ORP: Organisation und Personal

ORP.2: Personal

1 Beschreibung

1.1 Einleitung

Das Personal eines Unternehmens bzw. einer Behörde hat einen entscheidenden Anteil am Erfolg oder Misserfolg der Institution. Die Mitarbeiterinnen und Mitarbeiter haben dabei die wichtige Aufgabe, Informationssicherheit umzusetzen. Die aufwendigsten Sicherheitsvorkehrungen können ins Leere laufen, wenn sie im Arbeitsalltag nicht gelebt werden. Die elementare Bedeutung von Informationssicherheit für eine Institution und ihre Geschäftsprozesse muss daher für das Personal transparent und nachvollziehbar aufbereitet sein.

1.2 Zielsetzung

Ziel dieses Bausteins ist es aufzuzeigen, welche „personellen" Sicherheitsmaßnahmen die Personalabteilung oder Vorgesetzten ergreifen müssen, damit die Mitarbeiterinnen und Mitarbeiter verantwortungsbewusst mit den Informationen der Institution umgehen und sich so gemäß den Vorgaben verhalten.

1.3 Abgrenzung und Modellierung

Der Baustein ORP.2 *Personal* ist für den Informationsverbund einmal anzuwenden.

Der Baustein beschäftigt sich mit den Anforderungen, die durch die Personalabteilung oder die Vorgesetzten einer Institution zu beachten und zu erfüllen sind. Personelle Anforderungen, die an eine bestimmte Funktion gebunden sind, wie z. B. die Ernennung des Systemadministrators eines LAN, werden in den Bausteinen angeführt, die sich mit dem jeweiligen Themengebiet beschäftigen. Der Baustein ORP.2 *Personal* behandelt keine spezifischen Aspekte zu Schulung von Mitarbeitern oder Verwaltung von Identitäten und Berechtigungen. Diese Aspekte werden in den Bausteinen ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* und ORP.4 I*dentitäts- und Berechtigungsmanagement* behandelt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein ORP.2 *Personal* von besonderer Bedeutung:

2.1 Personalausfall

Der Ausfall von Personal kann dazu führen, dass bestimmte Aufgaben nicht mehr oder nicht zeitnah wahrgenommen werden können.

2.2 Unzureichende Kenntnis über Regelungen

Regelungen festzulegen allein garantiert noch nicht, dass diese auch beachtet werden und der Betrieb störungsfrei funktionieren kann. Allen Mitarbeitern müssen die geltenden Regelungen bekannt sein, vor allem den Funktionsträgern. Ein Schaden, der entsteht, weil bestehende Regelungen nicht bekannt sind, sollte sich nicht mit den Aussagen entschuldigen lassen: „Ich habe nicht gewusst, dass ich dafür zuständig bin." oder „Ich habe nicht gewusst, wie ich zu verfahren hatte."

2.3 Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass es in Institutionen zwar viele organisatorische und technische Sicherheitsverfahren gibt, diese jedoch durch den sorglosen Umgang der Mitarbeiter wieder umgangen werden. Ein typisches Beispiel hierfür sind etwa Zettel am Monitor, auf denen Zugangspasswörter notiert sind.

2.4 Unzureichende Qualifikationen der Mitarbeiter

Im täglichen IT-Betrieb einer Institution können viele Störungen und Fehler auftreten. Sind die verantwortlichen Mitarbeiter nicht ausreichend qualifiziert, sensibilisiert und geschult, haben sie z. B. einen veralteten Wissensstand für ihre Aufgabenerfüllung, könnten sie sicherheitsrelevante Ereignisse nicht als solche identifizieren und so Angriffe unerkannt bleiben. Auch wenn die Mitarbeiter ausreichend für die Belange der Informationssicherheit qualifiziert, sensibilisiert bzw. geschult sind, kann trotzdem nicht ausgeschlossen werden, dass sie Sicherheitsvorfälle nicht erkennen. In manchen Situationen, wie bei Personalmangel oder Kündigungen, kann es passieren, dass Mitarbeiter die Aufgaben andere Mitarbeiter vorübergehend übernehmen müssen. Hierbei können Fehler entstehen, wenn Mitarbeiter nicht die notwendigen Qualifikationen haben oder unzureichend geschult sind, um die Aufgabe zu übernehmen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.2 *Personal* aufgeführt. Grundsätzlich ist die Personalabteilung für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	Personalabteilung
Weitere Zuständigkeiten	IT-Betrieb, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein ORP.2 *Personal* vorrangig erfüllt werden:

ORP.2.A1 Geregelte Einarbeitung neuer Mitarbeiter [Vorgesetzte] (B)

Die Personalabteilung sowie die Vorgesetzten MÜSSEN dafür sorgen, dass Mitarbeiter zu Beginn ihrer Beschäftigung in ihre neuen Aufgaben eingearbeitet werden. Die Mitarbeiter MÜSSEN über bestehende Regelungen, Handlungsanweisungen und Verfahrensweisen informiert werden. Eine Checkliste und ein direkter Ansprechpartner („Pate") kann hierbei hilfreich sein und SOLLTE etabliert werden.

ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitern [Vorgesetzte, IT-Betrieb] (B)

Verlässt ein Mitarbeiter die Institution, MUSS der Nachfolger rechtzeitig eingewiesen werden. Dies SOLLTE idealerweise durch den ausscheidenden Mitarbeiter erfolgen. Ist eine direkte Übergabe nicht möglich, MUSS vom ausscheidenden Mitarbeiter eine ausführliche Dokumentation angefertigt werden.

Außerdem MÜSSEN von ausscheidenden Mitarbeitern alle im Rahmen ihrer Tätigkeit erhaltenen Unterlagen, Schlüssel und Geräte sowie Ausweise und Zutrittsberechtigungen eingezogen werden.

Vor der Verabschiedung MUSS noch einmal auf Verschwiegenheitsverpflichtungen hingewiesen werden. Es SOLLTE besonders darauf geachtet werden, dass keine Interessenkonflikte auftreten. Um nach einem Stellenwechsel Interessenkonflikte zu vermeiden, SOLLTEN Konkurrenzverbote und Karenzzeiten vereinbart werden.

Weiterhin MÜSSEN Notfall- und andere Ablaufpläne aktualisiert werden. Alle betroffenen Stellen innerhalb der Institution, wie z. B. das Sicherheitspersonal oder die IT-Abteilung, MÜSSEN über das Ausscheiden des Mitarbeiters informiert werden. Damit alle verbundenen Aufgaben, die beim Ausscheiden des Mitarbeiters anfallen, erledigt werden, SOLLTE hier ebenfalls eine Checkliste angelegt werden . Zudem SOLLTE es einen festen Ansprechpartner der Personalabteilung geben, der den Weggang von Mitarbeitern begleitet.

ORP.2.A3 Festlegung von Vertretungsregelungen [Vorgesetzte] (B)

Die Vorgesetzten MÜSSEN dafür sorgen, dass im laufenden Betrieb Vertretungsregelungen umgesetzt werden. Dafür MUSS sichergestellt werden, dass es für alle wesentlichen Geschäftsprozesse und Aufgaben praktikable Vertretungsregelungen gibt. Bei diesen Regelungen MUSS der Aufgabenumfang der Vertretung im Vorfeld klar definiert werden. Es MUSS sichergestellt werden, dass die Vertretung über das dafür nötige Wissen verfügt. Ist dies nicht der Fall, MUSS überprüft werden, wie der Vertreter zu schulen ist oder ob es ausreicht, den aktuellen Verfahrens- oder Projektstand ausreichend zu dokumentieren. Ist es im Ausnahmefall nicht möglich, für einzelne Mitarbeiter einen kompetenten Vertreter zu benennen oder zu schulen, MUSS frühzeitig entschieden werden, ob externes Personal dafür hinzugezogen werden kann.

ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal (B)

Wird externes Personal beschäftigt, MUSS dieses wie alle eigenen Mitarbeiter dazu verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Fremdpersonal, das kurzfristig oder einmalig eingesetzt wird, MUSS in sicherheitsrelevanten Bereichen beaufsichtigt werden. Bei längerfristig beschäftigtem Fremdpersonal MUSS dieses wie die eigenen Mitarbeiter in seine Aufgaben eingewiesen werden. Auch für diese Mitarbeiter MUSS eine Vertretungsregelung eingeführt werden. Verlässt das Fremdpersonal die Institution, MÜSSEN Arbeitsergebnisse wie bei eigenem Personal geregelt übergeben und eventuell ausgehändigte Zugangsberechtigungen zurückgegeben werden.

ORP.2.A5 Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal (B)

Bevor externe Personen Zugang und Zugriff zu vertraulichen Informationen erhalten, MÜSSEN mit ihnen Vertraulichkeitsvereinbarungen in schriftlicher Form geschlossen werden. In diesen Vertraulichkeitsvereinbarungen MÜSSEN alle wichtigen Aspekte zum Schutz von institutionsinternen Informationen berücksichtigt werden.

ORP.2.A14 Aufgaben und Zuständigkeiten von Mitarbeitern [Vorgesetzte] (B)

Alle Mitarbeiter MÜSSEN dazu verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Den Mitarbeitern MUSS der rechtliche Rahmen ihre Tätigkeit bekannt sein. Die Aufgaben und Zuständigkeiten von Mitarbeitern MÜSSEN in geeigneter Weise dokumentiert sein. Außerdem MÜSSEN alle Mitarbeiter darauf hingewiesen werden, dass alle während der Arbeit erhaltenen Informationen ausschließlich zum internen Gebrauch bestimmt sind. Den Mitarbeitern MUSS bewusstgemacht werden, die Informationssicherheit der Institution auch außerhalb der Arbeitszeit und außerhalb des Betriebsgeländes zu schützen.

ORP.2.A15 Qualifikation des Personals [Vorgesetzte] (B)
Mitarbeiter MÜSSEN regelmäßig geschult bzw. weitergebildet werden. In allen Bereichen MUSS sichergestellt werden, dass kein Mitarbeiter mit veralteten Wissensstand arbeitet. Weiterhin SOLLTE den Mitarbeitern während ihrer Beschäftigung die Möglichkeit gegeben werden, sich im Rahmen ihres Tätigkeitsfeldes weiterzubilden.

Werden Stellen besetzt, MÜSSEN die erforderlichen Qualifikationen und Fähigkeiten genau formuliert sein. Anschließend SOLLTE geprüft werden, ob diese bei den Bewerbern für die Stelle tatsächlich vorhanden sind. Es MUSS sichergestellt sein, dass Stellen nur von Mitarbeitern besetzt werden, für die sie qualifiziert sind.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein ORP.2 *Personal*. Sie SOLLTEN grundsätzlich erfüllt werden.

ORP.2.A6 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.2.A7 Überprüfung der Vertrauenswürdigkeit von Mitarbeitern (S)
Neue Mitarbeiter SOLLTEN auf ihre Vertrauenswürdigkeit hin überprüft werden, bevor sie eingestellt werden. Soweit möglich, SOLLTEN alle an der Personalauswahl Beteiligten kontrollieren, ob die Angaben der Bewerberinnen und Bewerber, die relevant für die Einschätzung ihrer Vertrauenswürdigkeit sind, glaubhaft sind. Insbesondere SOLLTE sorgfältig geprüft werden, ob der vorgelegte Lebenslauf korrekt, plausibel und vollständig ist. Dabei SOLLTEN auffällig erscheinende Angaben überprüft werden.

ORP.2.A8 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.2.A9 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.2.A10 ENTFALLEN (S)
Diese Anforderung ist entfallen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein ORP.2 *Personal* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

ORP.2.A11 ENTFALLEN (H)
Diese Anforderung ist entfallen.

ORP.2.A12 ENTFALLEN (H)
Diese Anforderung ist entfallen.

ORP.2.A13 Sicherheitsüberprüfung (H)
Im Hochsicherheitsbereich SOLLTE eine zusätzliche Sicherheitsüberprüfung zusätzlich zur grundlegenden Überprüfung der Vertrauenswürdigkeit von Mitarbeitern durchgeführt werden.

Arbeiten Mitarbeiter mit nach dem Geheimschutz klassifizierten Verschlusssachen, SOLLTEN sich die entsprechenden Mitarbeiter einer Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz (SÜG) unterziehen. Diesbezüglich SOLLTE der ISB den Geheimschutzbeauftragten bzw. Sicherheitsbevollmächtigten der Institution einbeziehen.

4 Weiterführende Informationen

4.1 Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 „Information technology-Security techniques-Information security management systems-Requirements“ im Anhang A.7 Personalsicherheit Vorgaben für die Personalsicherheit.

Das Infomation Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel PM: People Management Vorgaben für die Personalsicherheit.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein ORP.2 *Personal* von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.33 Personalausfall

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

G 0.32 Missbrauch von Berechtigungen