Bundesamt
für Sicherheit in der
Informationstechnik

ORP.3 Sensibilisierung und Schulung zur Informationssicherheit

1. Beschreibung

1.1. Einleitung

Mitarbeitende sind ein wichtiger Erfolgsfaktor für ein hohes Maß an Informationssicherheit in einer Institution. Daher ist es wichtig, dass sie die Sicherheitsziele kennen, die Sicherheitsmaßnahmen verständlich sind und jeder einzelne Mitarbeitende bereit ist, diese umzusetzen. Die Voraussetzung dafür ist, dass es ein Sicherheitsbewusstsein innerhalb der Institution gibt. Darüber hinaus sollte eine Sicherheitskultur aufgebaut und im Arbeitsalltag mit Leben gefüllt werden.

Mitarbeitende müssen für relevante Gefährdungen sensibilisiert werden und wissen, wie sich diese auf ihre Institution auswirken können. Ihnen muss bekannt sein, was von ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollen.

1.2. Zielsetzung

In diesem Baustein wird beschrieben, wie ein effektives Sensibilisierungs- und Schulungsprogramm zur Informationssicherheit aufgebaut und aufrechterhalten werden kann. Ziel des Programms ist es, die Wahrnehmung der Mitarbeitenden für Sicherheitsrisiken zu schärfen und ihnen die notwendigen Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten zu vermitteln.

1.3. Abgrenzung und Modellierung

Der Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* ist für den Informationsverbund einmal anzuwenden.

Dieser Baustein formuliert Anforderungen an die Sensibilisierung und Schulung zur Informationssicherheit, die das Arbeitsumfeld in der Institution, den Telearbeitsplatz und die mobile Arbeit betreffen.

Der Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* beschreibt die prozessualen, technischen, methodischen und organisatorischen Anforderungen an die

Sensibilisierung und Schulung von Informationssicherheit. Weitere Schulungsthemen werden durch die Personalabteilung oder das Weiterbildungsmanagement geplant, gestaltet und durchgeführt.

In vielen der anderen IT-Grundschutz-Bausteine werden konkrete Schulungsinhalte zu den dort betrachteten Themen beschrieben. Der vorliegende Baustein beschäftigt sich damit, wie in den Bereichen Sensibilisierung und Schulung zur Informationssicherheit ein planvolles Vorgehen effizient gestaltet werden kann.

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.3 *Sensibilisierung und Schulung zur Informationssicherheit* von besonderer Bedeutung.

2.1. Unzureichende Kenntnis über Regelungen

Regelungen zur Informationssicherheit lediglich festzulegen, garantiert nicht, dass sie auch beachtet werden. Allen Mitarbeitenden, insbesondere die in Funktion gewählten Personen, müssen die geltenden Regelungen auch bekannt sein. Bei vielen Sicherheitsvorfällen ist die Nichtbeachtung von Regelungen zwar nicht der alleinige Auslöser des Vorfalls, aber mit ein Grund dafür, dass er auftritt. Sicherheitslücken aufgrund unzureichender Kenntnisse über Regelungen können die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, mit denen gearbeitet wird, gefährden. Die Aufgabenerfüllung und die Abwicklung von Geschäftsprozessen und Fachaufgaben können dadurch eingeschränkt werden.

2.2. Unzureichende Sensibilisierung für Informationssicherheit

Die Erfahrung zeigt, dass es nicht genügt, Sicherheitsmaßnahmen lediglich anzuordnen. Die Mitarbeitenden sollten die Bedeutung und den Zweck der Maßnahmen kennen, da diese ansonsten im Arbeitsalltag ignoriert werden könnten. Werden Mitarbeitende unzureichend zu Informationssicherheitsthemen sensibilisiert, können die Sicherheitskultur, die Sicherheitsziele und die Sicherheitsstrategie der Institution gefährdet sein.

2.3. Unwirksame Aktivitäten zur Sensibilisierung und Schulung

Nicht immer sind die zur Sensibilisierung und Schulung durchgeführten Aktivitäten so erfolgreich wie gewünscht. Ursachen dafür können sein:

- eine fehlende Management-Unterstützung,
- unklare Ziele,
- schlechte Planung,
- mangelnde Erfolgskontrolle,
- fehlende Kontinuität sowie
- zu geringe finanzielle oder personelle Ressourcen.

