KURATORIUM SICHERES ÖSTERREICH

CYBER TRUST AUSTRIA

Cyber Risk Rating & Cyber Trust Label

Schema Policy

Versionskontrolle

Version	Datum	Freigabe
1.0	8. September 2020	KSÖ Cyber Risk Advisory Board

Inhaltsverzeichnis

1 Einführung

Das Cyber Risk Rating und das darauf basierenden Cyber Trust Label stellen ein Schema zur Bewertung des Cyber Risk Status von Organisationen (Unternehmen, Vereinen, etc.) dar. Das vorliegende Dokument beschreibt alle relevanten Aspekte des Schemas. Dies soll sowohl den geprüften Organisationen als auch deren Kunden die notwendige Sicherheit (Assurance) in das vom Cyber Risk Rating bzw. vom Cyber Trust Label ausgedrückte, erwartbare Sicherheitsniveau der bewerteten Organisationen vermitteln.

Dieses Dokument basiert auf der internationalen Normierungsreihe für Konformitätsbewertungen (ISO/IEC 170xx, insbesondere ISO/IEC 17000 und ISO/IEC 17029) und wendet dieses sinngemäß an (siehe Begriffsbestimmungen).

Zielsetzung von Konformitätsbewertungen ist die Herstellung von Vertrauen in die bewerteten Organisationen, Produkte oder Prozesse. Eine Konformitätsbewertung zielt darauf ab, die Erfüllung definierter Anforderungen beim Bewertungsobjekt (z.B. einer Organisation) darzulegen (Assurance) und dies in geeigneter Weise zu demonstrieren. Der Wert einer solchen Bewertung wird bestimmt vom Vertrauen, das in das zugehörige Schema gesetzt wird. Dieses umfasst unter anderem die Anforderungen selbst, die Überprüfungsmethoden sowie die Steuerungsmechanismen zur Prüfung und Weiterentwicklung des Schemas.

2 Grundlegende Prinzipien und Ziele

Die grundlegenden Werte des Cyber Risk Ratings sowie des darauf basierenden Cyber Trust Labels sind Sicherheit und Vertrauen, ebenso wie Offenheit, Transparenz und Nachvollziehbarkeit. Das Rating sowie das Label sollen Vertrauen in die bewertete Organisation erzeugen, dass dieses das Thema Cybersicherheit ernst nimmt und in angemessener Weise behandelt. Durch Offenlegung des Schemas und der damit zusammenhängenden Kriterien und Bewertungsmethoden soll sichergestellt werden, dass dies in einer offenen, transparenten und nachvollziehbaren Art und Weise geschieht. Dies trägt wiederum dazu bei, dass die Aussagekraft des Ratings und des Labels gestärkt wird und Unternehmen darauf vertrauen können, dass gute geratete Organisationen sowie Organisationen, welche das Cyber Trust Label tragen, vertrauenswürdige Partner mit einem entsprechend niedrigen Cyber-Risiko sind.

Speziell die Anforderungen des B-Ratings stellen Basisanforderungen an die Cybersicherheit dar, die jede Organisation weitgehend erfüllen sollte. Eine starke Verbreitung von Organisationen mit einem guten B-Rating bzw. einem Cyber Trust Label ist somit eine positive Aussage über die Cyberresilienz eines Standorts. In diesem Sinne ist es auch eine der Zielsetzungen, durch die Einführung und Verbreitung des Cyber Risk Ratings eine Verbesserung der Cybersicherheit des Wirtschaftsstandorts Österreich zu erreichen.

Für jedes Unternehmen, das die Vertrauenswürdigkeit seiner Lieferanten hinsichtlich Cybersicherheit prüfen will, stellt das Cyber Risk Rating eine effiziente und effektive Methode dar, seiner Sorgfaltspflicht beim Third Party Risk Management nachzukommen. Betreiber wesentlicher Dienste sind gemäß § 11 Abs. 1 Z 2 iVm Anlage 1 NISV rechtlich verpflichtet, hinsichtlich des Umgangs mit Dienstleistern, Lieferanten und sonstigen Dritten

entsprechende Sicherheitsvorkehrungen zu treffen. Das vorliegende Schema zielt auf die Erfüllung dieser Anforderung ab, ersetzt aber nicht den notwendigen Nachweis eines Betreibers wesentlicher Dienste gemäß § 17 Abs. 3 NISG.

3 Cyber Risk Rating Schema

Das Cyber Risk Rating Schema beschreibt die Anforderungen, deren Erfüllung im Rahmen der Bewertung zu bestätigen ist, ebenso wie die Prüfmethoden und erforderlichen Nachweise, die zur objektiven Bewertung der Erfüllung bzw. Nichterfüllung herangezogen werden.

