PSW GROUP

ISA+
Informations-Sicherheits-Analyse

ISA+ Fragenkatalog

Informations-Sicherheits-Analyse für kleine & mittlere Unternehmen

CISSP® | Certified Information Systems Security Professional

CISA | Certified Information Systems Auditor

CISM | Certified Information Security Manager

ISMS | IRCA ISO 27001 ISMS | (Lead) Auditor

1. Organisatorisch

u. a. zu Richtlinien, Anweisungen, Schulung & Verantwortlichkeiten

1.1.1. Gibt es eine dedizierte Leitlinie zur Informationssicherheit und ist sie von der Geschäftsführung unterschrieben?

Die Leitlinie zur Informationssicherheit soll kein umfängliches Konzeptpapier zur Informationssicherheit sein. Sie repräsentiert den hohen Stellenwert der Informationssicherheit für das Unternehmen und muss die vollständige Unterstützung der Unternehmensleitung der für die Umsetzung der Leitlinie entsprechend notwendigen Maßnahmen bekräftigen. Die Informationssicherheitsleitlinie sollte mindestens unternehmensweit so kommuniziert werden, dass ihre Bedeutung den Anwendern ersichtlich ist, jeder davon Betroffene darauf Zugriff hat und sie verstehen kann.

Die Leitlinie sollte folgende Punkte enthalten (angelehnt an BSI IT-Grundschutz):

- Der Stellenwert der Informationssicherheit & die Bedeutung der wesentlichen Informationen, Geschäftsprozesse & IT des Unternehmens
- Die Sicherheitsziele und der Bezug der Sicherheitsziele zu den Geschäftszielen und Aufgaben des Unternehmens
- Die Kernelemente der Sicherheitsstrategie
- Bereitschaft der Unternehmensleitung zur Durchsetzung der Leitlinie und Aussagen zur Umsetzungs-Kontrolle
- Beschreibung der Organisationsstruktur für die Umsetzung des Sicherheitsprozesses
- Unterschrift der Geschäftsleitung

1.1.2. Gibt es einen Beauftragten für Informationssicherheit?

Für die wirksame Umsetzung und vor allem für die regelmäßige Überprüfung und Anpassung der Leitlinie zur Informationssicherheit ist die zentrale Rolle eines Beauftragten für Informationssicherheit unerlässlich. Aufgrund der durchaus vorhandenen Anforderungen an Sicherheits-Know-how, Koordinations-/ Kommunikations-Fähigkeiten und auch Fähigkeit zur Schulung und Beratung sollte der entsprechende Beauftragte nach Eignung ausgewählt werden. Der Beauftragte muss die explizite Unterstützung durch die Leitung des Unternehmens haben.

In kleinen Unternehmen kann diese Aufgabe auch vom IT-Beauftragten oder dem Administrator wahrgenommen werden. Zum Teil wird auch der Datenschutzbeauftragte zum IS-Beauftragten bestellt und umgekehrt. Grundsätzlich ist auch eine Beauftragung eines externen Dienstleisters möglich.

1.1.3. Ist der Beauftragte für die Aufgabe geeignet?

Die Aufgabenstellung des Beauftragten für Informationssicherheit umfasst die Initiierung, Koordination und Dokumentation der Entwicklung, Umsetzung, Kontrolle und Fortschreibung des Regelwerks zur Informationssicherheit. Er ist bei der Einführung neuer Verfahren/ Prozesse, Systeme oder Regeln sowie bei der Änderung bestehender Verfahren/Prozesse, Systeme oder Regeln frühzeitig zu beteiligen. Auch ist es seine Aufgabe, intern (Leitung und Mitarbeiter) und extern (z. B. Partner/Kunden) zu Fragen der Informationssicherheit mit Bezug auf die Leitlinie des Unternehmens zu beraten und zu sensibilisieren.

Gemessen an dieser Aufgabenstellung sollte die Eignung des Beauftragten verifiziert und gegebenenfalls durch Schulungen oder externe Beratung hergestellt werden. Diese Aufgaben können als Nebentätigkeit durchgeführt werden. Vom Beauftragten für Informationssicherheit wird eine einschlägige Aus- oder Fortbildung erwartet.

1.1.4. Ist ein notwendiger Datenschutzbeauftragter bestellt und hat dieser ein betriebliches Datenschutzkonzept erstellt?

Das Bundesdatenschutzgesetz fordert unter bestimmten Voraussetzungen die Bestellung eines betrieblichen Datenschutzbeauftragten. Diese Funktion kann auch von einem externen Dienstleister gestellt oder vom IS-Beauftragten wahrgenommen werden.

In kleinen und mittleren Unternehmen (KMU) kann die Behandlung der wichtigsten Rahmendaten der Datenschutzorganisation auch in einem zentralen Sicherheitskonzept zur Informationssicherheit (PA 1.1.7) abgebildet werden.

