfolgen.

Bei der Überprüfung der Wiederherstellungsfunktion sollten die gesicherten Daten auf ein separates Prüfmedium zurückgespielt werden, statt das Ursprungsmedium zu überschreiben, um im Fall eines fehlgeschlagenen Sicherungs- oder Wiederherstellungsprozesses eine irreparable Beschädigung oder sogar einen Verlust der Daten zu vermeiden.

Es sollten Ereignisprotokolle angefertigt, aufbewahrt und regelmäßig geprüft werden, in denen Aktivitäten der Benutzer, Ausnahmen, Fehler und Informationssicherheitsereignisse aufgezeichnet werden.

52. Ist der Zugriff auf Datensicherungsträger geregelt?

Die Sicherungs-/Backup-Leitlinie sollte den Zugriff auf die Datensicherungsträger regeln.

Ereignisprotokolle können sensible Daten und personenbezogene Informationen enthalten. Daher sollten entsprechende Maßnahmen zum Schutz personenbezogener Daten ergriffen werden.

Die Systemadministratoren sollten keine Befugnis besitzen, die Protokollierung ihrer eigenen Aktivitäten zu löschen oder zu deaktivieren.

53. Sind Sicherungs- und Rücksicherungsverfahren dokumentiert?

Eine entsprechende Dokumentation sollte angefertigt und für Notfälle zugriffsbereit abgelegt werden. Zusätzlich sollten physische Kopien (Papier) der Rücksicherungsverfahren bereitgestellt werden.

I. Infrastruktursicherheit

54. Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung oder Stromausfall?

Es muss sichergestellt werden, dass Daten gegen zufällige Zerstörung oder Verlust geschützt werden. Daher ist ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung oder Stromausfall notwendig. Wichtige IT-Systeme sollten ausschließlich mit unterbrechungsfreien Stromversorgungs-Anlagen mit Überspannungsschutz ausgestattet werden. Können Kühl- und Feuerlöschsysteme aufgrund von baulichen Vorschriften und Gegebenheiten nicht installiert werden, sollte ein entsprechendes Überwachungs- und Alarmierungssystem eingerichtet werden. Darüber hinaus sollte die Verfügbarkeit von Daten und IT-Systemen durch Redundanzen und Backups sichergestellt werden.

55. Ist der physische Zutritt zu wichtigen IT-Systemen und Räumen geregelt?

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, auf denen insbesondere personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Der Zutritt zu den wichtigen IT-Systemen und Räumen sollte geregelt, dokumentiert und überwacht werden.

56. Werden Besucher, Handwerker, Servicekräfte etc. begleitet bzw. beaufsichtigt?

Die Anlage zu § 9 Satz 1 BDSG schreibt vor, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Daher sollten Besucher, Handwerker, Servicekräfte während des Aufenthaltes in den Räumlichkeiten des Unternehmens begleitet bzw. beaufsichtigt werden. Entsprechende Aufenthalte von Externen sollten dokumentiert werden.

57. Besteht ein ausreichender Schutz vor Einbruch, Diebstahl und Sabotage?

Ein präventiver Schutz vor Einbruch, Diebstahl und Sabotage sichert bedeutsame Unternehmenswerte und Daten. Die Durchführung einer Risikoanalyse und die Erstellung eines umfassenden Sicherheitskonzeptes mit eindeutiger Zielsetzung werden für den Schutz von Gebäuden, Räumen und Anlagen als erste Maßnahme empfohlen.

Falls die eigenen Räumlichkeiten nicht ausreichend geschützt werden können, wird empfohlen, IT-Systeme mit personenbezogenen Daten in externe zertifizierte Rechenzentren auszulagern.

58. Ist der Bestand an Hard- und Software in einer Inventarliste erfasst?

Der gesamte Bestand an Hard- und Software sollte in einer Inventarliste erfasst und regelmäßig aktualisiert werden. In vielen Fällen können diese Informationen auch aus den Buchhaltungsdaten entnommen werden. Zusätzlich sollte eine Liste über Software-Lizenzen und deren Laufzeiten gepflegt werden. Eine direkte Verknüpfung mit der Verantwortlichkeit über die entsprechende Systemressource verringert die Reaktionszeit, falls es zu Ausfällen der Hardware oder Problemen mit der Software kommt.

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Engineer for System Security" (T.E.S.S.) sowie des Qualitätszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
http://www.teletrust.de

TeleTrusT
Pioneers in IT security.


TeleTrusT
Pioneers in IT security.