Das Cyber Risk Rating unterscheidet drei Bewertungsschemata, die sich in Bezug auf ihren Anspruch (*Security Claim*) als auch in Bezug auf die Rigorosität der Überprüfung (*Assurance Level*) unterscheiden: das B Rating, das A Rating sowie das A+ Rating. Aufbauend auf diesen Ratings wird weiters das Cyber Risk Label angeboten, welches als nach Außen sichtbares Qualitätsmerkmal für ein angemessenes Cybersicherheitsniveau steht.

3.1 B Rating

Das B-Rating bewertet den Anspruch eines Basissicherheitslevels (Baseline Security Claim) einer Organisation. Die definierten Anforderungen beziehen sich auf ein grundlegendes Schutzniveau, das von jeder Organisation (auch von kleinen) eingehalten werden sollte. Die gestellten Anforderungen und die verlangten Nachweise sind dementsprechend allgemein gehalten, erfordern aber dennoch eine definierte Mindestqualität, um den notwendigen Mindestsicherheitsanspruch zu gewährleisten.

Die Bewertungsmethode ist eine Selbstdeklaration der Organisation, es handelt sich demnach um ein *first-party conformity assessment*. Die Unternehmen bewerten hierbei selbst, inwiefern sie die vom Schema definierten Anforderungen im Rahmen der definierten Kriterien (siehe Anhang A) erfüllen und dies anhand der definierten Nachweise (Evidenzen) im Bedarfsfall auch nachweisen können. Um die Nachvollziehbarkeit und Plausibilisierung der Selbstbewertung zu gewährleisten, müssen die Organisationen zu jeder Frage eine Beschreibung abgeben, wie die Anforderung in der Organisation konkret erfüllt ist und welche Evidenzen im Bedarfsfall vorgelegt werden können. Im Rahmen der Validierung der vorgelegten Selbstdeklarationen wird von einem qualifizierten Prüfer (Mindestanforderungen an Validierer siehe Anhang B) eine Bewertung der Beschreibungen vorgenommen, inwiefern diese die Erfüllung der gestellten Anforderung hinreichend belegen. Um eine neutrale Bewertung sicherzustellen werden Selbstdeklarationen gegenüber dem Validierer anonymisiert. Sollte eine Beschreibung unvollständig oder unklar sein oder Fragen bezüglich der tatsächlichen Erfüllung offenlassen, so erfolgt eine Anfrage zur Klärung bei der bewerteten Organisation. Diese ist innerhalb zwei Wochen seitens der Organisation zu beantworten. Sollte dies unterbleiben oder die Klarstellung nicht in der erforderlichen Qualität erfolgen, so wird die gegenständliche Frage als nicht erfüllt bewertet. Spätere Klarstellungen können nur im Rahmen einer gänzlich neuen Risikobewertung vorgenommen werden. Um die Qualität der Selbstbewertung weiter zu erhöhen, verpflichten sich die bewerteten Organisationen im Rahmen der Rating-Vereinbarung, dem mit der Validierung betrauten Unternehmen bzw. einem Auditor auf Anfrage Zugang zu den beschriebenen Nachweisen (Evidenzen) zu gewähren. Dies kann

stichprobenartig im Rahmen der Validierung beziehungsweise im Rahmen eines Überprüfungs-Audits bei Verdacht auf Unregelmäßigkeiten erfolgen, zum Beispiel nach einem bekannt gewordenen schwerwiegenden Sicherheitsvorfall. Die bewertete Organisation muss demnach jederzeit in der Lage sein, auf Anfrage die Nachweise für die in der Selbstdeklaration getätigte Selbstbewertung vorlegen zu können.
Auf Basis der finalen validierten Selbstbewertung wird das B-Rating berechnet und der bewerteten Organisation mitgeteilt. Das Rating wird weiters in der KSV1870 Rating-Datenbank gespeichert.

Sollte sich herausstellen, dass im Rahmen der Selbstbewertung vorsätzlich oder grob fahrlässig Falschangaben gemacht wurden, treten die im Kapitel 3.7 beschriebenen Maßnahmen in Kraft. Jede Falschangabe stellt einen Verstoß gegen die Rating-Vereinbarung dar und kann zu einer Aussetzung des Ratings und (sofern vergeben) zu einem Entzug der Label-Nutzungslizenz führen.

3.2 A Rating

Das A Rating bewertet den Anspruch eines fortgeschrittenen Sicherheitslevels einer Organisation (Advanced Security Claim). Die definierten Anforderungen beziehen sich auf ein erhöhtes Schutzniveau, das von jeder Organisation eingehalten werden sollte, die aufgrund ihres Tätigkeitsfeldes einen erhöhten Sicherheitsanspruch hat.

Die Bewertungsmethode ist eine Selbstdeklaration der Organisation und erfolgt analog zu 3.1.

3.3 A+ Rating

Das A+ Rating bewertet ebenfalls den Anspruch eines fortgeschrittenen Sicherheitslevels einer Organisation (Advanced Security Claim). Es beruht auf denselben Anforderungen wie 3.2.