1. Organisatorisch

u. a. zu Richtlinien, Anweisungen, Schulung & Verantwortlichkeiten

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

Eine vollständige Aufstellung zu Hardware, Software, Anwendungen, Systemen, Netzen etc. ist die Grundvoraussetzung für diesen Überblick. Aktuelle Netzpläne sollten vorhanden sein. Änderungen in der Umgebung sollten regelmäßig dokumentiert werden. Eine Einschätzung der Eintrittswahrscheinlichkeit von Bedrohungen und in der Folge eine angemessene Risikobewertung (Risikoanalyse, Schutzbedarf) sollte durch den Netzwerkpartner und interne Mitarbeiter unterstützt, aber nicht in der Gesamtheit selbst durchgeführt werden, um Interessenskonflikte auszuschließen und die Objektivität einer Bewertung zu sichern.

1.1.6. Gibt es Checklisten, was beim Eintritt neuer Mitarbeiter und beim Austritt von Mitarbeitern zu beachten ist?

Checklisten sind für die vollständige Umsetzung von Sicherheitsprozessen notwendig. Sie müssen Punkte enthalten wie z. B. Kenntnisnahme eines neuen Mitarbeiters zur Leitlinie und zu Anweisungen für die konkrete Umsetzung von Informationssicherheit im Unternehmen (z. B. private Internetnutzung am Arbeitsplatz, Passwort-Richtlinie etc.), Vergabe und Entzug von Zugangs-/Zutritts-Berechtigungen, Nutzerrechten, Schlüssel-Rückgabe, Umgang mit Benutzerdaten usw.

1.1.7. Gibt es ein Konzept zur Informationssicherheit?

In kleinen und mittleren Unternehmen (KMU) kann die Behandlung der wichtigsten Rahmendaten in einem zentralen Sicherheitskonzept abgebildet werden. Es müssen alle wichtigen Themen enthalten sein, wie z. B. Virenschutz, Datensicherung, Notfallmaßnahmen etc. Sicherheitskonzepte enthalten noch keine detaillierten Beschreibungen zur technischen Umsetzung. Sie dienen der Richtungsgebung für Handlungsanweisungen sowie zur Sensibilisierung und Schulung aller Mitarbeiter. So muss enthalten sein, welche Pflichten Mitarbeiter/Nutzer haben, aus welchen Gründen Maßnahmen durchgeführt werden und welche Prozesse implementiert sind. Vorbeugungs-Maßnahmen, Schadens-Szenarien, Verhaltensregelungen, allgemeines Wissen zu Bedrohungen sollten im Sicherheitskonzept vermittelt werden.

1.2.1. Gibt es Maßnahmen, welche die Informationssicherheit im Unternehmen gewährleisten?

Technische Maßnahmen zur IT-Sicherheit sind essentiell für die Informationssicherheit, reichen jedoch bei weitem alleine nicht aus. Für eine vollständige Umsetzung muss Informationssicherheit als laufender Prozess gesehen werden, den es ständig zu verbessern gilt. Dies betrifft nicht nur IT-Mitarbeiter, sondern alle Personen im Unternehmen.

Maßnahmen sind daher auch z. B.:
- Regelmäßige Schulung aller Mitarbeiter zu Themen der Informationssicherheit
- Aktuelle Information zu Bedrohungen
- Sensibilisierung der Mitarbeiter (z. B. um Phishing-Angriffe zu verhindern)
- Fortlaufende Bekräftigung der Wichtigkeit von Informationssicherheit für das Unternehmen

1.2.2. Verfügen alle Mitarbeiter über ausreichend Kenntnisse, um Informationssicherheit zu gewährleisten?

Hiermit sind nicht (nur) die IT-Mitarbeiter gemeint. Diese sollten natürlich insbesondere zu technischen Themen der Informationssicherheit fortlaufend geschult werden. Wichtig ist aber auch, dass normale Anwender über Basis-Wissen zu IT und Informationssicherheit über den normalen Gebrauch von Systemen und Anwendungen hinaus verfügen. Dies kann durch regelmäßige Schulungen und durch interne Multiplikatoren, wie z. B. den Informationssicherheitsbeauftragten, erreicht werden. Regelungen sowie deren Änderungen sind den Mitarbeitern zu kommunizieren.

1.2.3. Werden alle Mitarbeiter angehalten, Sicherheitsvorfälle zu melden?

Es sollte ein Prozess (Ansprechpartner, Kommunikationsweg) bekannt gemacht sowie auf die Verpflichtung der Mitarbeiter hingewiesen werden, Sicherheitsvorfälle zu melden. Um Klarheit zu schaffen, welche Vorfälle zu melden sind, sollte der Mitarbeiter über Schulungsmaßnahmen für ungewöhnliche Vorgänge sensibilisiert werden und den Mitarbeitern die Wichtigkeit der Meldung bewusst gemacht werden. Dies betrifft auch Bereiche über die IT-Sicherheit hinaus, wie z. B. Zutritts-Regelungen zu Räumlichkeiten des Unternehmens.

