Bundesamt
für Sicherheit in der
Informationstechnik

ORP: Organisation und Personal

ORP.1: Organisation

1 Beschreibung

1.1 Einleitung

Jede Institution benötigt eine hierfür zuständige Dienststelle, um den allgemeinen Betrieb zu steuern und zu regeln sowie um Verwaltungsdienstleistungen zu planen, zu organisieren und durchzuführen. Die meisten Institutionen haben hierfür eine Organisationseinheit, die dieses Zusammenspiel der verschiedenen Rollen und Einheiten mit den entsprechenden Geschäftsprozessen und Ressourcen steuert. Bereits auf dieser übergreifenden Ebene sind Aspekte der Informationssicherheit einzubringen und verbindlich festzulegen.

1.2 Zielsetzung

Mit diesem Baustein werden allgemeine und übergreifende Anforderungen im Bereich Organisation aufgeführt, die dazu beitragen, das Niveau der Informationssicherheit zu erhöhen und zu erhalten. In diesem Zusammenhang sind Informationsflüsse, Prozesse, Rollenverteilungen sowie die Aufbau- und Ablauforganisation zu regeln.

1.3 Abgrenzung und Modellierung

Der Baustein ORP.1 *Organisation* ist auf den Informationsverbund mindestens einmal anzuwenden. Wenn Teile des Informationsverbunds einer anderen Organisationseinheit zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Einheit separat angewandt werden.

Der Baustein bildet die übergeordnete Basis, um Informationssicherheit in einer Institution umzusetzen. Er behandelt keine spezifischen Aspekte zu Personal, Schulung von Mitarbeitern, Verwaltung von Identitäten und Berechtigungen sowie Anforderungsmanagement. Diese Aspekte werden in den Bausteinen ORP.2 *Personal,* ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit,* ORP.4 *Identitäts- und Berechtigungsmanagement* und ORP.5 *Compliance Management (Anforderungsmanagement)* behandelt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein ORP.1 *Organisation* von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Regelungen

Fehlende Regelungen können zu massiven Sicherheitslücken führen, wenn beispielsweise Mitarbeiter

nicht wissen, wie sie bei Vorfällen reagieren sollen. Probleme können auch dadurch entstehen, dass Regelungen veraltet, unpraktikabel oder unverständlich formuliert sind.

Die Bedeutung dieser übergreifenden organisatorischen Regelungen nimmt mit der Komplexität der Geschäftsprozesse und dem Umfang der Informationsverarbeitung, aber auch mit dem Schutzbedarf der zu verarbeitenden Informationen zu.

2.2 Nichtbeachtung von Regelungen

Allen Mitarbeitern müssen die geltenden Regelungen bekannt gemacht werden und zum Nachlesen zur Verfügung stehen. Die Erfahrung zeigt, dass es nicht ausreicht, Sicherheitsregeln lediglich festzulegen. Ihre Kommunikation an die Mitarbeiter ist elementar wichtig, damit die Vorgaben auch von allen Betroffenen im Arbeitsalltag gelebt werden können.

Werden Regelungen von Mitarbeitern missachtet, können beispielsweise folgende Sicherheitslücken entstehen:

- Vertrauliche Informationen werden in Hörweite fremder Personen diskutiert, beispielsweise in Pausengesprächen von Besprechungen oder über Mobiltelefonate in öffentlichen Umgebungen.
- Dokumente werden auf einem Webserver veröffentlicht, ohne dass geprüft wurde, ob diese tatsächlich zur Veröffentlichung vorgesehen und freigegeben sind.
- Aufgrund von fehlerhaft administrierten Zugriffsrechten kann ein Mitarbeiter Daten ändern, ohne die Brisanz dieser Integritätsverletzung einschätzen zu können.

2.3 Fehlende, ungeeignete oder inkompatible Betriebsmittel

Wenn benötigte Betriebsmittel in zu geringer Menge vorhanden sind oder nicht termingerecht bereitgestellt werden, können in der Institution Störungen eintreten. Ebenso kann es vorkommen, dass ungeeignete oder sogar inkompatible Betriebsmittel beschafft werden, die infolgedessen nicht eingesetzt werden können.