Werden keine geeigneten Maßnahmen ergriffen, um den Erfolg der durchgeführten Aktivitäten sicherzustellen, kann das Ziel der jeweiligen Schulungsaktivität häufig nicht erreicht werden. Wenn die Institution unzureichende Aktivitäten zur Sensibilisierung und Schulung der Mitarbeitenden durchführt, können Aspekte der Informationssicherheit gefährdet sein, was direkt die Aufgabenerfüllung einschränkt.

2.4. Unzureichende Schulung der Mitarbeitenden zu Sicherheitsfunktionen

Häufig wenden Mitarbeitende neu eingeführte Sicherheitsprogramme und -funktionen deswegen nicht an, weil sie nicht wissen, wie sie bedient werden, und sie es als zu zeitaufwendig ansehen, sich im täglichen Arbeitsablauf selbstständig darin einzuarbeiten. Darüber hinaus können fehlende Schulungen nach Einführung einer neuen Software dazu führen, dass Mitarbeitende diese falsch bedienen oder falsch konfigurieren und Arbeitsabläufe sich unnötig verzögern. Daher reicht die Beschaffung und Installation einer (Sicherheits-)Software nicht aus. Besonders bei kritischen IT-Systemen und -Anwendungen kann eine Fehlbedienung existenzbedrohende Auswirkungen nach sich ziehen.

2.5. Nicht erkannte Sicherheitsvorfälle

Im täglichen Betrieb von IT- und ICS-Komponenten können viele Störungen und Fehler auftreten. Dabei könnten Sicherheitsvorfälle durch das Personal nicht als solche identifiziert werden und auch Cyber-Angriffe bzw. Angriffsversuche unerkannt bleiben. Sicherheitsvorfälle und technische Fehler sind mitunter nicht einfach zu unterscheiden. Werden Benutzende und Administrierende nicht gezielt darin geschult und dafür sensibilisiert, Sicherheitsvorfälle zu erkennen und auf diese angemessen zu reagieren, können Sicherheitslücken unentdeckt bleiben und ausgenutzt werden. Falls Sicherheitsvorfälle zu spät oder gar nicht erkannt werden, können wirksame Gegenmaßnahmen nicht rechtzeitig ergriffen werden. Kleine Sicherheitslücken der Institution können zu kritischen Gefährdungen für die Integrität, Vertraulichkeit und Verfügbarkeit heranwachsen. Dies kann Geschäftsprozesse behindern, finanzielle Schäden hervorrufen oder regulatorische und gesetzliche Sanktionen nach sich ziehen.

2.6. Nichtbeachtung von Sicherheitsmaßnahmen

Verschiedenste Gründen, wie Unachtsamkeit oder Hektik, können dazu führen, dass beispielsweise vertrauliche Dokumente an Arbeitsplätzen offen herumliegen oder E-Mails nicht verschlüsselt werden. Durch solche vermeintlich kleinen Nachlässigkeiten können Schäden entstehen, die gut geschulten Mitarbeitenden in der Regel nicht passieren.

2.7. Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass in Institutionen zwar eine Vielzahl von organisatorischen und technischen Sicherheitsverfahren festgelegt sind, diese jedoch durch den sorglosen Umgang der Mitarbeitenden umgangen werden. Ein typisches Beispiel hierfür sind die fast schon berühmten Zettel am Monitor, auf denen Zugangspasswörter notiert sind. Ebenso schützt eine Festplattenverschlüsselung einen Laptop unterwegs nicht davor, dass vertrauliche Informationen etwa vom Sitznachbarn im Zug einfach mitgelesen werden können. Die besten technischen Sicherheitslösungen helfen nicht, wenn Ausdrucke mit vertraulichen Informationen am Drucker liegenbleiben oder in frei zugänglichen Altpapiercontainern landen.