1. Organisatorisch

u. a. zu Richtlinien, Anweisungen, Schulung & Verantwortlichkeiten

1.2.4. Werden die Systeme bei Verlassen mit Bildschirmschoner und Kennwort gesichert?

Hier ist eine explizite Handlungsanweisung und eine flankierende Schulungsmaßnahme (warum ist dies nötig?) hilfreich. Automatische Sperrung des Rechners bzw. Aktivierung des Kennwortschutzes bei Inaktivität sollte so eingerichtet werden, dass sie die normale Arbeit des Nutzers nicht übermäßig behindert (z. B. automatische Sperrung nach 5 Minuten Inaktivität).

1.2.5. Gibt es eine Passwortrichtlinie?

Den Nutzern muss bewusst gemacht werden, dass mit der Stärke und sorgfältigen Behandlung der Passwörter die Sicherheit der Daten und Informationen direkt zusammenhängt. Ein leicht zu erratendes Passwort oder ein Passwort für eine Vielzahl verschiedener Anwendungen reduziert die Sicherheit von IT-Systemen erheblich. In der Passwortrichtlinie sollte festgelegt und den Nutzern konkret bewusst gemacht werden, wie Passwörter gestaltet sein müssen, wie mit diesen umgegangen wird (keine Weitergabe etc.), wie oft diese gewechselt werden müssen etc.

Passwörter sollten regelmäßig geändert werden und nicht auf älteren Passwörtern basieren dürfen. Standard-Passwörter für den Zugang zu Systemen (z. B. Router) müssen umgehend geändert werden.

1.2.6. Werden Festlegungen der Passwortrichtlinie technisch erzwungen?

In Netzwerk-Domain-Umgebungen kann eine Passwortrichtlinie technisch z. B. über den Server und die Domain-Controller erzwungen werden. Diese Maßnahme sollte unbedingt umgesetzt werden, da eine Richtlinie bzw. Handlungsanweisung alleine noch zu häufig von den Nutzern umgangen wird. Diese Administrationsvorgänge sollten nur von Spezialisten vorgenommen werden. Für den Zugang zu besonders schutzbedürftigen Informationen und Systemen sollten starke Authentifizierungsmaßnahmen technisch implementiert werden (z. B. SmartCard, Biometrie, 2-Faktor-Authentisierung).

1.3.1. Ist die private Nutzung von E-Mail und Internet im Unternehmen klar geregelt und existieren Merkblätter oder Hinweise zur sicheren Nutzung dieser Dienste?

Ist eine Regelung nicht vorhanden, sollte das Unternehmen sich über die gesetzlichen Bestimmungen informieren und individuell für sich die passende Regelung festlegen. Diese sollte schriftlich fixiert werden und den Mitarbeitern in Zusatzvereinbarungen zum Anstellungsvertrag mitgeteilt werden. Existieren noch keine Merkblätter zur sicheren Nutzung von E-Mail und Internet, sollten verständliche Hinweise erarbeitet und jedem Mitarbeiter bekannt gemacht werden. Diese sollten mit Beispielen aus der Praxis angereichert werden. Unterstützung kann sich das Unternehmen vom eigenen Datenschutzbeauftragten oder IT-Sicherheitsexperten einholen. Auch eine Schulung der Mitarbeiter in diesem Bereich minimiert die Risiken.

1.3.2. Sind die Browser und E-Mail-Clients auf eine sinnvolle Sicherheitsstufe konfiguriert?

Das Unternehmen sollte eine Liste führen, welcher Mitarbeiter mit welchem Endgerät welche Browserfunktionen für seine Tätigkeiten benötigt. Z. B. ist Java wirklich bei jedem notwendig? Genauso wird bei den E-Mail Clients verfahren. Hier sind die Spam-Einstellungen, erlaubte Anhänge usw. zu beachten. Danach werden die Sicherheitsstufen an den Endgeräten eingerichtet und dokumentiert.

1.3.3. Erfolgt die Konfiguration einheitlich und kann sie nicht von den Nutzern geändert werden?

Nach der Abarbeitung von Punkt 1.3.2. ist zu prüfen, ob eine einheitliche Konfiguration an allen Endgeräten umgesetzt werden kann. Unabhängig davon sollte sichergestellt sein, dass die Benutzerrechte so eingerichtet sind, dass der Anwender die definierten und eingerichteten Sicherheitsstufen nicht selbst umstellen kann.

