

Bewertung der Informationssicherheit für Anwendungen

Autor	Beate Hansbach
Version	1.3

Inhalt

1	Zusammenfassung.....	2
2	Anwendungsübersicht.....	3
3	Verschlüsselung.....	5
4	Zugriffskontrolle und Authentifizierung	6
5	Sicherheit in Entwicklung und Betrieb	8
6	Standards und Konformitätskriterien	11
7	Datenschutz.....	13
8	Definitionen.....	14

Um einen hohen Sicherheitsstandard zu gewährleisten, führt die energie schwaben GmbH vor Beginn der Nutzung einer neuen Anwendung eine Sicherheitsbewertung für jede Anwendung und jeden Anbieter durch. Dieser Fragebogen gilt für alle Server- und Cloud-Anwendungen.

Die abgefragten Punkte beruhen auf den Vorgaben der ISO27001 und des BSI-Grundschatzes.

Diese Checkliste ist Teil des Managementsystem für Informationssicherheit (ISMS).

Weitere Informationen zum ISMS finden Sie unter folgendem Link: [Informationssicherheit](#)

Bitte geben Sie im Kommentar immer an, wie oder mit welcher Technologie die Frage gelöst wurde. Wenn eine der Fragen nicht mit dem Anwendungsbereich übereinstimmt, kennzeichnen Sie diese bitte mit N/A. Im Kommentar bitte eine Begründung für diese Auswahl hinterlegen.


1 Zusammenfassung

1.1 Zusammenfassung der Situation

(kurze Beschreibung der Anwendung und der Prozesse, ggf. Besonderheiten erläutern)

1.2 Offene Punkte

Diese Tabelle fasst die offenen Punkte der Detailbewertungen aus den Kapiteln 3 bis 7 zusammen.

Thema	Bewertung (rot/gelb/grün)	Offene Punkte
3 Verschlüsselung	  	
4 Zugriffskontrolle und Authentifizierung		
5 Sicherheit in Entwicklung und Betrieb		
6 Standards und Konformitätskriterien		
7 Datenschutz		

Erläuterung zur Bewertung:

Rot: Dieser Punkt ist ein Showstopper, d.h. die Anwendung kann ohne Lösung des Punktes nicht eingesetzt/genutzt werden.

Gelb: Dieser Punkt ist ein Risiko, aber kein Showstopper. Das Risiko ist durch geeignete Maßnahmen so weit als möglich zu reduzieren. Für einen Einsatz der Anwendung unter Beachtung des Risikos ist eine Entscheidung im IT Steuerboard oder auf GF-Ebene notwendig.

Grün: Hier gibt es keine offenen Punkt bzw. die aufgeführten offenen Punkte werden im Rahmen der Einführung der Anwendung gelöst/erledigt.

1.3 Bewertung des Risikos

Exposition der Anwendung	Hoch/mittel/niedrig
Kritikalität der Daten (siehe 2.1.4)	Hoch/mittel/niedrig
Restrisiko der offenen Punkte (siehe 1.2)	Hoch/mittel/niedrig
Eintrittswahrscheinlichkeit des Risikos	Hoch/mittel/niedrig
Bereits bekannte Sicherheitsvorfälle aus der Vergangenheit	Ja/nein; wenn ja, welche?

Gesamt Risikowert: hoch/mittel/niedrig

Bewertung der Informationssicherheit für Anwendungen

2 Anwendungsübersicht

2.1 Eckdaten

Frage	Antwort
2.1.1 Anwendungsname	
2.1.2 Anwendungsverantwortlicher intern	Name / Abteilung
2.1.3 Dienstleister extern	
2.1.4 Kritikalität der Anwendung hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit	Vertraulichkeit: öffentlich/intern/vertraulich Integrität: niedrig/mittel/hoch Verfügbarkeit: niedrig/mittel/hoch
2.1.5 Anwendung aus der Leittechnik	Ja/Nein (bei Ja, sind zusätzlich gesonderte Anforderungen ISMS zu beachten)

2.2 Exposure

Frage	Verantwortlich	Antwort	Kommentar
2.2.1 Wo wird die Anwendung betrieben?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
2.2.2 Wo wird die Hardware betrieben? (Region)	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
2.2.3 Besteht eine Schnittstelle / Verbindung ins interne Netzwerk	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
2.2.4 Welche Art von Schnittstelle besteht?	Wählen Sie ein Element aus.		

2.3 Architektur

Frage	Verantwortlich	Antwort	Kommentar
2.3.1 Bitte fügen Sie ein Bild der Architektur bei	Wählen Sie ein Element aus.	Bitte geben Sie den Namen des Dokuments und den Ablageort an	

2.4 Dokumentation

Frage	Verant- wortlich	Antwort	Kommentar
2.4.1 Wie und wo sind die Anwendung und ihre dazugehörigen Prozesse dokumentiert?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	

3 Verschlüsselung

3.1 Verschlüsselung

Frage	Verantwortlich	Antwort	Kommentar
3.1.1 Sind die gespeicherten Daten mit einer aktuellen Methode verschlüsselt?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
3.1.2 Werden die übertragenen Daten mit einem aktuellen Verfahren verschlüsselt?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	

4 Zugriffskontrolle und Authentifizierung

4.1 Zugriffskontrolle

Frage	Verantwortlich	Antwort	Kommentar
4.1.1 Wird die Anwendung von einem oder mehreren Benutzern genutzt?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	Anzahl der Benutzer angeben
4.1.2 Wird die Anwendung auch von Dritten (DL, Lieferanten) genutzt?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
4.1.3 Verfügen die Benutzer über differenzierte Zugriffsrechte (Rollen)?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
4.1.4 Gibt es ein formales Verfahren für die Zuweisung von Zugriffsrechten?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	Bei Vertraulichkeit intern oder vertraulich: 4-Augen Prinzip
4.1.5 Gibt es ein formales Verfahren für den Entzug von Zugriffsrechten?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
4.1.6 Wie werden inaktive Benutzer deaktiviert?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
4.1.7 Werden die Zugriffsrechte regelmäßig überprüft?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	

