Allianz für Cyber-Sicherheit

ORP.3 – Sensibilisierung und Schulung

Anforderungen	**Die Basisanforderungen A1 –A3 sind umzusetzen.** Das sind im Detail: • A1: Sensibilisierung: Die Geschäftsführung und das leitende Management muss selbst für IT Sicherheit sensibilisiert sein und die getroffenen Sicherheitsmaßnahmen für Mitarbeiter unterstützen und vorleben. • A2: Es muss ein ausreichend geschulter, allg. bekannter Ansprechpartner zu IT Sicherheitsfragen im Unternehmen existieren • A3: Alle Mitarbeiter müssen gemäß Ihrer Arbeitsinhalte durch allgemeine, verständliche Richtlinien in den sicheren Umgang mit IT Komponenten eingewiesen und für IT Sicherheitsfragen sensibilisiert werden/worden sein. **Es ist unsere Empfehlung, beim Baustein ORP.3 zusätzlich auch die Standardanforderungen A4-A8 umzusetzen**. Im Detail: • A4: Schulungsplanung: Es sollte ein detailliertes, zielgruppenorientiertes Schulungsprogramm erarbeitet und regelmäßig aktualisiert werden. • A5:Zielgruppen: Es sollten die entsprechenden Zielgruppen gemäß Ihrer betrieblichen Aufgaben und ihres Kenntnisstandes festgelegt werden. • A6: Die Sicherheitsschulungen sollten alle Mitarbeiter gemäß Ihrer Position und Aufgaben in die Lage versetzen, die Sicherheitsregeln und Maßnahmen des Unternehmens umzusetzen und zu leben. • A7: Der IT Sicherheitsbeauftragte sollte regelmäßig im IT Grundschutz geschult und weitergebildet sein bzw. werden. • A8: Die Lernerfolge der Schulungen sollten regelmäßig Zielgruppenorientiert überprüft und gemessen werden, um das Schulungsprogramm mittels eines KVP Prozesses zu optimieren. Ggf. können noch speziell exponierte Personen gesondert geschult werden, wenn dieses nicht schon durch Ihre Zielgruppenzuordnung gemäß A4-8 gegeben ist. • A9: Besondere Schulungen sollten für besonders exponierte Gruppen durchgeführt werden
Ausnahmen	Wenn die Umsetzung des IT Sicherheitskonzeptes schwerpunktmäßig nach ISO 2700* erfolgt, sollte auch die Aus-/Fortbildung des IT Sicherheitsbeauftragten primär sich an dieser Normenreihe orientieren.
Priorisierung	**R1**

	Schulungen und Sensibilisierungsmaßnahmen sind wesentlich für den Aufbau der s.g. menschlichen Firewalls und damit für den Schutz des Unternehmens. Der Großteil der Einbrüche in die Netzwerke von Unternehmen erfolgt durch Schadsoftware geöffnete „Türen“ bewusst oder unbewusst angetriggert durch Userinteraktion. Diesem geht es durch geeignete Sensibilisierungen zu begegnen. Dieses gilt besonders für eine Branche wie die Papierindustrie, die traditionell sehr hohe physikalische Zugangsbeschränkungen vorhält. (abgesicherte Werksgelände, Pförtner etc.)
Allgemeine Empfehlungen zum Baustein	Die Themen Sensibilisierung und Schulung sind sicherlich sehr global und werden in Abhängigkeit von der jeweiligen Unternehmenskultur unterschiedlich gelebt. Das IT Sicherheitsschulungskonzept sollte immer in die bestehende Kultur integriert werden, um den optimalen Erfolg zu erzielen ohne allerdings Abstriche in Kauf zu nehmen.
Empfehlungen zur Umsetzung der Anforderung [Link zu den Umsetzungs-hinweisen des BSI]	[Zu jeder Anforderung könnten nach Möglichkeit Hinweise zur Umsetzung im Kontext vom jeweiligen Profil gegeben werden.] **Zu A1: „Schulung und Sensibilisierung der Mitarbeiter schützt das Unternehmen“** Schulung der Mitarbeiter kann nur funktionieren, wenn sie von der Geschäftsführung unterstützt wird und diese selbst den Sinn einsieht und sich entsprechend verhält. Führen heißt auch immer „mit gutem Beispiel vorangehen“. Gerade im Falle von IT Sicherheit ist es aber oft schwierig, die abstrakte Bedrohung zu verdeutlichen. Hier sollte klar mit Kosten für mögliche Stillstände z.B. einer PM argumentiert werden. Was funktioniert noch wie lange ohne IT und was kostet das dann? Wenn verdeutlicht wird, wie Bedrohungen normalerweise in das Netzwerk eindringen, sollte auch der letzten Führungskraft die Notwendigkeit dieses Themas klar werden. Um die Bedeutung von IT-Sicherheit von Seiten der Geschäftsführung sichtbar zu machen, sollte eine Einbindung in die interne Unternehmenskommunikation (Intranet, Managementsysteme, MA-Zeitschrift) erfolgen. Auch Berichte auf Betriebsversammlungen von IT-Verantwortlichen zusammen mit der Geschäftsführung erhöhen die Aufmerksamkeit für das Thema. **Zu A2: Ansprechpartner im Unternehmen** IT Sicherheitswissen ist komplex, teilweise unternehmensspezifisch und entwickelt sich extrem schnell weiter. Hier sind entsprechend geeignete, praxisorientierte, im Unternehmen anerkannte und akzeptierte Mitarbeiter dafür freizustellen und entsprechend regelmäßig intensiv zu schulen. Diese können Teil der IT-System- und Netzwerkadministration sein oder separat hierfür freigestellte CISO (Chief Information Security Officer).