Beispiel: Der Speicherplatz von Festplatten bei Clients und Servern sowie mobiler Datenträger steigt ständig. Dabei wird häufig vergessen, IT-Komponenten und Datenträger zu beschaffen, die für eine regelmäßige Datensicherung ausreichend Kapazität bieten.

Ebenso muss die Funktionsfähigkeit der eingesetzten Betriebsmittel gewährleistet sein. Wenn Wartungsarbeiten nicht oder nur unzureichend durchgeführt werden, können daraus hohe Schäden entstehen.

Beispiele:

- Die Kapazität der Batterien einer unterbrechungsfreien Stromversorgung (USV-Anlage) wurde nicht rechtzeitig überprüft. Ist die Kapazität bzw. der Säuregehalt zu gering, kann die USV-Anlage einen Stromausfall nicht mehr ausreichend lange überbrücken.
- Die Feuerlöscher wurden nicht rechtzeitig gewartet und verfügen deshalb nicht mehr über einen ausreichenden Druck. Ihre Löschleistung ist somit im Brandfall nicht mehr gewährleistet.

2.4 Gefährdung durch Institutionsfremde

Bei Institutionsfremden kann grundsätzlich nicht vorausgesetzt werden, dass sie mit ihnen zugänglichen Informationen und der Informationstechnik entsprechend den Vorgaben der besuchten Institution umgehen.

Besucher, Reinigungs- und Fremdpersonal können interne Informationen, Geschäftsprozesse und IT-Systeme auf verschiedene Arten gefährden, angefangen von der unsachgemäßen Behandlung der technischen Einrichtungen über den Versuch des „Spielens“ an IT-Systemen bis hin zum Diebstahl von Unterlagen oder IT-Komponenten.

Beispiele:

- Unbegleitete Besucher können auf Unterlagen und Datenträger zugreifen oder Zugang zu Geräten haben, diese beschädigen oder schützenswerte Informationen ausspähen.
- Reinigungskräfte können versehentlich Steckverbindungen lösen, Wasser in Geräte laufen lassen, Unterlagen verlegen oder mit dem Abfall entsorgen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.1 *Organisation* aufgeführt. Grundsätzlich ist die Zentrale Verwaltung 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 festgelegten 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	Zentrale Verwaltung
Weitere Zuständigkeiten	Mitarbeiter, Benutzer, IT-Betrieb, Haustechnik, Institutionsleitung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein ORP.1 *Organisation* vorrangig erfüllt werden:

ORP.1.A1 Festlegung von Verantwortlichkeiten und Regelungen [Institutionsleitung] (B)

Innerhalb einer Institution MÜSSEN alle relevanten Aufgaben und Funktionen klar definiert und voneinander abgegrenzt sein. Es MÜSSEN verbindliche Regelungen für die Informationssicherheit für die verschiedenen betrieblichen Aspekte übergreifend festgelegt werden. Die Organisationsstrukturen sowie verbindliche Regelungen MÜSSEN anlassbezogen überarbeitet werden. Die Änderungen MÜSSEN allen Mitarbeitern bekannt gegeben werden.

ORP.1.A2 Zuweisung der Zuständigkeiten [Institutionsleitung] (B)

Für alle Geschäftsprozesse, Anwendungen, IT-Systeme, Räume und Gebäude sowie Kommunikationsverbindungen MUSS festgelegt werden, wer für diese und deren Sicherheit zuständig ist. Alle Mitarbeiter MÜSSEN darüber informiert sein, insbesondere wofür sie zuständig sind und welche damit verbundenen Aufgaben sie wahrnehmen.

ORP.1.A3 Beaufsichtigung oder Begleitung von Fremdpersonen [Mitarbeiter] (B)

Institutionsfremde Personen MÜSSEN von Mitarbeitern zu den Räumen begleitet werden. Die Mitarbeiter der Institution MÜSSEN institutionsfremde Personen in sensiblen Bereichen beaufsichtigen. Die Mitarbeiter SOLLTEN dazu angehalten werden, institutionsfremde Personen in den Räumen der Institution nicht unbeaufsichtigt zu lassen.

