DAS CYBERRISK RATING by KSV1870

KSV1870

Anforderungen
CyberRisk Rating

basierend auf dem Cyber Risk Schema des KURATORIUM SICHERES ÖSTERREICH

Version 2.0

14. September 2021

Anforderungen für B-Rating

B1 Haben Sie eine aktuelle Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie), die für Ihr Unternehmen gültig ist?

Die Informationssicherheitsrichtlinie muss die wesentlichen Anforderungen an Informationssicherheit abdecken (alle Kernthemen müssen - sofern sie anwendbar sind - in dieser Richtlinie beschrieben werden) und sollte auf ein bestehendes Regelwerk aufbauen (zB. ISO 27002, NIST 800, IT Grundschutz, IT-Sicherheitshandbuch der WKO, u.ä.). Die Richtlinie muss von der Geschäftsführung freigegeben und für Mitarbeiter verfügbar sein.

EVIDENZEN

- Dokument muss vorhanden sein und die letzte Überprüfung darf nicht länger als zwei Jahre zurückliegen

---

B2 Schulen Sie Ihre Mitarbeiter regelmäßig in Informationssicherheit?

Die Schulung muss die Inhalte der Informationssicherheitsrichtlinie umfassen und auf aktuelle Bedrohungen eingehen. Die Inhalte müssen zumindest folgende Themen umfassen:

- -Sicherer Umgang mit Computern und Informationen
- -Passwörter richtig auswählen und verwalten
- -Sicher im Internet
- -E-Mails, Spam und Phishing
- -Gefährliche Schadprogramme (zB. Ransomware)
- -Verhalten und Vorgehen bei Verdacht auf IT Sicherheitsvorfall

Eine vollständige Schulung muss zumindest beim Eintritt stattfinden und aktualisierte Information muss zumindest alle zwei Jahre kommuniziert werden.

EVIDENZEN

- Schulungsunterlagen sowie Nachweis der Einschulung beim Eintritt

---

B3 Gibt es in Ihrem Unternehmen eine oder mehrere Personen, die für das Thema Informationssicherheit zuständig sind?

Es muss zumindest eine namentlich benannte Person geben, die für das Thema Informationssicherheit zuständig ist, d.h. die Richtlinie erstellt und sich um die Umsetzung der Maßnahmen kümmert und dafür die notwendige Zeit zur Verfügung gestellt bekommt. Diese Person muss das notwendige fachliche Grundwissen zu den Themen haben. Diese Tätigkeit kann neben anderen Tätigkeiten ausgeübt werden oder auch von Externen im Auftrag des Unternehmens wahrgenommen werden.

EVIDENZEN

- Nachweis der Qualifikation der benannten Person (kann auch Selbststudium sein, wenn dies glaubhaft gemacht werden kann)

B4 Pflegen Sie regelmäßig ein Verzeichnis all Ihrer IT-Assets und -Services sowie der damit verbundenen Verantwortlichkeiten?

Es muss ein Verzeichnis aller verwendeten Systeme geben. Dieses Verzeichnis muss zumindest Name und Version des Systems enthalten und den dafür Verantwortlichen.

EVIDENZEN

- Verzeichnis der Systeme

B5 Verwalten Sie den Zugang zu Ihren Systemen nach einem Berechtigungskonzept, das jedem nur die für seine Arbeit notwendigen Rechte einräumt?

Sowohl der Zugang zu den Anwendungen als auch zu den Dateisystemen muss reglementiert sein und über korrekt gesetzte Berechtigungen sichergestellt werden, dass nur die Personen zugreifen können, die aufgrund ihres Jobprofils einen Bedarf dafür haben. Es gibt eine Vorgehensweise zur Vergabe und Entzug von Berechtigungen.

EVIDENZEN

- Berechtigungskonzept oder Berechtigungslisten

B6 Verlangen Sie von Ihren Mitarbeitern für alle Anwendungen Passwörter mit einer sicheren Mindeststärke zu verwenden?

Es muss klar beschriebene Mindestkriterien für Passwörter geben, die die Empfehlungen aktueller Standards umsetzen (Passwortstärke, Zweifaktor-Authentifizierung wo notwendig und sinnvoll, Trennung Passworte, etc.). Referenz: BSI, NIST 800, etc.

EVIDENZEN

- Passwortrichtlinie (kann Teil der Sicherheitsrichtlinie sein)
- Setzen eines eigenen Passworts bei Zugang zum Assessment

B7 Verwenden Sie die vom Hersteller empfohlenen Sicherheitseinstellungen und achten Sie auf eine sichere Konfiguration all Ihrer IT-Systeme?

Es muss ein Dokument geben, dass die Anforderungen an die sichere Konfiguration der eingesetzten Systeme beschreibt. Verweise auf Herstellerempfehlungen sind ausreichend. Diese Einstellungen müssen auch auf allen verwendeten Geräten - soweit technisch möglich - tatsächlich umgesetzt sein. Alternativ wird ein Abnahmescan vor Inbetriebnahme durchgeführt.

EVIDENZEN

- Beschreibung der Anforderungen (bzw. schriftlicher Verweis auf Herstellerempfehlungen)
- Stichprobenartiger Nachweis auf Systemen

B8 Überprüfen Sie - sofern vorhanden - individuell entwickelte, aus dem Internet zugängliche Anwendungen auf Sicherheitslücken vor Inbetriebnahme?

Individualsoftware (zB. angepasste Open Source Software, aber nicht Standardsoftware), die aus dem Internet erreichbar ist, muss zumindest vor Inbetriebnahme durch einen Penetration Test auf Schwachstellen geprüft werden.

EVIDENZEN

- Penetration Test Bericht

B9 Aktualisieren Sie all Ihre IT-Systeme und Anwendungen regelmäßig mit Sicherheitsupdates?

Regelmäßige Aktualisierung der Systeme mit Updates, die vom Hersteller zur Verfügung gestellt werden. Kein Systemupdate darf länger als ein Quartal überfällig sein (außer es gibt einen dokumentierten Grund, warum ein Update nicht eingesetzt werden kann). Systeme, die nicht mehr vom Hersteller mit Sicherheitsupdates versorgt werden, werden rechtzeitig außer Betrieb genommen bzw. es gibt definierte Ausnahmeprozesse inklusive einer Abweichungsliste.

EVIDENZEN

- Versionsnachweise der verwendeten Betriebssysteme und der wichtigsten Softwareprodukte

---

B10 Sichern Sie Ihr Netzwerk vor unberechtigtem Zugriff von außen ab?

Es ist eine Netzwerk-Segmentierungseinrichtung (zB. Firewall, Router, etc.) im Einsatz, welche auf Basis möglichst restriktiv gesetzter Regeln den Netzwerkverkehr mit dem Internet filtert.

EVIDENZEN

- Versionsnachweise der verwendeten Systeme
- Regeln der Netzwerk-Segmentierungseinrichtung

B11 Überwachen Sie Ihre IT-Systeme auf Malware?

Es muss zumindest eine aktuelle Antivirussoftware im Einsatz sein, welche laufend die Systeme und Dateien auf Schadsoftware überprüft. Im Verdachtsfall erfolgt eine Alarmierung im Unternehmen.

EVIDENZEN

- Versionsnachweise der verwendeten Antivirussoftware
- Lizenz für alle verwendeten Geräte (gemäß Systemverzeichnis)

B12 Verschlüsseln Sie sensible Daten bei der Übertragung im Internet?

Es muss die Möglichkeit bestehen, Dateien verschlüsselt zu übertragen, entweder per eMail (zB. S/MIME, PDF verschlüsselt, mandatory enforced TLS, etc.) oder per verschlüsseltem Upload. Formulare auf der Webseite werden ausschließlich über https hochgeladen.

EVIDENZEN

- Nachweis der verwendeten Verschlüsselungsmechanismen

B13 Protokollieren Sie die Nutzung Ihrer IT-Systeme, um Sicherheitsvorfälle nachvollziehbar zu machen?

Es müssen zumindest die Standardprotokolle der Betriebssysteme aktiviert sein. Die Protokolle müssen dem Unternehmen zur Verfügung stehen. Es existiert eine Übersicht aller aktiven Systemprotokolle und deren Speicherort. Die Protokolle werden zumindest drei Monate aufbewahrt.

EVIDENZEN

- Übersicht der Systemprotokolle

B14 Haben Sie einen Notfallplan, anhand dessen Sie auf einen IT-Sicherheitsvorfall reagieren?

Der Notfallplan muss beschreiben, wie auf einen schwerwiegenden IT-Sicherheitsvorfall reagiert wird. Schwerwiegende Sicherheitsvorfälle sind zum Beispiel:

- Ausfall der Systeme,
- Schadsoftware-Befall (inkl. Kryptolocker) sowie
- Data Leakage

Die Pläne müssen mindestens alle zwei Jahre getestet werden.

EVIDENZEN

- Dokumentierter Notfallplan. Die letzte Aktualisierung darf nicht länger als zwei Jahre zurückliegen.
- Testnachweis

Anforderungen für A-Rating (zusätzlich zu B)

A1 Überprüfen Sie Ihre eingesetzte Software auf Sicherheitslücken?

Ein Tool zum Schwachstellenscannen muss im Einsatz sein und muss mindestens einmal pro Monat verwendet werden.

EVIDENZEN

- Monatliche Scanberichte

A2 **Haben Sie Mechanismen im Einsatz, die bei der Erstellung bzw. dem Erwerb von Software deren Sicherheit überprüft?**

Es gibt eine Policy zur sicheren Software-Entwicklung, welche Sicherheitsanforderungen, Secure Coding Rules sowie ein Testkonzept umfasst. Für den Erwerb von Software gibt es eine Sicherheits-Anforderungsliste und einen Prozess zur Risikoanalyse des Anbieters.

EVIDENZEN

- Policy zur sicheren Software-Entwicklung
- Sicherheits-Anforderungsliste für Software-Beschaffung

A3 **Führen Sie in Ihrer Systemlandschaft Penetration Tests durch?**

Zumindest alle zwei Jahre werden Penetration Tests durchgeführt, welche die Angreifbarkeit des Unternehmens prüfen. Aus den gefundenen Schwachstellen werden Maßnahmen abgeleitet und umgesetzt.

EVIDENZEN

- Prüfplan
- Prüfberichte

A4 **Überwachen Sie Ihre Netzwerke auf ungewöhnliche Aktivitäten und Anomalien?**

Es muss mindestens ein Intrusion Detection / Prevention System im Einsatz sein, das entweder über Baselining-Ansatz oder über heuristische Prozesse bzw. Machine Learning Verdacht auf unautorisierte Aktivitäten im Netzwerk identifizieren kann..

EVIDENZEN

- Versionsnachweise der verwendeten Systeme
- Netzwerkchart
- Netzwerk-Logs (mind. 1 Monat zurückreichend)

A5 Haben Sie Whitelisting im Einsatz, um die Ausführung nicht autorisierter Prozesse und Anwendungen zu unterbinden?

Auf allen Systemen (Clients/Servern) muss ein Mechanismus aktiv sein, der nur freigegebene Prozesse und Anwendungen ausführen lässt.

EVIDENZEN

- Dokumentation des Whitelisting-Mechanismus

A6 Verwalten Sie Identitäten und Berechtigungen aller Benutzer in nachvollziehbarer Weise?

Eine Identitäts- und Berechtigungsverwaltung ist im Einsatz, die alle Identitäten und deren Berechtigungen eindeutig auf Personenbasis nachvollziehbar macht. Die Berechtigungsverwaltung muss auch administrative-Berechtigungen sowie Berechtigungen für Zugänge zu Kundensystemen umfassen.

