accenture

Empfehlungen zu IT-Sicherheit (Mindest-) Standards

IT-Sicherheits-Strategie

Umsetzung und Dokumentation einer IT-Sicherheits-Strategie, um alle notwendigen IT-Sicherheits-Anforderungen konkret zu definieren und strategische Anforderungen zu beschreiben.

IT Governance und Organisation

Implementation einer IT-Sicherheitsorganisationsstruktur (Organigramm, RACI Matrix) mit Definition von notwendigen Aufgaben, Rollen und Verantwortlichkeiten (z.B. IT-Sicherheitsbeauftragter, IT Risk Manager, IT Compliance Manager, IT-Sicherheitsgremium) sowie Reporting-strukturen.

Training und Awareness

Ein Schulungskonzept zum Thema IT-Sicherheit sollte im Einklang mit den Sicherheitsrichtlinien erarbeitet und regelmäßig auf Basis von gewonnenen Erkenntnissen aus ua. Informationssicherheits-Vorfällen aktualisiert werden.

IT-Risikomanagement

Die Erstellung einer IT-Risikomanagement-struktur mit Risikomanagementlebenszyklus und -prozess sowie einem Behandlungsplan zur Überwachung und Reporting von IT-Risiken sollte durchgeführt werden.

Benutzer- und Berechtigungsmanagement

Erstellung der notwendigen Prozesse für Benutzer- und Berechtigungsmanagement unter Berücksichtigung von IT-Sicherheitsprinzipien, wie z.B. Aufgabentrennung (Segregation of Duties), geringsten Rechte (Principle of Least Privilege) und “Kenntnis nur bei Bedarf“ (Need to Know).

IT Betriebskontinuitäts-Management und Notfallplanung

Umsetzung angemessener Vorkehrungen, um die Kontinuität und Ordnungsmäßigkeit der IT-unterstützenden Tätigkeiten im Unternehmen zu gewährleisten.

Updates und Sicherheitspatches

Update und Sicherheitspatches sollten zeitnah eingespielt werden. Es wird empfohlen, das Patchmanagement und der dafür notwendige Prozess unter Einbezug jeglicher Software (inkl. Firmware) zu definieren.

Backup / Datensicherungen

Ein Datensicherungskonzept sollte vorhanden und umgesetzt sein. Eine mögliche Manipulation der Sicherungskopien sollte mittels technischer Maßnahmen (z.B. für den Fall einer Ransomeware-Attacke) verhindert werden.

Protokollierung und Überwachung

Festlegung von Prozessen für die regelmäßige Aufzeichnung von Ereignissen in den IT-Systemen (Benutzeraktivitäten, Fehler, Sicherheitsereignis, Administratoraktivitäten, ...) und für die sichere Aufbewahrung der Log- und Protokolldateien zum Schutz vor Manipulation und unerlaubtem Zugriff.

Kommunikationssicherheit

Mobile Datenträger (z.B. Mobilgeräte) sollten entsprechend gesichert, verschlüsselt und mithilfe von Passwörtern geschützt werden. Maßnahmen zum Umgang und zur Entsorgung von Datenträgern sollten definiert sein. Firmenserver sollten mit einer Firewall geschützt sein.

Weiterführende Informationen zum Thema IT-Sicherheit

- Finanzmarktaufsichtsbehörde (FMA) Leitfäden zum Thema IT-Sicherheit https://www.fma.gv.at/fma/fma-leitfaeden/
- Wirtschaftskammer Österreich (WKO) https://www.wko.at/service/innovation-technologie-digitalisierung/it-sicherheit-datensicherheit.html
- IKT-Sicherheitsportal Österreich https://www.onlinesicherheit.gv.at/
- Gesamtverband der Deutschen Versicherungswirtschaft e.V. (Der GDV) https://www.gdv.de/de/themen/schwerpunkte/cybersecurity
- Allianz für Cyber-Sicherheit https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/ErsteSchritte/Erste_Schritte_node.html
- Bundesamt für Sicherheit in der Informationstechnik https://www.bsi.bund.de/DE/Home/home_node.html

Weitere Details - Empfehlungen zu IT-Sicherheit (Mindest-)Standards

IT-Sicherheits-Strategie

Diese sollte diverse strategische Sicherheits-Anforderungen beschreiben, wie zum Beispiel die Steuerung der IT-Sicherheit sowie Definitionen von Grundsatzstrategien zu den Themen der IT-Landschaft, IT-Notfallpläne und Lebenszyklusmanagement. Die IT Sicherheits-Strategie sollte unter Einbindung aller relevanten Stakeholder in regelmäßigen Abständen diskutiert und auf Aktualität sowie Erreichung überprüft werden.

IT Governance und Organisation

Erstellung und Implementierung einer IT-Sicherheitsorganisationsstruktur (Organigramm, RACI Matrix), Definition von notwendigen Aufgaben, Rollen und Verantwortlichkeiten (z.B. IT-Sicherheitsbeauftragter, IT Risk Manager, IT Compliance Manager, IT-Sicherheitsgremium) sowie Reportingstrukturen. Bei der Definition der Aufgaben, Rollen und Verantwortlichkeiten sollte auf Interessenskonflikte geachtet und nach dem Prinzip „Segregation of Duties“ gehandelt werden.