2. Technisch

u. a. zu vorhanden IT-Systemen, Datensicherung, Notfallvorsorge

2.1.1.1. Sind nicht benötigte Programme und Dienste auf Endgeräten deinstalliert bzw. deaktiviert und individuelle Erweiterungen abgesichert?
Sind auf dem Rechner nicht mehr benötigte Programme und Dienste vorhanden, sollten diese vom Administrator deinstalliert werden. Veraltete Programme und Dienste erhalten keine Updates mehr und aufkommende Sicherheitslücken können von Angreifern ausgenutzt werden.
2.1.1.2. Sind auf den Servern und aktiven Netzwerkgeräten alle unnötigen Programme deinstalliert und Dienste deaktiviert?
Sind auf den Servern nicht mehr benötigte Programme und Dienste vorhanden, sollten diese vom Administrator deinstalliert werden. Veraltete Programme und Dienste erhalten keine Updates mehr und aufkommende Sicherheitslücken können von Angreifern ausgenutzt werden.
2.1.1.3. Sind die eingesetzten Systeme (Betriebssysteme, Software, Browser etc.) auf dem neuesten Softwarestand und werden alle zutreffenden Sicherheitsupdates für die gesamte Software zeitnah eingespielt?
Bei Betriebssystemen, Software, Browsern etc. können über einen längeren Zeitraum Sicherheitslücken entstehen. Um diese zu schließen, sollten Betriebssysteme etc. immer auf den neuesten Stand gebracht werden. Hierzu sollte der Administrator ein Patch- bzw. Updatemanagement betreiben.
2.1.1.4. Ist der Zugang zum WLAN abgesichert?
Sollte WLAN im Unternehmen zur Anwendung kommen, ist unbedingt auf eine Verschlüsselung zu achten. Bei nicht verschlüsselten Netzen können Angreifer sicherheitskritische Daten wie Passwörter etc. auslesen und somit an Unternehmensdaten kommen. Um dies zu verhindern, sollte bei der Verschlüsselungsmethode der gängigen Standard WPA2 und ein Passwort mit mindestens 13 Stellen verwendet werden.
2.1.1.5. Ist geregelt, welche Funktionen jeder Mitarbeiter nutzen darf und auf welche Datenbestände er zugreifen darf?
Sind die Rollen und Profile für Mitarbeiter angelegt, sollten diese noch durch entsprechende Rechte eingeschränkt werden. In diesen Rechten wird definiert, welche Funktionen oder auf welche Datenbestände ein Mitarbeiter Zugriff hat. Bevor die Rollen und Profile für die Mitarbeiter angelegt werden können, ist erst zu definieren, welche Funktionen oder auf welche Datenbestände ein Mitarbeiter Zugriff hat.
2.1.1.6. Sind Rollen definiert und allen Systembenutzern entsprechend zugeordnet?
Für jeden Mitarbeiter sollten entsprechende Rollen und Profile für die tägliche Arbeit an etwaigen Systemen eingerichtet werden. So ist es besser nachzuvollziehen, wer an einem Rechner arbeitet und welche Rechte er hierzu benötigt.
2.1.1.7. Sind die Rechte entsprechend eingeschränkt?
Je nach Arbeitsumfeld sollten entsprechende Rechte definiert werden. Ein Administrator sollte alle Rechte besitzen, um beispielsweise Wartungsarbeiten etc. durchführen zu können. Ein Sachbearbeiter sollte auf Buchhaltungsdaten keine Zugriffsrechte erhalten, sondern nur die Buchführung selbst oder der Geschäftsführer.