Die Bewertungsmethode ist ein unabhängiges Audit der Organisation, es handelt sich demnach um ein *third-party conformity assessment*. Die Organisation wird hierbei von einem unabhängigen qualifizierten Auditor überprüft, inwiefern es die vom Schema definierten Anforderungen im Rahmen der definierten Kriterien (siehe Anhang A) erfüllt. Dies erfolgt anhand der definierten Nachweise (Evidenzen), welche dem Auditor vorgelegt und plausibel gemacht werden müssen. Es obliegt der sachverständigen Bewertung des Auditors, ob die vorgelegten Evidenzen vollständig und stichhaltig sind, um die geforderten Anforderungen zu erfüllen. Es liegt weiters im Ermessen des Auditors, im Bedarfsfall weitere Evidenzen einzufordern oder stichprobenartige Überprüfungen vorzunehmen, um die Wirksamkeit der geforderten Anforderungen sicherzustellen (Mindestanforderungen an Auditoren siehe Anhang B). Auf Basis des durchgeführten Audits erstellt der Auditor einen Audit-Bericht, welcher zu jeder Anforderung festhält, ob diese - seiner sachverständigen Bewertung entsprechend - erfüllt ist oder nicht. Dieser Audit-Bericht wird der bewerteten Organisation zugänglich gemacht, worauf es innerhalb einer Frist von zwei Wochen die Möglichkeit des Einspruchs und des Begehrens auf Richtigstellung hat. Dazu sind dem Auditor gegebenenfalls weitere Evidenzen vorzulegen. Die Letztentscheidung der Bewertung liegt beim Auditor. Danach wird der Audit-Bericht an den KSV1870 übermittelt,

wo auf Basis des Berichts das A-Rating berechnet und der bewerteten Organisation mitgeteilt wird. Das Rating wird weiters in der KSV1870 Rating-Datenbank gespeichert.

3.4 C-Score

Der C-Score ist eine vollautomatisierte externe Sicherheitsprüfung, welche aus dem Internet zugängliche Anwendungen einer Organisation auf nicht intrusive Weise überprüft und aufgrund dessen Rückschlüsse auf die zugrundeliegende technische und organisatorische Cybersicherheit in diesem Bereich ermöglicht. Die zur Organisation gehörigen Domänen und IP-Adressbereiche, welche Bestandteil dieser Überprüfung sind, müssen bei der Beantragung bekannt gegeben werden und werden durch technisch zuordenbare, aus dem Internet zugängliche Anwendungen ergänzt. Der C-Score wird bei der Validierung der B- und A-Ratings als Indikator berücksichtigt und extra ausgewiesen. Falls die bewertete Organisation Einsprüche gegen den C-Score hat, kann es diese innerhalb einer Frist von zwei Wochen einbringen.

3.5 Cyber Trust Label

Das Cyber Trust Label baut auf dem Cyber Risk Rating auf. Es gibt zwei Arten von Cyber Trust Labels: das Cyber Trust Label sowie das Cyber Trust Label Gold. Das Recht zur Nutzung der Labels setzt das Erreichen eines Mindestratings beim Cyber Risk Rating voraus:

Label	Logo	Voraussetzung
Cyber Trust Label	CYBER TRUST AUSTRIA	Vorliegen eines gültigen B Ratings von 190 oder besser
Cyber Trust Label Gold	CYBER TRUST AUSTRIA	Vorliegen eines gültigen A+ Ratings von 190 oder besser

Das erreichte Label darf nach Erfüllung der Voraussetzungen und Bezahlung der Label Gebühr auf Printmedien und elektronischen Dokumenten sowie auf allen angegebenen Domänen (siehe 3.4) der qualifizierten Organisation zu Informations- und Werbezwecken angezeigt werden.

Die Nutzung des Cyber Trust Labels ohne gültigem Label-Nutzungsvertrag und aufrechten Voraussetzungen (gültiges, nicht-zurückgezogenes Mindestrating, siehe 3.7) stellt einen Verstoß gegen geltende Lizenz- und Markenrechte dar und wird zivilrechtlich geahndet.

3.6 Überwachung

Die Überwachung des Cyber Risk Ratings erfolgt auf jährlicher Basis. Dementsprechend hat ein Cyber Risk Rating eine Gültigkeitsdauer von einem Jahr, danach muss es erneut ermittelt werden. Dies gilt sowohl für das B Rating als auch für das A/A+ Rating. Das auf den

Cyber Risk Ratings basierende Cyber Trust Label muss daher ebenfalls jährlich erneuert werden.

3.7 Überprüfungs-Audits und Zurückziehung von Ratings

Der Wert eines Schemas bemisst sich an dem Vertrauen, das in dieses gesetzt wird. Dafür werden nach bestem Wissen und Gewissen die oben beschriebenen Prüfmechanismen eingesetzt. Kein Bewertungsschema kann jedoch eine hundertprozentige Aussage zum tatsächlichen Status Quo treffen, ebenso wie keine Sicherheitsmaßnahme hundertprozentige Sicherheit garantieren kann. Aus diesem Grund ist es wichtig, klare Regeln für den Umgang mit Vorfällen, Verdachtsfällen und Verstößen gegen die Rating-Vereinbarung festzulegen.

Grundsätzlich verpflichtet sich jede Organisation, die sich einem KSV1870 Cyber Risk Rating unterzieht, bereits vorab einem allfälligen Überprüfungs-Audit zuzustimmen. Überprüfungs-Audits können notwendig werden, wenn es einen schwerwiegenden Sicherheitsvorfall bei einer gerateten Organisation gegeben hat oder wenn es Verdachtsmomente zu Missbrauch oder Falschinformationen gibt. Weiters können Überprüfungs-Audits stichprobenartig ohne Angabe von Gründen durchgeführt werden. Die Entscheidung für die Durchführung eines Überprüfungs-Audits liegt beim KSV1870. Bei wahrheitsgemäßer Beantwortung der Fragen in der Selbstdeklaration sollte ein Überprüfungs-Audit das gleiche Risk Rating ergeben. Kleinere Abweichungen werden im Sinne von Ermessensspielräumen akzeptiert. Sollte die Abweichung im Risk Rating zwischen Selbstdeklaration und Überwachungsaudit jedoch mehr als 100 Punkte betragen, dann ist von vorsätzlichen oder grob fahrlässigen Falschangaben in der Selbstdeklaration auszugehen. In diesem Fall wird das Rating *zurückgezogen* und ein neues Ratingverfahren kann frühestens nach einer Cool-Off Periode von 6 Monaten – auf Kosten der Organisation – erneut durchgeführt werden. In der Zwischenzeit wird in der KSV1870 Rating Datenbank das Rating der Organisation als „Zurückgezogen“ gekennzeichnet. Weiters werden alle KSV1870 Kunden, die in den letzten 12 Monaten das Rating der betroffenen Organisation abgefragt hatten, über den Status „Zurückgezogen“ des zugehörigen Ratings informiert. Wenn das Rating zurückgezogen wird, erlischt auch das allfällige Nutzungsrecht des Cyber Risk Labels und dieses muss innerhalb von Monatsfrist von allen Unterlagen der Organisation entfernt werden. Wenn bei einer Organisation zweimal Abweichungen von mehr als 100 Punkten festgestellt werden, so werden von dieser Organisation nur noch A+ Ratings akzeptiert.

4 Steuerung des Cyber Risk Schemas

Der Owner des Cyber Risk Schemas ist das Kuratorium Sicheres Österreich als neutraler und überparteilicher Verein, der sich der Erhöhung der Cybersicherheit in Österreich verpflichtet sieht. Das KSÖ betreibt dazu das Cyber Risk Advisory Board, welches sich aus acht gewählten Repräsentanten der Betreiber wesentlicher Dienste gemäß NIS-Gesetz zusammensetzt: je einen Repräsentanten pro NIS-Sektor. Diese Repräsentanten sind fachlich qualifiziert und nehmen in ihrem jeweiligen Unternehmen eine verantwortliche Rolle zum Thema Cyber-Risiko ein. Sie bringen ihre Erfahrung und ihr Know-How zur Gestaltung und Weiterentwicklung des Cyber Risk Schemas ein, um dieses bestmöglich an

den Sicherheitsanforderungen aus Sicht Betreiber wesentlicher Dienste auszurichten. Der Beschluss des Schemas erfolgt durch das Cyber Risk Advisory Board.
Die operative Steuerung des Schemas erfolgt durch das Cyber Risk Management Board, welches sich aus drei Vertretern der beteiligten Partner zusammensetzt (KSV1870, KSÖ, Cyber Trust Services). Das Cyber Risk Management Board agiert als Eskalationsinstanz.

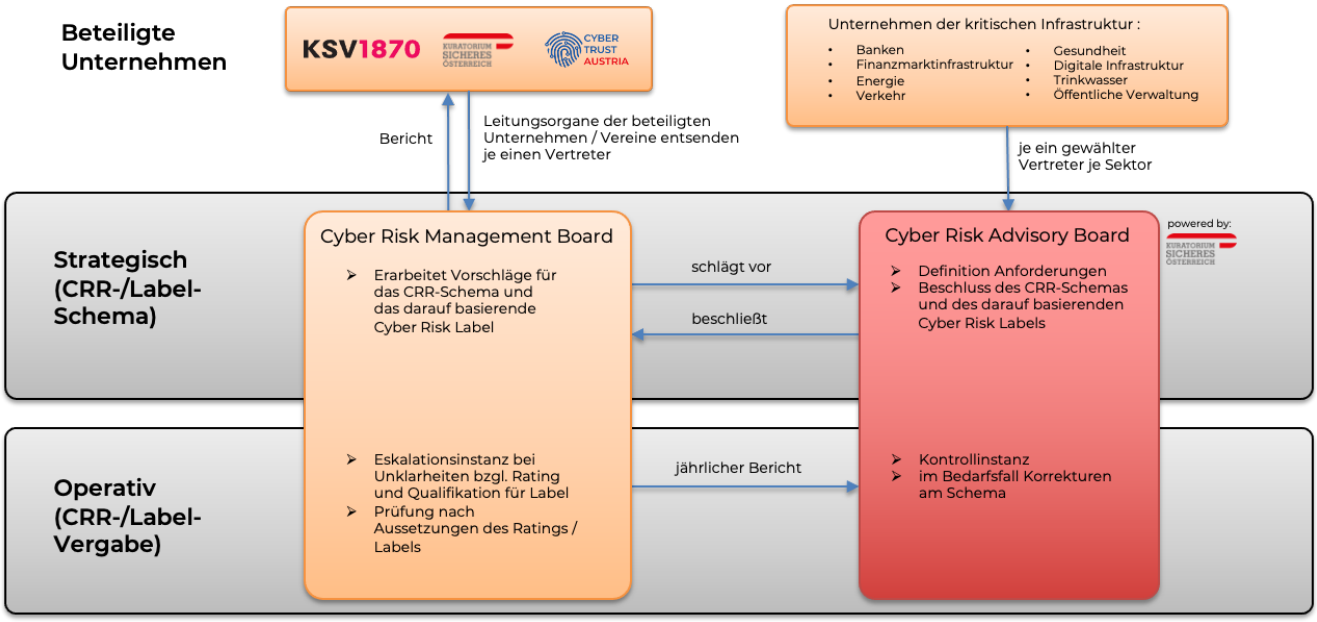

Abb. 1 Governance Modell des Cyber Risk Ratings

5 Voraussetzungen für das Cyber Risk Rating

Grundsätzlich kann jede Organisation einem Cyber Risk Rating unterzogen werden. Die Organisation kann dies selbst anfordern oder es kann von einer anderen Organisation angefordert werden (zum Beispiel im Rahmen einer Lieferantenüberprüfung). Die Teilnahme am Rating ist freiwillig. Wenn eine Organisation einwilligt, unterwirft sie sich der Rating-Vereinbarung mit dem KSV1870 entsprechend der vorliegenden Policy.

Folgende Informationen müssen von einer Organisation, die sich einem Rating unterzieht, verpflichtend angegeben werden:

- Eindeutige Identifikation der bewerteten Organisation (Name, Sitz der Organisation, Firmenbuchnummer bzw. Vereinsnummer o.ä.)
- Ansprechpartner in der Organisation (Name, Funktion, Telefon, E-Mail)
- Angabe aller bekannten, zugehörigen qualifizierten Internet-Domänen (für C-Score)

6 Sicherheit der verarbeiteten Daten

Sicherheits- und Risikobewertungen von Organisationen stellen sensible und schützenswerte Daten dar. Dementsprechend werden zum Schutz dieser Daten von allen beteiligten Partnern des Cyber Risk Ratings entsprechend hohe Sicherheitsmaßnahmen

eingehalten. Die detaillierten Bewertungsunterlagen inklusive der vom Kunden zur Verfügung gestellten Angaben werden für die Dauer der Bewertung verschlüsselt auf den Systemen des KSV1870 und der Cyber Trust Services GmbH gespeichert. Nach Vorliegen des finalen Ratings werden diese Daten der bewerteten Organisation verschlüsselt und signiert zugesandt; gemäß Rating-Vereinbarung ist die bewertete Organisation verpflichtet, diese Unterlagen (ebenso wie die dazugehörigen Evidenzen) zumindest ein Jahr über den Gültigkeitszeitraum des Ratings hinaus aufzubewahren und bei Bedarf vorzuweisen. Die detaillierten Bewertungsunterlagen werden danach beim KSV1870 und der Cyber Trust Services GmbH gelöscht. Gespeichert wird nur das finale Rating und das Datum der Ausgabe sowie gegebenenfalls der Label-Nutzungsvertrag. Das Rating (sowie die bei Antragstellung getätigten Bestätigungen des Kunden) wird in der Cyber Risk Rating Datenbank des KSV1870 gespeichert und die Berechtigung für das Label samt Nutzungsdauer in der Label-Datenbank. Der Label-Nutzungsvertrag samt dem zugrundeliegenden Rating zum Stichzeitpunkt (sowie die bei Antragstellung getätigten Bestätigungen des Kunden) werden bei der Cyber Trust Services GmbH gespeichert. Es werden somit auch keine personenbezogenen Daten im Zusammenhang mit dem Cyber Risk Rating oder dem Cyber Trust Label gespeichert. Auditoren werden mittels eines Code of Conduct dazu verpflichtet, ebenfalls alle erhaltenen Unterlagen vertraulich zu behandeln, ausschließlich im Rahmen des Audits zu verwenden und nach Abschluss der Bewertung auf all ihren Systemen zu löschen.