Training und Awareness

Ein Schulungskonzept zum Thema IT-Sicherheit sollte im Einklang mit den Sicherheitsrichtlinien erarbeitet und regelmäßig auf Basis von gewonnenen Erkenntnissen aus ua. Informationssicherheitsvorfällen aktualisiert werden. Hierbei können die Schulungen auf unterschiedlichen Kanälen wie Vorträge, Online Trainings, Selbststudium oder Kampagnen (z.B. Phishing-Nachrichten) durchgeführt werden. Schulungen sind nach dem Schulungskonzept in regelmäßigen Abständen durchzuführen. Empfohlen wird nicht nur die einführende Einschulung rasch nach dem Dienstantritt, sondern auch die regelmäßige Weiterbildung.

IT Risikomanagement

Die Erstellung einer IT-Risikomanagementstruktur mit Risikomanagementlebenszyklus und -prozess sowie einem Behandlungsplan zur Überwachung und Reporting von IT-Risiken sollte durchgeführt werden. IT-Risiken sollten entsprechend analysiert und behandelt werden, um mögliche negative Auswirkungen auf den IT-Betrieb und die operativen Kernprozesse des Unternehmens rechtzeitig zu erkennen und zu beheben. Weiters sollten IT-Risiken in den IT-abhängigen Kernprozessen im unternehmensweiten Risikomanagementprozess entsprechend berücksichtigt werden.

Benutzer- und Berechtigungsmanagement

Erstellung der notwendigen Prozesse für Benutzer- und Berechtigungsmanagement unter Berücksichtigung von IT-Sicherheitsprinzipien, wie z.B. Aufgabentrennung (Segregation of Duties), geringsten Rechte (Principle of Least Privilege) und “Kenntnis nur bei Bedarf“ (Need to Know).

Folgende Punkte sollten ua dabei berücksichtigt werden:

IT-Administrator einrichten, sparsam nutzen und für die tägliche Arbeit einen Zugang mit weit weniger Rechten nutzen

Individuelle Mitarbeiterzugänge einrichten und keine „Sammeluser“ verwenden (eigenen Benutzeraccount mit eigenem Passwort für jeden Mitarbeiter)

Komplexe Passwörter erzwingen (z.B. empfohlen min. 10 Zeichen, Sonderzeichen, Zahlen, Groß- und Kleinschreibung, …)

Die Authentifizierung von Benutzern muss auf sicheren Login Prozeduren basieren. Remote-Zugriffe sollten besonders abgesichert werden, wie zum Beispiel mittels Zwei-Faktor-Authentifizierung

IT Betriebskontinuitäts-Management und Notfallplanung

Umsetzung angemessener Vorkehrungen, um die Kontinuität und Ordnungsmäßigkeit der IT-unterstützenden Tätigkeiten im Unternehmen zu gewährleisten.

Folgende Punkte sollten ua dabei berücksichtigt werden:

- Erstellung eines unternehmensweiten Notfallplans, der alle relevanten Bedrohungsszenarien berücksichtigt und auf Basis einer Risikoanalyse ausgearbeitet wird
- Erarbeitung und Dokumentation der Reaktion auf diese Risiken; Festlegen von Maßnahmen, um den Risiken entgegenwirken zu können (siehe IT Risikomanagement)
- Entwicklung eines operativen Notfallplans unter Berücksichtigung der Szenarien aus der Risikoanalyse sowie Definition der Verantwortlichen für die jeweiligen Notfallszenarien
- Festlegung eines Prozesses zur Durchführung und Dokumentation von regelmäßigen Tests des Notfallplans
- Festlegung eines Prozesses für die laufende Weiterentwicklung des Notfallplans

Updates und Sicherheitspatches

Update und Sicherheitspatches sollten zeitnah eingespielt werden. Es wird empfohlen, das Patchmanagement und der dafür notwendige Prozess unter Einbezug jeglicher Software (inkl. Firmware) zu definieren.

Der Patchmanagement Prozess für IT-Systeme sollte ua beinhalten:

- Dokumentation (Test) von Updates und Patches
- Regelmäßige Überprüfung der Aktualität und Verteilung von Updates und Patches
- Programme (z.B. Antivirus) auf dem neuesten Stand halten
- Automatisierte Benachrichtigungen durch Hersteller einzurichten

Backup / Datensicherungen

Ein regelmäßiges (je öfter Daten gesichert werden, desto besser) Datensicherungskonzept sollte vorhanden und umgesetzt sein. Eine mögliche Manipulation der Sicherungskopien sollte mittels technischer Maßnahmen (z.B. für den Fall einer Ransomeware Attacke) verhindert werden. Sicherungskopien sollten in regelmäßigen Abständen getestet werden.

Protokollierung und Überwachung

Festlegung von Prozessen für die regelmäßige Aufzeichnung von Ereignissen in den IT-Systemen (Benutzeraktivitäten, Fehler, Sicherheitsereignis, Administratoraktivitäten, ...) und für die sichere Aufbewahrung der Log- und Protokolldateien zum Schutz vor Manipulation und unerlaubtem Zugriff.

Kommunikationssicherheit

Mobile Datenträger (z.B. Mobilgeräte) sollten entsprechend gesichert, verschlüsselt und mithilfe von Passwörtern geschützt werden. Maßnahmen zum Umgang und zur Entsorgung von Datenträgern sollten definiert sein. Darüber hinaus sollten die Daten auf Handys oder Laptops aus der Ferne gelöscht werden können. Firmenserver sollten mit einer Firewall geschützt sein. Um unberechtigten Zugriff und Sicherheitsvorfälle im Netzwerk erkennen zu können, sollte eine entsprechende Software und technische Maßnahmen zur Sicherheitsüberwachung (Monitoring, Angriffserkennung, Intrusion Detection, ...) definiert und umgesetzt werden.