ORP.1.A4 Funktionstrennung zwischen unvereinbaren Aufgaben (B)

Die Aufgaben und die hierfür erforderlichen Rollen und Funktionen MÜSSEN so strukturiert sein, dass unvereinbare Aufgaben wie operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden. Für unvereinbare Funktionen MUSS eine Funktionstrennung festgelegt und dokumentiert sein. Auch Vertreter MÜSSEN der Funktionstrennung unterliegen.

ORP.1.A5 ENTFALLEN (B)
Diese Anforderung ist entfallen.

ORP.1.A15 Ansprechpartner zu Informationssicherheitsfragen (B)
In jeder Institution MUSS es Ansprechpartner für Sicherheitsfragen geben, die sowohl scheinbar einfache wie auch komplexe oder technische Fragen beantworten können. Die Ansprechpartner MÜSSEN allen Mitarbeitern der Institution bekannt sein. Diesbezügliche Informationen MÜSSEN in der Institution für alle verfügbar und leicht zugänglich sein.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein ORP.1 *Organisation*. Sie SOLLTEN grundsätzlich erfüllt werden.

ORP.1.A6 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.1.A7 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.1.A8 Betriebsmittel- und Geräteverwaltung [IT-Betrieb] (S)
Alle Geräte und Betriebsmittel, die Einfluss auf die Informationssicherheit haben und die zur Aufgabenerfüllung und zur Einhaltung der Sicherheitsanforderungen erforderlich sind, SOLLTEN in ausreichender Menge vorhanden sein. Es SOLLTE geeignete Prüf- und Genehmigungsverfahren vor Einsatz der Geräte und Betriebsmittel geben. Geräte und Betriebsmittel SOLLTEN in geeigneten Bestandsverzeichnissen aufgelistet werden. Um den Missbrauch von Daten zu verhindern, SOLLTE die zuverlässige Löschung oder Vernichtung von Geräten und Betriebsmitteln geregelt sein (siehe hierzu *CON.6 Löschen und Vernichten*).

ORP.1.A9 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.1.A10 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.1.A11 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.1.A12 ENTFALLEN (S)
Diese Anforderung ist entfallen.

ORP.1.A13 Sicherheit bei Umzügen [IT-Betrieb, Haustechnik] (S)
Vor einem Umzug SOLLTEN frühzeitig Sicherheitsrichtlinien erarbeitet bzw. aktualisiert werden. Alle Mitarbeiter SOLLTEN über die vor, während und nach dem Umzug relevanten Sicherheitsmaßnahmen informiert werden. Nach dem Umzug SOLLTE überprüft werden, ob das transportierte Umzugsgut vollständig und unbeschädigt bzw. unverändert angekommen ist.

ORP.1.A16 Richtlinie zur sicheren IT-Nutzung [Benutzer] (S)
Es SOLLTE eine Richtlinie erstellt werden, in der für alle Mitarbeiter transparent beschrieben wird, welche Rahmenbedingungen bei der IT-Nutzung eingehalten werden müssen und welche Sicherheitsmaßnahmen zu ergreifen sind. Die Richtlinie SOLLTE folgende Punkte abdecken:

- Sicherheitsziele der Institution,
- wichtige Begriffe,
- Aufgaben und Rollen mit Bezug zur Informationssicherheit,
- Ansprechpartner zu Fragen der Informationssicherheit sowie

- von den Mitarbeitern umzusetzende und einzuhaltende Sicherheitsmaßnahmen.

Die Richtlinie SOLLTE allen Benutzern zur Kenntnis gegeben werden. Jeder neue Benutzer SOLLTE die Kenntnisnahme und Beachtung der Richtlinie schriftlich bestätigen, bevor er die Informationstechnik nutzen darf. Benutzer SOLLTEN die Richtlinie regelmäßig oder nach größeren Änderungen erneut bestätigen. Die Richtlinie sollte zum Nachlesen für alle Mitarbeiter frei zugänglich abgelegt werden, beispielsweise im Intranet.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein ORP.1 *Organisation* 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.1.A14 ENTFALLEN (H)
Diese Anforderung ist entfallen.

4 Weiterführende Informationen

4.1 Wissenswertes

Für den Baustein ORP.1 *Organisation* sind keine weiterführenden Informationen vorhanden.

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.1 *Organisation* von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.38 Missbrauch personenbezogener Daten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen