CHECKLISTE ZUR CYBER-SECURITY

für kleine und mittlere Einrichtungen

1 Einleitung

1.1 Zielsetzung

Die Absicherung von IT-Infrastrukturen ist eine komplexe Aufgabe, die einen methodischen Ansatz erfordert. Der damit verbundene Aufwand ist gerade für kleine und mittlere Einrichtungen oft nicht zu leisten. Die folgende Themenliste stellt daher eine Auswahl von besonders relevanten Handlungsfeldern zusammen und verweist auf entsprechende Empfehlungen aus den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Je Themenfeld werden einige ausgewählte Anforderungen benannt, durch deren Umsetzung maßgeblich die Informationssicherheit positiv beeinflusst werden kann. Die Themenliste kann ein methodisches IT-Sicherheitskonzept nicht ersetzen, gibt aber dort eine Umsetzungshilfe, wo ein Sicherheitskonzept nicht vorliegt oder nicht praktikabel realisierbar ist.

Das BSI hat zu den nachfolgend aufgeführten Themenfeldern IT-Grundschutz-Bausteine verfasst. Jeder dieser Bausteine enthält eine kurze Beschreibung der jeweiligen Thematik und des Ziels, das mit der Umsetzung des Bausteins erreicht werden soll. Zudem gibt es einen Überblick über die spezifischen Gefährdungen des betrachteten Themengebietes. Schwerpunkte eines jeden Bausteins sind die Sicherheitsanforderungen. Diese gliedern sich in Basis- und Standardanforderungen sowie Anforderungen mit erhöhtem Schutzbedarf. Für die Umsetzung der Anforderungen dienen die drei Abstufungen als Orientierung. Basisanforderungen stellen grundlegende Sicherheitsanforderungen dar, deren Umsetzung als essenziell für die Informationssicherheit eingeschätzt wird. Im nächsten Schritt sollten Standardanforderungen erfüllt werden. Die Umsetzung von Anforderungen für hohen Schutzbedarf sollte je nach Schutzbedarf der Geschäftsprozesse im Unternehmen umgesetzt werden. Als ergänzende Hilfestellung hat das BSI mit Buchstaben gekennzeichnet, auf welche Grundwerte die Anforderung maßgeblich hinwirkt (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

Zusätzlich zu den Sicherheitsanforderungen gibt es zu einigen Bausteinen des IT-Grundschutz-Kompendiums Umsetzungshinweise. Diese beschreiben, wie die Anforderungen der Bausteine in der Praxis erfüllt werden können, und enthalten dafür passende Sicherheitsmaßnahmen mit detaillierten Beschreibungen, die auf dem Erfahrungsschatz und den Best Practices des BSI und von IT-Grundschutz-Anwendern basieren.

1.2 Zielgruppe

Die folgende Themenliste richtet sich insbesondere an kleine und mittlere Unternehmen (KMU), für die aufgrund der überschaubaren Größe die Einführung eines kompletten Informationssicherheitsmanagementsystems (ISMS) unverhältnismäßig erscheint. Hierbei gilt zu berücksichtigen, dass auch für KMU die Einführung eines ISMS erforderlich sein kann, z. B. aufgrund vertraglicher Anforderungen oder des Schutzbedarfes von Geschäftsprozessen. Dabei umfasst der Schutzbedarf die Anforderungen hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität der Geschäftsprozesse und dazu erforderlichen Assets.

2 Anforderungen an die Organisation

2.1 Organisationsstrukturen für die Informationssicherheit

Unabhängig vom Aufbau eines Informationssicherheitsmanagementsystems sollten grundlegende Strukturen für die Wahrung der Informationssicherheit im Unternehmen geschaffen werden. Es sollten Verantwortlichkeiten und Kompetenzen definiert werden und im Rahmen dessen sollten Zielsetzungen für die Informationssicherheit festgelegt werden. Um diese erreichen zu können, sollte geprüft und definiert werden, in welche Prozesse und Gremien die Informationssicherheit als fester Bestandteil eingebettet und die Verantwortlichen eingebunden werden sollten.

Referenz	Anforderung	Umgesetzt
ISMS.1.A1	Übernahme der Gesamtverantwortung für Informationssicherheit und Unterstützung der Informationssicherheit durch die Leitungsebene	☐
ISMS.1.A2	Festlegung und Bekanntmachung der Sicherheitsziele und -strategie	☐
ISMS.1.A3	Erstellung und Bekanntmachung einer Leitlinie zur Informationssicherheit	☐
ISMS.1.A4	Benennung und Einbindung eines Informationssicherheitsbeauftragten	☐
ISMS.1.A6	Aufbau einer geeigneten und angemessenen Organisationsstruktur für Informationssicherheit	☐
ISMS.1.A9	Integration der Informationssicherheit in wesentliche organisationsweite Abläufe, Gremien und Projekte	☐

Weiterführende Links

- Baustein ISMS.1 Sicherheitsmanagement
- Umsetzungshinweise zu ISMS.1 Sicherheitsmanagement

2.2 Einbindung und Sensibilisierung der Mitarbeitenden

Die Mitarbeitenden sind ein notwendiger und bedeutender Erfolgsfaktor, um Informationssicherheit erfolgreich und effizient zu verwirklichen. Daher müssen sich alle Mitarbeitenden über ihre Rolle und ihren Einfluss auf die Informationssicherheit bewusst sein. Durch die Vermittlung der Sicherheitsziele sowie durch die Sensibilisierung für Gefahren für die Institution sollte ein Sicherheitsbewusstsein (Awareness) bei den Mitarbeitenden geschaffen werden. Die Wirkung von Sicherheitsmaßnahmen sollte erläutert werden, um die Bereitschaft der Mitarbeitenden für die Mitwirkung und Umsetzung zu gewinnen.

Referenz	Anforderung	Umgesetzt
ORP.3.A6	Durchführung von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit für die Mitarbeitenden (z. B. Umgang mit vertraulichen Informationen, Sicherheit beim mobilen Arbeiten, Warnung vor Social Engineering und weiteren Gefahren)	☐
ORP.3.A3	Einweisung von Mitarbeitenden in den sicheren Umgang mit IT-Geräten	☐
ORP.1.A15	Bekanntmachung von Ansprechpersonen für Sicherheitsfragen	☐
ORP.1 INF.9.A8	Erstellung von Arbeitsanweisungen/Richtlinien für die Mitarbeitenden für spezielle Themen, z. B. Umgang mit betriebsfremden Personen oder mobiles Arbeiten	☐
ORP.2	Verpflichtung der Mitarbeitenden zur Einhaltung der Sicherheitsvorgaben	☐

Weiterführende Links

- » Baustein ORP.3 Sensibilisierung und Schulung
- » Umsetzungshinweise zu ORP.3 Sensibilisierung und Schulung
- » Baustein ORP.1 Organisation
- » Baustein ORP.2 Personal
- » Baustein INF.9 Mobiler Arbeitsplatz

2.3 Sicherheitsvorfall- und Notfallmanagement

Um bei Eintritt von Ereignissen die Schäden zu begrenzen und weitere Schäden zu vermeiden, müssen diese frühzeitig erkannt und effizient bearbeitet werden. Es sollten sowohl Verfahren zur Meldung und Behandlung von Sicherheitsvorfällen als auch zur Bewältigung von Notfällen etabliert werden.

Unter einem Sicherheitsvorfall werden generell alle Ereignisse gefasst, welche die Grundwerte Verfügbarkeit, Vertraulichkeit und Integrität von Informationen gefährden.

Als Notfall bezeichnet das BSI alle Schadenereignisse, bei dem Prozesse bzw. Ressourcen nicht vorgesehen funktionieren und nicht innerhalb der tolerierbaren Ausfallzeit wiederhergestellt werden können. Der Geschäftsbetrieb ist soweit beeinträchtigt, dass eine Behebung innerhalb des normalen Tagesgeschäfts nicht mehr möglich ist. Zudem ist mit hohen bis sehr hohen Schäden zu rechnen.

Referenz	Anforderung	Umgesetzt
DER.2.1.A1	Definition von Sicherheitsvorfall und Notfall für das Unternehmen	☐
DER.2.1.A3/8 DER.4.A5	Aufbau geeigneter Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen, Notfällen und Krisen (inkl. Definition von Kompetenzen)	☐
DER.2.1.A15 DER.4.A8	Sensibilisierung der Mitarbeitenden für Sicherheitsvorfälle bzw. Notfälle	☐
DER.2.1.A4 DER.4.A8	Definition und Bekanntmachung von Meldewegen für potenzielle und eingetretene Sicherheitsvorfälle bzw. Notfälle (inkl. Pflege von Alarmierungslisten)	☐
DER.4.A16	Vereinbarung von Service Level Agreements und Meldewegen mit Dienstleistern	☐

Weiterführende Links

- » Baustein DER.2.1 Behandlung von Sicherheitsvorfällen
- » Baustein DER.4 Notfallmanagement
- » BSI-Standard 100-4, Version 1.0, November 2008

3 Anforderungen an den IT-Betrieb

3.1 Sichere IT-Administration

Die sichere und kontinuierliche Administration von IT-Systemen und -Komponenten ist für den IT-Betrieb grundlegend. Die Systemadministratoren richten IT-Systeme und Anwendungen ein, beobachten den Betrieb und reagieren mit Maßnahmen, die die Funktion, die Leistungsfähigkeit und Sicherheit der Systeme erhalten. Um diese Aufgaben wahrnehmen zu können, verfügen Administratoren über sehr weitreichende Berechtigungen und haben damit maßgeblichen Einfluss auf die Informationssicherheit. Dementsprechend bedarf es klarer Regelungen und Sicherheitsmaßnahmen, um die Systemadministration vor unbefugten Zugriffen abzusichern.

Referenz	Anforderung	Umgesetzt
ORP.2.A7, ORP.2.A15	Sorgfältige Personalauswahl von IT-Administratoren hinsichtlich Sicherheitsanforderungen und fachlicher Qualifikation	☐
OPS.1.1.2.A2	Definition von Vertretungsregelungen für den IT-Betrieb	☐
OPS.1.1.2.A3 und A4	Geregelter Ein- und Austritt von Administratoren, inkl. Rechtevergabe bzw. -entzug und Weitergabe von Wissen	☐
OPS.1.1.2.A7	Definition von Regeln für die IT-Administration, insbesondere Befugnisse, Aufgaben und Pflichten	☐
OPS.1.1.2. A12, OPS.1.2.5	Vorgaben für Wartungs- und Reparaturarbeiten sowie Fernzugriffe	☐

Weiterführende Links

» **Baustein OPS.1.1.2 Ordnungsgemäße IT-Administration**

» **Umsetzungshinweise zu OPS.1.1.2 Ordnungsgemäße IT-Administration**

3.2 Datensicherung

Um die Verfügbarkeit von Informationen sicherzustellen, sind regelmäßige Datensicherungen zu erstellen. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen, z. B. durch defekte Hardware, Schadsoftware oder Verlust eines Gerätes.

Referenz	Anforderung	Umgesetzt
CON.3.A2	Festlegung der Verfahrensweise (Art, Häufigkeit, Zeitpunkt) der Datensicherung auf Basis der Anforderungen an die Verfügbarkeit	☐
CON.3.A5	Durchführung regelmäßiger Datensicherungen	☐
CON.3.A.10	Verpflichtung der Mitarbeitenden Datensicherungen durchzuführen, falls Daten lokal gespeichert werden	☐
CON.3.A12/ A13	Angemessener Schutz der Datensicherungen, z. B. Verschlüsselung vertraulicher Daten und Schutz vor physischer Zerstörung	☐

Weiterführende Links

» **Baustein CON.3 Datensicherungskonzept**

» **Umsetzungshinweise zu CON.3 Datensicherungskonzept**

3.3 Patch- und Change-Management

Stetig steigende Anforderungen an IT-Systeme sowie Sicherheitslücken und Störungen erfordern zeitnahe Anpassungen und Aktualisierungen der IT-Systeme. Ein fehlendes oder vernachlässigtes Patch- und Änderungsmanagement führt schnell zu Fehlern oder Lücken in der Sicherheit einzelner Komponenten und damit zu möglichen Angriffspunkten. Aufgabe des Patch- und Änderungsmanagements ist es allgemein, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozessen und Verfahren steuer- und kontrollierbar zu gestalten.

Referenz	Anforderung	Umgesetzt
OPS.1.1.3.A2	Festlegung von Verantwortlichkeiten für das Patch- und Change-Management	☐
OPS.1.1.3.A3	Konfiguration von Autoupdate-Mechanismen	☐
OPS.1.1.3.A5 bis A9	Etablierung eines Prozesses für das Patch- sowie Change-Management (Planung, Abstimmung Anforderungen, Genehmigungs-, Test- und Freigabeverfahren etc.)	☐
OPS.1.1.3.A11	Dokumentation von Patches und Änderungen (Changes)	☐

Weiterführende Links

» **Baustein OPS.1.1.3 Patch- und Änderungsmanagement**

» **Umsetzungshinweise zu OPS.1.1.3 Patch- und Änderungsmanagement**

3.4 Schutz vor Schadprogrammen und Angriffen

Schadprogramme sind Programme, die in der Regel ohne Wissen und Einwilligung des Benutzers oder Besitzers eines IT-Systems schädliche Funktionen auf diesem ausführen. Diese Funktionen können ein breites Feld abdecken, das von Spionagemöglichkeiten über Erpressung (sogenannte Ransomware) bis hin zur Sabotage und Zerstörung von Informationen oder gar Geräten reicht.

Schadprogramme können grundsätzlich auf allen Betriebs- und IT-Systemen auftreten. Dazu gehören neben klassischen IT-Systemen wie Clients und Server auch mobile Geräte wie Smartphones. Netzkomponenten wie Router, Industriesteuerungsanlagen und sogar IoT-Geräte wie vernetzte Kameras sind heutzutage ebenfalls vielfach durch Schadprogramme gefährdet.

Referenz	Anforderung	Umgesetzt
OPS.1.1.4.A3 bis A6	Auswahl, Einsatz und Pflege von Virenschutzprogrammen für Endgeräte, für Gateways und IT-Systeme zum Datenaustausch	☐
OPS.1.1.4.A7	Sensibilisierung der Mitarbeitenden für den sicheren Umgang mit IT, inkl. regelmäßige und anlassbezogene Warnung vor Gefahren wie Spam-E-Mails	☐
APP.6	Prüfung der Integrität von Software und Daten sowie Verwendung sicherer Quellen	☐
OPS.1.1.3	Regelmäßiges Einspielen von Patches und Updates	☐

Weiterführende Links

- Baustein OPS.1.1.4 Schutz vor Schadprogrammen
- Umsetzungshinweis zu OPS.1.1.4 Schutz vor Schadprogrammen
- Baustein APP.6 Allgemeine Software

3.5 Protokollierung

Für einen verlässlichen IT-Betrieb sollten IT-Systeme und Anwendungen alle oder ausgewählte betriebs- und sicherheitsrelevante Ereignisse protokollieren, d. h. sie automatisch speichern und für die Auswertung bereitstellen. Eine Protokollierung wird in vielen Institutionen eingesetzt, um einerseits Hard- und Softwareprobleme sowie Ressourcenengpässe zeitnah entdecken und um andererseits Sicherheitsprobleme und Angriffe anhand von Protokollierungsdaten nachvollziehen zu können. Protokolldaten können im Zuge dessen durch forensische Untersuchungen als Beweise gesichert werden.

Referenz	Anforderung	Umgesetzt
OPS.1.1.5.A3	Konfiguration der Protokollierung auf System- und Netzebene	☐
ORP.1.A1 OPS.1.1.5.A9	Regelmäßige Auswertung der Protokolldaten (Definition der Verantwortlichkeiten hierfür)	☐
OPS.1.1.5.A5	Einhaltung der rechtlichen Rahmenbedingungen z. B. Mitbestimmungsrechte der Mitarbeitervertretung	☐
OPS.1.1.5.A10	Sicherstellung des Zugriffsschutzes und der angemessenen Aufbewahrung (Archivierung) von Protokolldaten	☐

Weiterführende Links

» **Baustein OPS.1.1.5 Protokollierung**

» **Umsetzungshinweis zu OPS.1.1.5 Protokollierung**

3.6 Nutzer- und Rechtemanagement

Benutzer oder auch IT-Komponenten, die auf Ressourcen einer Institution zugreifen, müssen zweifelsfrei identifiziert und authentisiert werden. Beim Berechtigungsmanagement geht es darum, ob und wie Benutzerinnen und Benutzer oder IT-Komponenten auf Informationen oder Dienste zugreifen und diese benutzen dürfen, ihnen also basierend auf dem Benutzerprofil Zutritt, Zugang oder Zugriff zu gewähren oder zu verweigern ist. Berechtigungsmanagement bezeichnet die Prozesse, die für Zuweisung, Entzug und Kontrolle der Rechte erforderlich sind. Generell sollten nur erforderliche Rechte vergeben werden „Need-to-know-Prinzip“.