2. Technisch

u. a. zu vorhanden IT-Systemen, Datensicherung, Notfallvorsorge

2.1.2.1. Sind Virenscanner auf den eingesetzten Systemen vorhanden?
Um Sicherheitsrisiken zu vermeiden, sollte auf jedem System ein Virenscanner installiert sein. Gute Virenscanner erhält man bereits als Freeware; für das Unternehmen sollten jedoch Lizenzen erworben werden. Die Virenscanner sollten in regelmäßigen Abständen das System auf Viren, Trojaner etc. scannen.
2.1.2.2. Werden regelmäßig in kurzen Abständen Aktualisierungen des Virenschutzes vorgenommen?
Die Hersteller bringen regelmäßig Updates für ihre Virenscanner heraus, die meist automatisch von der Software installiert werden. Diese Updates sind wichtig, da täglich neue Viren, Trojaner etc. bekannt werden.
2.1.2.3. Gibt es ein Merkblatt zum Schutz vor Schadsoftware?
Der Informationssicherheitsbeauftragte muss für die Belegschaft eine Richtlinie bzw. ein Merkblatt erstellen, in der die Mitarbeiter in Bezug auf Schutz vor Schadsoftware sensibilisiert werden. Hierzu empfehlen sich auch regelmäßige Schulungen für die Mitarbeiter.
2.1.2.4. Gibt es ein Merkblatt zum Verhalten beim Eintreten eines Vorfalls?
Mitarbeiter sollten über Richtlinien, Regelungen oder Merkblätter auf den Eintritt eines Vorfalls vorbereitet werden. In diesen Richtlinien sollte der Mitarbeiter darüber informiert werden, welche Anhaltspunkte er an den Informationssicherheitsbeauftragten weitergeben soll. Generell sollten Mitarbeiter jeglichen Vorfall beim Administrator umgehend melden, um weiteren Schaden zu vermeiden.
2.1.2.5. Sind die Merkblätter zum Schutz vor Schadsoftware und zum Verhalten beim Eintreten eines Vorfalls allen Mitarbeitern bekannt?
Über Schulungen sollten den Mitarbeitern die Regelungen, Merkblätter und Richtlinien näher gebracht werden. Hierbei kann auf unverständliche Punkte in den Regelungen, Merkblättern und Richtlinien oder auf Fragen der Mitarbeiter eingegangen werden.
2.1.3.1. Ist das Unternehmensnetzwerk durch eine Firewall geschützt?
Ist im Unternehmen keine Firewall vorhanden, sollte der Informationssicherheitsbeauftragte bzw. der Administrator umgehend eine Firewall installieren. Ohne Firewall können Angreifer gezielt auf Unternehmensdaten zugreifen. Passende Lösungen zum Thema „Firewall für Kleinunternehmen“ sind in einer Vielzahl vorhanden.
2.1.3.2. Werden Konfiguration und Funktionsfähigkeit der Firewall regelmäßig kritisch überprüft und kontrolliert?
Um Sicherheitslücken ausfindig zu machen, sollte der Administrator regelmäßig Penetrationstests durchführen. Auch das regelmäßige Aufspielen von neuen Updates ist hier von großer Bedeutung.
2.1.4.1. Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung, Stromausfall und Einbruch?
Um einen angemessenen Schutz der IT-Systeme zu gewährleisten, sollten sich Räume oder Gebäudeteile, in denen IT-Systeme vorhanden sind, in einer sicheren Umgebung befinden. Hierbei ist auch auf Brandschutzvorschriften oder auf Gefahrenlagen wie Wasserschäden oder Blitzeinschlag zu achten. Abhilfe schaffen z. B. Brandmelder, Wassermelder sowie Blitzableiter. Gegen Diebstahl sollten Einbruchsmelder installiert werden.

2. Technisch

u. a. zu vorhanden IT-Systemen, Datensicherung, Notfallvorsorge

2.1.4.2. Ist der Zutritt zu IT-Systemen und Räumen geregelt?

Ein Zutritt zu wichtigen IT-Systemen sollte generell nur der Administrator sowie die Geschäftsleitung besitzen. Räume mit Servern oder anderen wichtigen IT-Systemen sollten stets abgeschlossen werden und es sollte darauf geachtet werden, wer derartige Räume betreten darf. Für diesen Zweck sollte eine Zutrittsregelung und -kontrolle festgelegt werden.

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

Externer Besuch sollte aufgrund des Datenschutzes und zu Präventivmaßnahmen immer begleitet bzw. beaufsichtigt werden. Wichtige Räumlichkeiten sollten daher abgeschlossen werden und es ist darauf zu achten, dass z. B. Handwerker nur Zutritt zu unbedenklichen Räumen haben.

2.2.1. Gibt es geeignete Vertretungsregelungen für Verantwortliche und sind die Vertreter mit ihren Aufgaben vertraut?

Für alle wesentlichen Geschäftsprozesse und Aufgaben müssen tragfähige Vertretungsregelungen vorhanden sein. Diese müssen regelmäßig aktualisiert werden. Die Übernahme von Aufgaben im Vertretungsfall setzt voraus, dass der Verfahrens- oder Projektstand hinreichend dokumentiert ist.

Es muss festgelegt sein, welcher Aufgabenumfang im Vertretungsfall von wem wahrgenommen werden soll. Es muss überprüft werden, wie der Kenntnisstand des Vertreters für die zu übernehmende Aufgabe ist, evtl. muss der Vertreter vorab entsprechend geschult werden.

Siehe dazu beispielsweise IT-Grundschutz-Maßnahme „M 3.3 Vertretungsregelungen“.

2.2.2. Sind die wichtigsten Passwörter für Notfälle sicher hinterlegt?

Passwörter, die zur Konfiguration und Wartung benötigt werden, sollten für Notfälle sicher hinterlegt werden. Bei der Passwort-Hinterlegung sind die benötigten aktuellen Passwörter durch jeden Mitarbeiter an einer geeigneten Stelle (z. B. im Sekretariat in einem Safe in einem geschlossenen Umschlag) zu hinterlegen. Bei jeder Änderung eines der Passwörter ist dieses zu aktualisieren. Es darf kein Passwort dabei vergessen werden.