Die gesamte Kommunikation mit der bewerteten Organisation erfolgt verschlüsselt (sofern der Kunde dies unterstützt):

- über TLS verschlüsselte Webseiten bzw.
- über S/MIME verschlüsselte E-Mails.

7 Anhang A

7.1 Anforderungen für B Rating

Anforderung	Anforderungskriterien
Haben Sie eine aktuelle Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie), die für Ihr Unternehmen gültig ist?	Die Informationssicherheitsrichtlinie muss die wesentlichen Anforderungen an Informationssicherheit und Datenschutz abdecken (alle Kernthemen müssen - sofern sie anwendbar sind - in dieser Richtlinie beschrieben werden) und sollte auf ein bestehendes Regelwerk aufbauen (z.B. ISO 27002, NIST 800, IT Grundschutz, IT-Sicherheitshandbuch der WKO, u.ä.). Die Richtlinie muss von der Geschäftsführung freigegeben und für Mitarbeiter verfügbar sein.
Schulen Sie Ihre Mitarbeiter regelmäßig in IT-Sicherheit und Datenschutz?	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 (inkl. Datenschutz) -Passwörter richtig auswählen und verwalten -Sicher im Internet -E-Mails, Spam und Phishing -Gefährliche Schadprogramme -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.
Gibt es in Ihrem Unternehmen eine oder mehrere Personen, die für das Thema Informationssicherheit und Datenschutz zuständig sind?	Es muss zumindest eine namentlich benannte Person geben, die für das Thema Informationssicherheit & Datenschutz 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.
Pflegen Sie regelmäßig ein Verzeichnis all Ihrer Datenverarbeitungsprozesse, IT-Systeme und der damit verbundenen Verantwortlichkeiten?	Es muss ein Verzeichnis aller verwendeten Systeme und aller (nicht nur personenbezogener) datenverarbeitenden Prozesse geben. Dieses Verzeichnis muss zumindest Name und Version des Systems enthalten und den dafür Verantwortlichen.
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, damit nur die Personen zugreifen können, die aufgrund ihres Jobprofils einen Bedarf dafür haben.
Verlangen Sie von Ihren Mitarbeitern für alle Anwendungen Passwörter mit einer sicheren Mindeststärke zu verwenden?	Es muss klar beschriebene Mindestkriterien für Passwörter geben, die Empfehlungen aktueller Standards umsetzen (Passwortstärke, Zweifaktor-Authentifizierung wo notwendig und sinnvoll, Trennung Passworte etc.). Referenz: BSI, NIST 800 etc.
Verwenden Sie die vom Hersteller empfohlenen Sicherheitseinstellungen und achten Sie auf eine sichere Konfiguration all Ihrer IT-Systeme?	Es muss ein Dokument geben, das 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.

Überprüfen Sie - sofern vorhanden - individuell entwickelte, aus dem Internet zugängliche Anwendungen auf Sicherheitslücken vor Inbetriebnahme?	Individualsoftware, die aus dem Internet erreichbar ist, muss zumindest vor Inbetriebnahme durch einen Penetration Test auf Schwachstellen geprüft werden.
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.
Sichern Sie Ihr Netzwerk vor unberechtigtem Zugriff von außen ab?	Es ist eine Netzwerk-Segmentierungseinrichtung (z.B. Firewall, Router etc.) im Einsatz, welche auf Basis möglichst restriktiv gesetzter Regeln den Netzwerkverkehr mit dem Internet filtert.
Überwachen Sie Ihre IT-Systeme auf Malware und IT-Sicherheitsvorfälle?	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.
Verschlüsseln Sie sensible Daten bei der Übertragung im Internet?	- Es muss die Möglichkeit bestehen, Dateien verschlüsselt zu übertragen, entweder per E-Mail (z.B. S/MIME oder PDF verschlüsselt) oder per verschlüsseltem Upload. - Formulare auf der Webseite werden ausschließlich über https hochgeladen.
Protokollieren Sie die Nutzung Ihrer IT-Systeme, um Malware und IT-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.
Haben Sie einen Notfallplan, anhand dessen Sie auf einen IT-Sicherheitsvorfall reagieren?	Der Notfallplan inklusive Backupkonzept 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.

7.2 Anforderungen für A Rating (zusätzlich zu B)

Anforderung	Anforderungskriterien
Überprüfen Sie Ihre eingesetzte Software auf Sicherheitslücken?	Ein Tool zum Schwachstellenscannen muss im Einsatz sein und muss mindestens einmal pro Monat verwendet werden.
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.
Führen Sie in Ihrer Systemlandschaft Penetration Tests durch?	Zumindest alle zwei Jahre werden Penetration Tests durchgeführt, welche die Angreifbarkeit des Unternehmens prüfen.