EVIDENZEN

- Beschreibung der verwendeten Prozesse (und ggf. Systeme)
- (Stichprobenartige) Berechtigungslisten für normale- und privilegierte Anwender

---

A7 Haben Sie ein Security Event & Information Management im Einsatz, das die Log Files Ihrer Systeme korreliert und analysiert?

Es ist ein SIEM im Einsatz, an das zumindest die kritischen Netzwerk- und Sicherheitssysteme angeschlossen sind und deren Logfiles laufend korreliert und auf Unregelmäßigkeiten analysiert werden.

EVIDENZEN

- Versionsnachweise der verwendeten Systeme
- Dokumentation der angebundenen Systeme
- SIEM-Berichte

A8 Haben oder nutzen Sie ein Security Operations Team?

Es müssen Mitarbeiter mit nachgewiesenen Qualifikationen im Bereich IT-Sicherheit im Unternehmen beschäftigt sein oder es muss ein SLA mit einem entsprechenden Unternehmen bestehen, das die laufende Überwachung übernimmt. Verdachtsfälle müssen untersucht werden und bei bestätigten Vorfällen muss eine Alarmierung stattfinden sowie – sofern relevant – betroffene Kunden informiert werden.

EVIDENZEN

- Dokumentation der Monitoring- und Incident-Handling-Prozesse ODER
- SLA mit externem SOC sowie Nachweis der Reports

A9 Können Sie auf qualifizierte Ressourcen zurückgreifen, wenn Sie einen schwerwiegenden Sicherheitsvorfall haben?

Es müssen Mitarbeiter mit nachgewiesenen Qualifikationen in den Bereichen vertiefte Incident Response und IT-Forensik im Unternehmen beschäftigt sein oder es muss ein SLA mit einem entsprechenden Unternehmen bestehen, bzw. der Zugriff auf ein solches muss über eine Cyberversicherung gedeckt sein.

EVIDENZEN

- Nachweis der (forensisch-technischen) Qualifikation der benannten Person(en) ODER
- SLA mit Dienstleister sowie Nachweis der Qualifikation des Dienstleisters ODER
- Cyberversicherungspolizze mit Leistungsbestandteil Forensik

---

A10 Verfügen Sie über ein getestetes Resilienzkonzept, das Ihre Betriebskontinuität sicherstellt?

Das Resilienzkonzept muss präventive und reaktive Maßnahmen umfassen, um auf schwere Sicherheitsvorfälle reagieren zu können und somit Betriebskontinuität sicherzustellen. Schwerwiegende Sicherheitsvorfälle sind unter anderem:

- Ausfall der Systeme,
- Schadsoftware-Befall (inkl. Kryptolocker) sowie
- Data Leakage
- Zielgerichtete Hackingangriffe (z.B. APTs)

Bei Betrieb kritischer Anwendungen in der Cloud müssen diese Maßnahmen und Tests vom Cloud-Betreiber nachgewiesen werden (z. B. über ISAE 3402-Berichte). Tests müssen mindestens einmal jährlich durchgeführt und notwendige Verbesserungsmaßnahmen umgesetzt werden..

EVIDENZEN

- Resilienzkonzept
- Teskonzept
- Testbericht

A11 **Haben Sie einen Prozess zum Management Ihrer Lieferantenrisiken?**

Es muss einen dokumentierten Prozess geben, welcher vorab und laufend sicherstellt, dass kritische Lieferanten ihre Risiken bezüglich Informationssicherheit und Business Continuity Management adäquat managen.

EVIDENZEN

- Prozessbeschreibung, Checklisten
- Standardverträge mit Lieferanten mit Sicherheitsanforderungen und Right to Audit

---

Fragen zum CyberRisk Rating?
So erreichen Sie uns:

Per E-Mail
crr@nimbusec.com

POWERED BY
nimbusec
Part of **KSV1870**

NIMBUSEC GMBH, EIN UNTERNEHMEN DER **KSV1870** GRUPPE

Nimbusec GmbH | Fadingerstraße 15 | 4020 Linz
FN 394170m | FBG Linz | UID ATU67830957
Behörde gem. ECG: Magistrat der Stadt Linz/Donau