Siehe dazu beispielsweise IT-Grundschutz-Maßnahme „M 2.22 Hinterlegen des Passwortes“.

2.2.3. Gibt es eine Liste mit Kontaktadressen für Notfälle?

Erstellung eines Notfallplans mit Verantwortlichkeiten, Kontaktadressen aller Mitarbeiter mit spezifischen Aufgaben in der Notfallbewältigung sowie von externen Kontaktpersonen, wie Kooperationspartner, Dienstleister, Hilfsorganisationen oder Aufsichtsbehörden. Evtl. Bestellung eines Notfallbeauftragten durch die Geschäftsführung.

2.2.4. Gibt es ein Vorgehen bei Systemausfall bzw. Datenverlust (Notfallkonzept)?

Der Ausfall eines IT-Systems kann gravierende Auswirkungen haben. Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind. Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher ist im Rahmen des allgemeinen Datensicherungskonzepts ein entsprechendes Konzept zu erstellen.

2. Technisch

u. a. zu vorhanden IT-Systemen, Datensicherung, Notfallvorsorge

2.2.5. Kennt jeder Mitarbeiter die Liste mit Kontaktadressen sowie das Vorgehen und sind diese gut zugänglich?

Der Notfallplan ist den Mitarbeitern in geeigneter Form bekannt zu geben. Es empfiehlt sich die Bekanntgabe zu dokumentieren. Darüber hinaus sind sämtliche Regelungen in der aktuellen Form an einer Stelle vorzuhalten und bei berechtigtem Interesse zugänglich zu machen.

Siehe dazu beispielsweise IT-Grundschutz-Maßnahme „M 6.115 Integration der Mitarbeiter in den Notfallmanagement-Prozess“.

2.2.6. Werden Datenbestände regelmäßig gesichert?

Zur Vermeidung von Datenverlusten müssen regelmäßige Datensicherungen durchgeführt werden. In den meisten Rechnersystemen können diese weitgehend automatisiert erfolgen. Es sind Regelungen zu treffen, welche Daten von wem wann gesichert werden. Empfehlenswert ist die Erstellung eines Datensicherungskonzepts.

Siehe dazu beispielsweise IT-Grundschutz-Maßnahme „M 6.32 Regelmäßige Datensicherung“.

2.2.7. Werden die Datensicherungen geschützt aufbewahrt?

Der Zugriff auf diese Datenträger darf nur befugten Personen möglich sein, so dass eine Entwendung ausgeschlossen werden kann. Der Aufbewahrungsort muss auch die klimatischen Bedingungen für eine längerfristige Aufbewahrung von Datenträgern gewährleisten. Für den Katastrophenfall müssen die Backup-Datenträger räumlich getrennt vom Rechner aufbewahrt werden, wenn möglich in einem anderen Brandabschnitt.

Siehe dazu beispielsweise IT-Grundschutz-Maßnahme „M 6.20 Geeignete Aufbewahrung der Backup-Datenträger“.

2.2.8. Werden Informationen und Datenträger klassifiziert und dementsprechend gehandhabt?

Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden. Die Backup-Medien müssen an einem sicheren Ort, möglichst außerhalb des Unternehmens bzw. des Dienstgebäudes, aufbewahrt werden. Der Aufbewahrungsort sollte zudem hinreichend gegen Elementarschäden wie Feuer, Wasser und Ähnliches geschützt sein. Der Zugriff auf diese Datenträger darf nur befugten Personen möglich sein, so dass eine Entwendung ausgeschlossen werden kann.

2.2.9. Werden Wartungsaufgaben durch geeignetes Personal durchgeführt?

Das Wartungs- und Administrationspersonal benötigt detaillierte Kenntnisse über die eingesetzten IT Komponenten. Daher sollte es mindestens so weit geschult werden, dass alltägliche Administrationsarbeiten selbst durchgeführt, einfache Fehler selbst erkannt und behoben, Datensicherungen regelmäßig selbsttätig durchgeführt, die Eingriffe von externem Wartungspersonal nachvollzogen und Manipulationsversuche oder unbefugte Zugriffe auf die Systeme erkannt und rasch behoben werden können. Entsprechende Schulungen werden in der Regel von den Herstellern der IT-Systeme bzw. TK-Anlagen angeboten.

2.2.10. Werden vertrauliche Informationen vor Wartungs- oder Reparaturarbeiten von Datenträgern oder IT-Systemen geschützt?