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.
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
Verwalten Sie Identitäten und Berechtigungen aller Benutzer in nachvollziehbarer Weise?	- Ein 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.
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 korrelierte und auf Unregelmäßigkeiten analysiert werden.
Haben 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.
Können Sie auf qualifizierte Ressourcen zurückgreifen, wenn Sie einen schwerwiegenden Sicherheitsvorfall haben?	Es müssen Mitarbeiter mit nachgewiesenen Qualifikationen im Bereich 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.
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. Cryptolocker) 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 werden.
Haben Sie einen Prozess zum Management ihrer Lieferantenrisiken?	Es muss einen Prozess oder Checklisten geben, um Lieferanten auf Ihre Risiken bezüglich Cybersicherheit, Datenschutz und Business Continuity Management zu überprüfen.

7.3 Prüfkriterien für C-Score

- Indikatoren für IT-Sicherheitsvorfälle
  - Malwareverteilung
  - Defacements
- Indikatoren für Qualität der Verschlüsselung

    - SSL-Ciphersuite
    - SSL-Gültigkeit
    - SSL-Hostname
    - SSL-Trustlevel
- Prüfung auf effektive NutzungIndikatoren für Mitigation von IT-Sicherheitsvorfällen
    - Security-Header Implementierung
- Indikatoren für IT-Reputation
    - Blacklisting von eigenen Domains
    - Blacklisting von fremden Domains, auf die eigene Domains verlinken

8 Anhang B

8.1 Mindestanforderung an Auditoren

Auditoren müssen benannte Mitarbeiter von Unternehmen sein, die gemäß Kriterien für qualifizierte Stellen nach dem Netz- und Informationssystemsicherheitsgesetz (Verordnung über qualifizierte Stellen – QuaSteV) vom Bundesministerium für Inneres akkreditiert sind.

8.2 Mindestanforderung an Validierer

Die Validierung der Selbstdeklarationen erfolgt durch die Cyber Trust Services GmbH. Mit der Validierung befasste Personen müssen mindestens eine gängige Personenzertifizierung im Bereich Cybersicherheit besitzen und über mindestens 2 Jahre Berufserfahrung in diesem Bereich verfügen.

9 Begriffsbestimmungen

Konformitätsbewertungsprogramm (Conformity assessment scheme)
Regeln und Verfahren, die den Gegenstand der Konformitätsbewertung beschreiben, die festgelegten Anforderungen identifizieren und die Vorgehensweise zur Durchführung der Konformitätsbewertung beschreibt. Die vorliegende Schema-Policy beschreibt das Konformitätsbewertungsprogramm (Schema) für das Cyber Risk Rating (CRR) und das Cyber Trust Label.

Eigentümer (Scheme-Owner)
Organisation, die für die Entwicklung und Instandhaltung des Programmes (Schemas) verantwortlich ist. Schema Owner des Cyber Risk Ratings und des darauf basierenden Cyber Trust Labels ist das Kuratorium Sicheres Österreich (KSÖ).

Anforderung (Specified requirement)
Erfordernis oder Erwartung, das oder die niedergelegt ist. Im Rahmen des Cyber Risk Rating sind die Anforderungen in den Fragekatalogen für das A- bzw. B-Rating spezifiziert.

Konformitätsbewertung (Conformity assessment)
Darlegung, dass festgelegte Anforderungen erfüllt sind. Konformitätsbewertung beruht auf überprüfenden Tätigkeiten, wie unter anderem Inspektion und Validierung.

Bewertung (Review)
Erwägung, ob die Auswahl- und Ermittlungstätigkeiten und deren Ergebnisse hinsichtlich der Erfüllung der festgelegten Anforderungen durch den Gegenstand der Konformitätsbewertung

geeignet, angemessen und wirksam sind. Beim Cyber Risk Rating erfolgt die Bewertung im Rahmen der Validierung der Selbstdeklaration bzw. des Audits der bewerteten Organisation.

Konformitätsbewertungsstelle (Conformity assessment body)
Stelle, die Konformitätsbewertungstätigkeiten durchführt. Im Rahmen des CRR-Schemas werden die Validierungstätigkeiten auf Basis der Selbstdeklarationen von der CTS Cyber Trust Services GmbH durchgeführt. Die dem A-Rating zugrundeliegenden Audits werden durch qualifizierte Audit Partner durchgeführt, welche gemäß NIS-Verordnung als qualifizierte Stellen akkreditiert sind.

