Bundesamt
für Sicherheit in der
Informationstechnik

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 Mitarbeitenden, 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

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen

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 Mitarbeitende 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 Mitarbeitenden 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 Mitarbeitenden ist elementar wichtig, damit die Vorgaben auch von allen Betroffenen im Arbeitsalltag gelebt werden können.

Werden Regelungen von Mitarbeitenden 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 können Mitarbeitende 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.

Besuchende, 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 Besuchende 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. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Zentrale Verwaltung
Weitere Zuständigkeiten	Mitarbeitende, Benutzende, IT-Betrieb, Haustechnik, Institutionsleitung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

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

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 Mitarbeitenden bekannt gegeben werden.

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

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

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

Institutionsfremde Personen MÜSSEN von Mitarbeitenden zu den Räumen begleitet werden. Die Mitarbeitenden der Institution MÜSSEN institutionsfremde Personen in sensiblen Bereichen beaufsichtigen. Die Mitarbeitenden 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 Ansprechperson zu Informationssicherheitsfragen (B)

In jeder Institution MUSS es Ansprechpersonen für Sicherheitsfragen geben, die sowohl scheinbar einfache wie auch komplexe oder technische Fragen beantworten können. Die Ansprechpersonen MÜSSEN allen Mitarbeitenden 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 diesen Baustein. 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 (S) [IT-Betrieb]

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 (S) [IT-Betrieb, Haustechnik]

Vor einem Umzug SOLLTEN frühzeitig Sicherheitsrichtlinien erarbeitet bzw. aktualisiert werden. Alle Mitarbeitenden 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 (S) [Benutzende]

Es SOLLTE eine Richtlinie erstellt werden, in der für alle Mitarbeitenden 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,
- Ansprechperson zu Fragen der Informationssicherheit sowie
- von den Mitarbeitenden umzusetzende und einzuhaltende Sicherheitsmaßnahmen.

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

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

ORP.1.A14 ENTFALLEN (H)

Diese Anforderung ist entfallen.

ORP.1.A17 Mitführverbot von Mobiltelefonen (H)

Mobiltelefone SOLLTEN NICHT zu vertraulichen Besprechungen und Gesprächen mitgeführt werden. Falls erforderlich, SOLLTE dies durch Mobilfunk-Detektoren überprüft werden.

4. Weiterführende Informationen

4.1. Wissenswertes

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