Für Wartungs- und Reparaturarbeiten im Hause, vor allem wenn sie durch Externe durchgeführt werden, sind Regelungen über deren Beaufsichtigung zu treffen: während der Arbeiten sollte eine fachkundige Kraft die Arbeiten soweit beaufsichtigen, dass sie beurteilen kann, ob während der Arbeit unautorisierte Handlungen vollzogen werden. Weiterhin ist zu überprüfen, ob der Wartungsauftrag im vereinbarten Umfang ausgeführt wurde. Der Zugriff auf Daten durch den Wartungstechniker ist soweit wie möglich zu vermeiden.

Siehe dazu beispielsweise IT-Grundschutz-Maßnahme „M 2.4 Regelungen für Wartungs- und Reparaturarbeiten“.

3. Rechtlich

u. a. zu Compliance und Leistungen Dritter

3.1.1. Gibt es einen Überblick über vertragliche und gesetzliche Anforderungen an die Informationsverarbeitung?

Für Unternehmen, unabhängig von der Unternehmensgröße, gelten heutzutage diverse gesetzliche Regelungen, welche die Informationstechnologie direkt betreffen bzw. indirekt, da die Informationstechnologie in fast alle Bereiche der Unternehmensprozesse eingebunden ist. Zu nennen sind dabei typische bekannte Regelungen aus der Abgabenordnung hinsichtlich Archivierungsvorschriften sowie die GoBD oder das Bundesdatenschutzgesetz. Für bestimmte Branchen gelten darüber hinaus weitergehende Anforderungen, bspw. für Banken und Finanzdienstleister mit den MaRisk oder im Medizinbereich. Diese Anforderungen können durch privatrechtliche Vertragsgestaltungen erweitert werden (z. B. im Rahmen von Kunden-Lieferanten-Beziehungen, aufgrund der Einbindung in Konzernstrukturen oder durch Auslagerungsvereinbarungen).

Verfügt ein Unternehmen nicht über einen Überblick, welche gesetzlichen und privatrechtlichen Anforderungen direkt oder indirekt an seine Informationsverarbeitung bestehen, sollte eine entsprechende Analyse vorgenommen werden. Diese sollte die Anforderungen aus den klassischen Bereichen Datenschutz, Datensicherheit, Archivierung, Branchennormen, Sonstige (bspw. privatrechtliche Anforderungen) umfassen. Erste Anlaufstellen hierfür können grundsätzlich z. B. Verbände, IHK oder der eigene Steuerberater sein.

3.1.2. Gibt es eine Vorgabe für die Auslagerung von Daten an externe Service-Unternehmen?

Eine Auslagerung von Daten an externe Service-Unternehmen kann Auswirkungen auf interne Prozesse, Konzepte und Schutzniveaus haben. Diese Entscheidung sollte auch immer gegen bestehende Vereinbarungen und Verträge geprüft werden. Für die Auslagerung von Daten sollte deswegen ein verständlicher Prozess zur Prüfung gegen die vorhandenen Rahmenbedingungen eingeführt sein oder es ist die Entscheidung getroffen, auf die Auslagerung von Daten zu verzichten.

3.1.3. Sind den Mitarbeitern und den Informationsempfängern (Dienstleister etc.) die aus der Auslagerung von Daten resultierenden Sorgfaltspflichten bekannt bzw. kommuniziert?

Fehlendes Bewusstsein bei den Mitarbeitern und engen Geschäftspartnern kann über Schulungen sowie Informationsblätter – unter Umständen sogar mit Verpflichtungscharakter in Form von Anweisungen – Abhilfe geschaffen werden. Adressaten außerhalb der direkten Einflusssphäre des Unternehmens sind über entsprechende Vorschriften zu informieren bzw. ggf. über entsprechende vertragliche Regelungen verbindlich zu verpflichten.

3.1.4. Wird geprüft, ob die Anforderungen eingehalten werden?

Wichtiger als die faktische Überprüfung ist die Konzeption eines wirksamen Kontroll-Systems, das aufgrund ablauforganisatorischer Regelungen sicherstellt, dass die Einhaltung der Anforderungen bereits natürlicher Teil der Arbeitsabläufe wird. Dazu sind u. U. Arbeitsabläufe und Zuständigkeiten / Verantwortlichkeiten neu zu organisieren.

3.1.5. Bestehen Regelungen, welche Daten wie lange gespeichert werden müssen bzw. dürfen?

Der Unternehmer muss sich einen Überblick über die in seinem Unternehmen vorhandenen Daten verschaffen. Wo werden Daten erzeugt, wo verarbeitet, wo gespeichert und was beinhalten sie. Auf Basis dieser Analyse kann dann für Datengruppen ein Lebenszyklusmanagement festgelegt werden, das die vorschriftsmäßige Speicherung aber auch Löschung von Daten strukturiert. Ein weiterer Mehrwert dieser Analyse ist, dass das Datensicherungskonzept auf die verschiedenen Lebenszyklen und Prioritäten abgestimmt werden kann und außerdem wichtige Erkenntnisse für das Notfallmanagement hieraus hervorgehen.

In vielen Unternehmen herrscht Unklarheit darüber, welche Daten wie lange gespeichert werden müssen bzw. wann Verpflichtungen bestehen, Daten auch wieder löschen zu müssen. Die typischen Anforderungen zur Datenspeicherung ergeben sich aus betrieblichen Belangen und gesetzlichen Vorschriften, wie der Abgabenordnung und dem HGB hinsichtlich der Archivierungsvorschriften. Aber aus dem Bundesdatenschutzgesetz ergeben sich auch Pflichten, Daten wieder zu löschen und zwar zu bestimmten Zeitpunkten und nicht irgendwann, wenn einmal zufällig Zeit dafür ist.

3. Rechtlich

u. a. zu Compliance und Leistungen Dritter

3.2.1. Gibt es eine Übersicht, in welcher Form Dritte beim IT-Betrieb beteiligt sind bzw. welche externen Leistungen genutzt werden?

Zur Analyse und Identifikation der einbezogenen dritten Parteien sollte eine Matrix der Regel- und Einzeltätigkeiten zur Planung, Implementierung und Aufrechterhaltung der IT-Landschaft des Unternehmens erstellt werden. Eine Orientierung bieten zum Beispiel die Maßnahmen M 2.4, M 2.5, M 2.252 des IT-Grundschutzkataloges des Bundesamtes für Sicherheit in der Informationstechnik. Der IT-Grundschutzkatalog wird vom Bundesamt für Sicherheit in der Informationstechnik gepflegt und ist auf dessen Homepage abrufbar.

Beispiele:

- Wartung der Telefonanlage und TK-Endgeräte• Bereitstellung Internetanschluss / Anbindung
- Wartung und Pflege Archivierungssystem
- Pflege und Wartung der Netzwerkinfrastruktur
- Wartung der EDV Werkssysteme
- Allgemeiner IT Support
- Hardwarewartung (Server)
- Hardwarewartung (Drucker und Multifunktionsgeräte)
- Versorgung mit Ersatzteilen und Verbrauchsmaterial
- Externer Datenschutzbeauftragter
- Reinigungsdienstleistungen / Gebäudereinigung
- Reinigungsdienstleistungen / Glas und Rahmen
- Pflege und Wartung Internetauftritt, CMS- und Newslettersystem

3.2.2. Sind die aus Verträgen resultierenden sicherheitsrelevanten Anforderungen identifiziert und enthalten die eigenen Verträge entsprechende Regelungen?

Damit alle sicherheitsrelevanten Fragenstellungen adäquat berücksichtigt werden können, ist eine Einbindung des IS-Beauftragten und/oder gegebenenfalls des Datenschutzbeauftragten bei der Erstellung und dem Eingang von Verträgen erforderlich. Dies ist insbesondere bei Verträgen zu berücksichtigen, in denen sicherheitsspezifische Anforderungen und Pflichten adressiert werden, die sowohl vom Unternehmen an dritte Parteien (z. B. Dienstleister) als auch von dritten Parteien an das Unternehmen gestellt werden. Alle bereits bestehenden Verträge sollten dem IS-Beauftragten und/oder gegebenenfalls dem Datenschutzbeauftragten zur Prüfung zur Verfügung gestellt werden, damit eine Bewertung hinsichtlich der sicherheitsrelevanten Anforderungen durchgeführt werden kann.

Weitere Informationen zur Gestaltung notwendiger vertraglicher Regelungen liefert der IT-Grundschutzkatalog, zum Beispiel in den Maßnahmen M 2.253 (Vertragsgestaltung mit dem Outsourcing-Dienstleister) oder M 2.475. Der IT-Grundschutzkatalog wird vom Bundesamt für Sicherheit in der Informationstechnik gepflegt und ist auf dessen Homepage abrufbar. Mit dieser Fragestellung wird ein grundsätzliches Verständnis der (Unternehmens-) Leitung für die Tatsache erwartet, dass viele Bereiche des operativen Handelns auch eine rechtliche Komponente / Dimension besitzen.

PSW GROUP

ISA+
Informations-Sicherheits-Analyse

Haben Sie Fragen?

Umfassende Beratung zählt zu unseren Kompetenzen

PSW GROUP
GmbH & Co. KG
Flemingstrasse 20-22
D-36041 Fulda

Phone +49 661 480276 10
Fax +49 661 480276 19
E-Mail info@psw.net
Internet www.psw-group.de

CISSP® | Certified Information Systems Security Professional

CISA | Certified Information Systems Auditor

CISM | Certified Information Security Manager

ISMS | IRCA ISO 27001 ISMS | (Lead) Auditor