4.2 Authentifizierung

Frage	Verantwortlich	Antwort	Kommentar
4.2.1 Ist die Anwendung an einen zentralen Authentifizierungsdienst angebunden? (vorzugsweise über M365 & EntraID)	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
4.2.2 Welche Art von Identität wird für die Anwendung verwendet?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
4.2.3 Welche Methode wird für die Authentifizierung verwendet?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
4.2.4 Ist eine Multi-Faktor-Authentifizierung konfiguriert?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	MUSS, wenn die Anwendung nicht an den internen AUTH-Dienst angebunden ist.
4.2.5 Ist eine IP-Beschränkung konfiguriert?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
4.2.6 Ist eine Zeitüberschreitungs-sperre konfiguriert?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
4.2.7 Welches Authentifizierungsprotokoll wird verwendet?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	

5 Sicherheit in Entwicklung und Betrieb

5.1 Entwicklung

Frage	Verantwortlich	Antwort	Kommentar
5.1.1 Wie ist die Entwicklung organisiert?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.1.2 Existieren separate Entwicklungs- und Testumgebungen?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.1.3 Sind Entwicklungs- und Testumgebung im Hinblick auf die IT Sicherheit genauso konfiguriert wie die Produktivumgebung?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.1.4 Wird der Code auf der Grundlage bewährter Sicherheitspraktiken, z.B. OWASP Top 10, überprüft?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.1.5 Wird vor der Inbetriebnahme ein Penetrationstest durchgeführt?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	

5.2 Dateneingaben

Frage	Verantwortlich	Antwort	Kommentar
5.2.1 Wird die Anwendung vor Code Injections geschützt?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.2.2 Sind Datei-Uploads auf bestimmte Datei-Typen beschränkt und werden Dateien auf Malware etc. gescannt?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	

5.3 Konfiguration

Frage	Verant- wortlich	Antwort	Kommentar
5.3.1 Werden Patches regelmäßig bereitgestellt und installiert?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.3.2 Liegt ein Härtungskonzept vor?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	

5.4 Backup

Frage	Verant- wortlich	Antwort	Kommentar
5.4.1 Gibt es einen Backupprozess für Konfigurationsdaten?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.4.2 Gibt es einen Backupprozess für Benutzerdaten?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.4.3 Wird die Wiederherstellung der Daten regelmäßig getestet?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.4.4 Wie wird das Backup gespeichert? (Technologie)	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.4.5 Wo wird das Backup aufbewahrt? (Standort)	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	

5.5 Monitoring / Logging

Frage	Verantwortlich	Antwort	Kommentar
5.5.1 Werden Benutzeraktivitäten protokolliert?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.5.2 Werden Aktivitäten privilegierter Benutzer (z. B. Administratoren) protokolliert?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.5.3 Werden sicherheitsrelevante Ereignisse gespeichert?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.5.4 Werden die Protokolle regelmäßig überprüft?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.5.5 Ist sichergestellt, dass die Protokolle nicht manipuliert werden können? (z.B. durch Verschlüsselung)	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
5.5.6 Ist eine Archivierung der Protokolle aufgrund von Compliance-Rahmenbedingungen oder gesetzlichen Bestimmungen erforderlich?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	

6 Standards und Konformitätskriterien

6.1 Administration

Frage	Verantwortlich	Antwort	Kommentar
6.1.1 Gibt es einen formalen Prozess für das Management von Schwachstellen?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
6.1.2 Gibt es einen formalen Prozess für die Versionsverwaltung?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
6.1.3 Gibt es einen formalen Prozess für das Änderungsmanagement?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
6.1.4 Gibt es einen formalen Prozess für Notfälle?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
6.1.5 Gibt es einen formalen Prozess für die sichere Administration?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	

6.2 Abhängigkeiten

Frage	Verantwortlich	Antwort	Kommentar
6.2.1 Gibt es Abhängigkeiten zu anderen Systemen, Anwendungen oder Anbietern? (Wenn ja, bitte alle im Kommentarfeld auflisten)	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	

6.3 Lieferant

Frage	Verant- wortlich	Antwort	Kommentar
6.3.1 Gibt es ein Service Level Agreement (SLA)?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
6.3.2 Hat der Anbieter sicherheitsbezogene Zertifizierungen?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
6.3.3 Wie wird der Support für die Anwendung gehandhabt?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
6.3.4 Liegt eine Ausstiegsstrategie vor?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
6.3.5 Gibt es eine Kontaktperson/Mail im Falle von Sicherheitsfragen/Vorfällen?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	<i>Kontaktdaten</i>

7 Datenschutz

7.1 Datenschutz und Verhinderung von Datenverlusten

Frage	Verantwortlich	Antwort	Kommentar
7.1.1 Werden mit der Anwendung personenbezogene Daten verarbeitet?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
7.1.2 Werden die Daten DSGVO konform verarbeitet?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
7.1.3 Wo werden die Daten gespeichert und verarbeitet? (Regional)	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	
7.1.4 Gibt es Maßnahmen zur Vermeidung von Datenverlusten und Datenlecks?	Wählen Sie ein Element aus.	Wählen Sie ein Element aus.	Auflistung der Maßnahmen

8 Definitionen

Begriff	Definition