Gegenstand der Konformitätsbewertung (Object of conformity assessment)
Einheit, auf die sich die definierten Anforderungen beziehen. Dies können unter anderem Produkte, Prozesse oder Organisationen sein. Im Rahmen des CRR-Schemas ist der Gegenstand der Konformitätsbewertung immer eine Organisation (ein Unternehmen), definiert durch ihre Firmenbuchnummer.

Konformitätsbewertungstätigkeit durch eine erste Seite (First-party conformity assessment activity)
Tätigkeit, durchgeführt von der Organisation, die Gegenstand der Konformitätsbewertung ist. Im Rahmen des Cyber Risk B-Ratings ist dies die Selbstdeklaration durch die bewertete Organisation (das Unternehmen) selbst.

Konformitätsbewertungstätigkeit durch eine dritte Seite (Third-party conformity assessment activity)
Tätigkeit, durchgeführt von einer Person oder einer Organisation, die nicht Gegenstand der Konformitätsbewertung ist und von dieser unabhängig ist und somit kein Interesse als Kunde oder Lieferant an dieser Organisation hat. Im Rahmen des Cyber Risk A-Ratings ist dies ein Audit durch einen unabhängigen qualifizierten Audit-Partner.

Inspektion (Inspection)
Untersuchung eines Gegenstands der Konformitätsbewertung und Ermittlung seiner Konformität mit detaillierten Anforderungen, auf der Grundlage einer sachverständigen Beurteilung.

Audit (Audit)
Prozess zum Erlangen relevanter Informationen über einen Gegenstand der Konformitätsbewertung und zu dessen objektiver Auswertung, um zu ermitteln, inwieweit die festgelegten Anforderungen erfüllt sind. Ein Audit erfolgt im Rahmen einer Inspektion.

Validierung (Validation)
Bestätigung der Plausibilität eines bestimmten Anwendungszwecks durch Bereitstellung eines objektiven Nachweises, dass die festgelegten Anforderungen erfüllt sind. Im Rahmen des Cyber Risk B-Ratings bezieht sich die Validierung auf die Selbstdeklaration der bewerteten Organisation. Im Rahmen des Cyber Risk A-Ratings bezieht sich die Validierung auf den durch den Audit-Partner erstellten Bericht zur Konformität der bewerteten Organisation.

Überwachung (Surveillance)
Systematisch sich wiederholende Konformitätsbewertungstätigkeiten als Grundlage zur Aufrechterhaltung der Gültigkeit einer Konformitätsaussage. Im Rahmen des CRR-Schemas sind die Konformitätsbewertungen einmal jährlich zu erneuern.

Aussetzung (Suspension)
Vorübergehende Beschränkung der Konformitätsaussage durch die Stelle, die die Konformitätsaussage erstellt hat. Zu einer Aussetzung kommt es bei begründetem Zweifel an der Stichhaltigkeit der Bewertung.

Zurückziehung (Withdrawal)
Widerruf der Konformitätsaussage durch die Stelle, die die Konformitätsaussage erstellt hat. Zu einer Zurückziehung kommt es, wenn begründete Zweifel an der Stichhaltigkeit der Bewertung nicht ausgeräumt werden können.

Ablauf (Expiry)
Ende der Validität der Konformitätsaussage nach einem festgelegten Zeitraum. Das reguläre Ablaufdatum beträgt ein Jahr nach Ausstellung der Bewertung.

Wiederherstellung (Restoration)
Wiedereinsetzung der vollständigen oder teilweisen Konformitätsaussage nach Aussetzung.

Einspruch (Appeal)
Verlangen des Gegenstandes der Konformitätsbewertung (bewerteter Organisation) gegenüber einer Konformitätsbewertungsstelle, ihre Entscheidung bezüglich dieses Gegenstandes zu überprüfen

Cyber Risk Rating
Kennzahl, die sich aus der Auswertung der Konformitätsbewertung ergibt und eine Aussage über den Cyber Risiko Status des bewerteten Unternehmens gibt. Der Eigentümer der Cyber Risk Ratings ist der KSV1870.

Cyber Trust Austria Label
Gütesiegel, das auf Basis des Cyber Risk Ratings erstellt und vergeben wird, sofern die erforderlichen Anforderungen erfüllt sind. Der Eigentümer und Issuer des Cyber Trust Austria Labels ist die CTS Cyber Trust Services GmbH.

Rating-Vereinbarung
Rechtlich verbindliche Vereinbarung zwischen dem Eigentümer des Cyber Risk Ratings und dem bewerteten Unternehmen, welche die Rechte und Pflichten des bewerteten Unternehmens hinsichtlich der Konformitätsbewertung im Rahmen der Cyber Risk Rating Erstellung und der Überwachung festhalten.

Label-Nutzungsvertrag
Vertragliche Vereinbarung zwischen dem Eigentümer des Cyber Trust Austria Labels und dem bewerteten Unternehmen, welche die Bedingungen zur Nutzung des Labels rechtsverbindlich festlegen.