Wenn die Mitarbeitenden sorglos mit Informationen umgehen, werden festgelegte Prozesse der Informationssicherheit unwirksam. Unbefugte könnten z. B. Nachlässigkeiten im Umgang mit Informationen ausnutzen, um gezielt Wirtschaftsspionage zu betreiben.

2.8. Fehlende Akzeptanz von Informationssicherheitsvorgaben

Es kann unterschiedliche Gründe dafür geben, warum Mitarbeitende die Vorgaben zur Informationssicherheit nicht umsetzen. Dazu zählen beispielsweise eine fehlende Sicherheitskultur der Institution oder eine fehlende Vorbildfunktion durch die Institutionsleitung. Aber auch übertriebene

Sicherheitsanforderungen können dazu führen, dass Mitarbeitende Sicherheitsmaßnahmen ablehnen. Probleme können außerdem dadurch entstehen, dass bestimmte Berechtigungen oder auch die Ausstattung mit bestimmter Hard- oder Software als Statussymbol gesehen werden. Einschränkungen in diesen Bereichen können auf großen Widerstand stoßen.

2.9. Social Engineering

Social Engineering ist eine Methode, um unberechtigten Zugriff auf Informationen oder Zugang zu IT-Systemen durch "Aushorchen" von Mitarbeitenden zu erlangen. Beim Social Engineering baut der oder die Angreifende meistens einen direkten Kontakt zu einem Opfer auf, z. B. per Telefon, E-Mail oder auch über Soziale Netzwerke. Angriffe über Social Engineering sind häufig mehrstufig. Indem der oder die Angreifende Insiderwissen vorgibt und gleichzeitig an die Hilfsbereitschaft appelliert, kann er oder sie sein oder ihr Wissen in weiteren Schritten ausbauen. Wenn Mitarbeitende für diese Art von Angriffen nicht ausreichend sensibilisiert sind, könnten sie durch geschickte Kommunikation so manipuliert werden, dass sie unzulässig handeln. Dies kann dazu führen, dass sie interne Informationen weitergeben, ihre IT-Systeme sich mit Schadsoftware infizieren oder sogar Geld an angebliche Geschäftspartner und Geschäftspartnerin überweisen.

So wird beispielsweise beim sogenannten „CEO Fraud“ Mitarbeitenden, die Geld im Namen der Institution transferieren dürfen, ein fiktiver Auftrag der Leitung vorgegaukelt. Sie sollen für ein angeblich dringendes und vertrauliches Geschäft Transaktionen durchführen, die für das weitere Bestehen der Institution äußerst wichtig sind.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* 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	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	IT-Betrieb, Vorgesetzte, Personalabteilung, 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.3.A1 Sensibilisierung der Institutionsleitung für Informationssicherheit (B) [Vorgesetzte, Institutionsleitung]

Die Institutionsleitung MUSS ausreichend für Sicherheitsfragen sensibilisiert werden. Die Sicherheitskampagnen und Schulungsmaßnahmen MÜSSEN von der Institutionsleitung unterstützt werden. Vor dem Beginn eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit MUSS die Unterstützung der Institutionsleitung eingeholt werden.

Alle Vorgesetzten MÜSSEN die Informationssicherheit unterstützen, indem sie mit gutem Beispiel vorangehen. Führungskräfte MÜSSEN die Sicherheitsvorgaben umsetzen. Hierüber hinaus MÜSSEN sie ihre Mitarbeitenden auf deren Einhaltung hinweisen.

ORP.3.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT (B) [Vorgesetzte, Personalabteilung, IT-Betrieb]

Alle Mitarbeitenden und externen Benutzenden MÜSSEN in den sicheren Umgang mit IT-, ICS- und IoT-Komponenten eingewiesen und sensibilisiert werden, soweit dies für ihre Arbeitszusammenhänge relevant ist. Dafür MÜSSEN verbindliche, verständliche und aktuelle Richtlinien zur Nutzung der jeweiligen Komponenten zur Verfügung stehen. Werden IT-, ICS- oder IoT-Systeme oder -Dienste in einer Weise benutzt, die den Interessen der Institution widersprechen, MUSS dies kommuniziert werden.