Zu A3: Einweisung des Personals
Jeder Mitarbeiter muss, bevor er IT Equipment benutzt, eine Basisschulung für den sicheren Umgang gemäß der im jeweiligen Unternehmen gültigen Richtlinien erhalten. Hier ist sicherlich mit Augenmaß orientiert am Arbeitsplatz vorzugehen. Ein reiner Maschinenführer oder Handwerker ohne Internetzugang unterliegt anderen Risiken als ein Vertriebsmitarbeiter im Außendienst. Nichtsdestotrotz sollten für alle gewisse Basisstandards gelten. Hier kann man sich u.a. an dem folgenden Orientieren:

- Sicherheitshinweise der eingesetzten Softwarehersteller bzw. interne Policies (Passwortlänge etc.)
- Betriebsvereinbarungen zur IT bzw. Internetnutzung
- Andere BSI Bausteine

Die erste Basisschulung sollte möglichst direkt als Präsenzschulung erfolgen, Folgeschulungen könne dann auch regelmäßig durch ggf. eingesetzte Schulungssoftware durchgeführt und überprüft werden. Im Bereich der IT-Sicherheit ist eine Zusammenarbeit mit den ZACs (Zentrale Ansprechstelle Cybercrime) der LKAs sowohl hinsichtlich Vor-Ort-Schulungen als auch zur Angriffssimulation möglich. Dies kann von Bundesland zu Bundesland unterschiedlich sein.

Zu A4/A5/6: Schulungsprogramm/Zielgruppen/Durchführung:
Die Festlegung von konkreten Zielgruppen mit Ihren spezifischen Anforderungen an IT Sicherheit ist ein wesentlicher Baustein für ein erfolgreiches Gesamtkonzept. Diesem Punkt sollte besondere Aufmerksamkeit geschenkt werden. Gruppiert man Zielgruppen nach Ihren Sicherheitsanforderungen so sind beispielhaft die folgenden typischen Zielgruppen denkbar:

1. Klasse: Geringe IT Sicherheitsanforderungen:
   - Mitarbeiter ohne Internet (Produktion)
   - Innendienstsachbearbeiter
   - ⇨ Basiskenntnisse in allg. IT Sicherheit

2. Klasse: Mittlere Sicherheitsanforderungen:
   - Kaufm. und gewerbl. Mitarbeiter mit Internetzugang
   - Ggf. Geringe Reisetätigkeit
   - Intensiver Mailverkehr
   - ⇨ zusätzlich Internetrisiken
   - ⇨ Phishing, Angriffsmechanismen von Schadsoftware
   - ⇨ Wechseldatenträger

3. Hohe IT Sicherheitsanforderungen /spezielle Angriffstechniken: / (teilweise) mobiles Arbeiten:
   - Geschäftsführung und leitende Angestellte
   - Sachbearbeiter FI/CO
   - Sales Außendienstmitarbeiter

- Personalsachbearbeiter für Bewerbungsunterlagen

⇨ Schulung in verschiedensten spezialisierten Angriffstechniken (CEO Fraud, Phishing)

⇨ Sonderanforderungen Mobile Computing

⇨ Bedrohung Social Engineering

Die Intensität und Frequenz der Schulung sollte sich an der jeweiligen Klassifizierung orientieren. Für die Durchführung können Schulungssoftwaretools verwendet werden.

Zu A8: Messung des Lernerfolges

Die Messung des Lernerfolges sollte durch interne Tests, Erfahrungsabfragen der jeweiligen Vorgesetzten und regelmäßige Überprüfungen erfolgen. Es bieten sich auch ggf. bewusste Lernvirenangriffe (Penetration Test) kombiniert mit entsprechenden Informationen an. Auf Basis der jeweiligen Lernerfolgskennzahlen sollten dann gezielte Folge/Wiederholungsschulungen durchgeführt werden.
Hierzu können einerseits vom BSI zertifizierte IT-Sicherheitsdienstleister in den Bereichen IT-Revision und IT-Penetrationstests eingesetzt werden.
Des Weiteren ist der Einsatz von Schulungssoftware neben dem Zweck der Schulung auch zur Kontrolle des Gelernten in Kombination mit Testangriffen möglich.

Zu 9: Spezielle Schulungen

Auf Grund der aktuellen Situation einer erheblichen Zunahme von Homeoffice Arbeitsplätzen sollten diese Mitarbeiter ggf. zielgerichtet im Hinblick auf die Gefahren von Homeoffice zusätzlich geschult werden. (siehe BSI Homeoffice) Neben der IT Sicherheit ist auch die Datensicherheit zu beachten, da im Homeoffice im Normalfall von einem geringeren physikalischen Sicherheitslevel ausgegangen werden muss. Es sollte in Zusammenarbeit mit dem Datenschutzbeauftragten des Unternehmens ebenfalls ein Hinweis auf die Datenschutzrichtlinien erfolgen, die auch im Homeoffice beachtet werden müssen.