Referenz	Anforderung	Umgesetzt
ORP.4.A2	Etablierung eines Prozesses für Einrichtung, Änderung und Entzug von Berechtigungen	☐
ORP.4.A5 bis A7	Regelung der Vergabe von Zugriffs-, Zugangs- und Zutrittsberechtigungen	☐
ORP.4.A8	Definition von Vorgaben zum Passwortgebrauch	☐

Weiterführende Links

» **Baustein ORP.4 Identitäts-. und Berechtigungsmanagement**

3.7 Kryptografie

Je nach Anforderungen an die Vertraulichkeit von Informationen sollten Verschlüsselungsverfahren eingesetzt werden. Beispielsweise kann der Bedarf bestehen, E-Mail-Kommunikation oder Festplatten zu verschlüsseln. Bei der Auswahl der Verfahren sollte der aktuelle Stand der Technik berücksichtigt werden. Hierzu bietet das Bundesamt für Sicherheit in der Informationstechnik umfangreiche Hilfestellungen, von denen einige unter „weiterführende Informationen“ aufgeführt sind.

Referenz	Anforderung	Umgesetzt
CON.1.A6	Prüfung des Bedarfs für Verschlüsselung (Kryptografie)	☐
CON.1.A1	Auswahl und Umsetzung geeigneter kryptografischer Verfahren	☐
CON.1.A2 und A4	Geeignetes Schlüsselmanagement und Datensicherung bei Einsatz von kryptografischen Verfahren	☐

Weiterführende Links

- Baustein CON.1 Kryptokonzept
- Kryptografische Verfahren – Empfehlungen und Schlüssellängen: BSI TR-02102, Bundesamt für Sicherheit in der Informationstechnik (BSI), Januar 2018

3.8 Cloud-Nutzung

Cloud-Dienstleistungen umfassen mittlerweile das komplette Spektrum der Informationstechnik und beinhalten unter anderem Infrastruktur (z. B. Rechenleistung und Speicherplatz), Plattformen und Software. Die IT-Dienste können bedarfsgerecht, skalierbar und flexibel genutzt und je nach Funktionsumfang, Nutzungsdauer und Anzahl der Benutzerinnen und Benutzer abgerechnet werden. Gleichzeitig bedarf es einer genauen Abwägung und Strategie, welche Dienste unter welchen Rahmenbedingungen über Cloud Computing bezogen werden sollen. Hierbei gilt es Anforderungen des IT-Betriebs sowie rechtliche und vertragliche Vorgaben zu berücksichtigen und zu regeln.

Referenz	Anforderung	Umgesetzt
OPS.2.2.A1	Erstellung einer Cloud-Nutzungsstrategie unter Beteiligung aller mitwirkenden Akteure (IT-Betrieb, Management, Datenschutz, ISB etc.)	☐
OPS.2.2.A4	Festlegung von Verantwortungsbereichen und Schnittstellen	☐
OPS.2.2.A8 und A9	Sorgfältige Auswahl und Vertragsgestaltung mit einem Cloud-Dienste-Anbieter	☐
OPS.2.2.A5 und A10	Planung und Umsetzung einer sicheren Migration zu einem Cloud-Dienst	☐

Weiterführende Links

» **Baustein OPS.2.2. Cloud-Nutzung**

» **Umsetzungshinweise zu OPS.2.2 Cloud-Nutzung**

2151.01/08.22

GRB Gesellschaft
für Risiko-Beratung mbH
Ecclesiastraße 1–4
32758 Detmold
Telefon + 49 5231 603-0
Fax + 49 5231 603-197

info@grb.de
www.grb.de

Ein Unternehmen
der Ecclesia Gruppe
www.ecclesia-gruppe.de

HiSolutions AG

Schloßstraße 1
12163 Berlin
Telefon +49 30 533 289-0
Fax +49 30 533 589-900

ecclesia@hisolutions.com
www.hisolutions.com