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.3.A4 Konzeption und Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit (S)

Sensibilisierungs- und Schulungsprogramme zur Informationssicherheit SOLLTEN sich an den jeweiligen Zielgruppen orientieren. Dazu SOLLTE eine Zielgruppenanalyse durchgeführt werden. Hierbei SOLLTEN Schulungsmaßnahmen auf die speziellen Anforderungen und unterschiedlichen Hintergründe fokussiert werden können.

Es SOLLTE ein zielgruppenorientiertes Sensibilisierungs- und Schulungsprogramm zur Informationssicherheit erstellt werden. Dieses Schulungsprogramm SOLLTE den Mitarbeitenden alle Informationen und Fähigkeiten vermitteln, die erforderlich sind, um in der Institution geltende Sicherheitsregelungen und -maßnahmen umsetzen zu können. Es SOLLTE regelmäßig überprüft und aktualisiert werden.

ORP.3.A5 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.3.A6 Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit (S)

Alle Mitarbeitenden SOLLTEN entsprechend ihren Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden.

ORP.3.A7 Schulung zur Vorgehensweise nach IT-Grundschutz (S)

Informationssicherheitsbeauftragte SOLLTEN mit dem IT-Grundschutz vertraut sein. Wurde ein Schulungsbedarf identifiziert, SOLLTE eine geeignete IT-Grundschutz-Schulung geplant werden. Für die Planung einer Schulung SOLLTE der Online-Kurs des BSI zum IT-Grundschutz berücksichtigt werden. Innerhalb der Schulung SOLLTE die Vorgehensweise anhand praxisnaher Beispiele geübt werden. Es SOLLTE geprüft werden, ob der oder die Informationssicherheitsbeauftragte sich zu einem BSI IT-Grundschutz-Praktiker qualifizieren lassen sollten.

ORP.3.A8 Messung und Auswertung des Lernerfolgs (S) [Personalabteilung]

Die Lernerfolge im Bereich Informationssicherheit SOLLTEN zielgruppenbezogen gemessen und ausgewertet werden, um festzustellen, inwieweit die in den Sensibilisierungs- und

Schulungsprogrammen zur Informationssicherheit beschriebenen Ziele erreicht sind. Die Messungen SOLLTEN sowohl quantitative als auch qualitative Aspekte der Sensibilisierungs- und Schulungsprogramme zur Informationssicherheit berücksichtigen. Die Ergebnisse SOLLTEN bei der Verbesserung des Sensibilisierungs- und Schulungsangebots zur Informationssicherheit in geeigneter Weise einfließen.

Der oder die Informationssicherheitsbeauftragte SOLLTE sich regelmäßig mit der Personalabteilung und den anderen für die Sicherheit relevanten Ansprechpartnern (Datenschutz, Gesundheits- und Arbeitsschutz, Brandschutz etc.) über die Effizienz der Aus- und Weiterbildung austauschen.

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.3.A9 Spezielle Schulung von exponierten Personen und Institutionen (H)

Besonders exponierte Personen SOLLTEN vertiefende Schulungen in Hinblick auf mögliche Gefährdungen sowie geeignete Verhaltensweisen und Vorsichtsmaßnahmen erhalten.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Kapitel 7.2 Vorgaben für die Sensibilisierung und Schulung von Beschäftigten.

Das Information Security Forum (ISF) definiert in seinem Standard „The Standard of Good Practice for Information Security“ unter PM2 verschiedene Anforderungen an Sensibilisierung und Schulung von Beschäftigten.

Das BSI bietet unter https://www.bsi.bund.de/grundschutzkurs einen Online-Kurs zum IT-Grundschutz an, der die Methodik des IT-Grundschutzes vorstellt.

Das BSI bietet ein zweistufiges Schulungskonzept zum Thema IT-Grundschutz an. Bei dem Schulungskonzept kann man einen Nachweis eines IT-Grundschutz-Praktikers erwerben und sich weiter zum IT-Grundschutz-Berater vom BSI zertifizieren lassen.

Eine Liste der Schulungsanbieter, die die BSI Schulung zum IT-Grundschutz-Praktiker und IT-Grundschutz-Berater anbieten, ist unter https://www.bsi.bund.de/dok/128348 zu finden.