Pflichtenheft über die Anforderungen

V2.0 – 25. November 2019

Inhaltsverzeichnis

1 Einleitung

1.1 Ziele des Dokuments

Dieses Dokument beschreibt die Voraussetzungen für den Erhalt des «cyber-safe»-Labels. Ausserdem beschreibt es die Berechnungsmethoden, die während des gesamten Labelling-Prozesses angewendet werden.

1.2 Grundsätze des «cyber-safe»-Labels

Während Computersystemangriffe und andere Cyber-Vorfälle alle Unternehmen gleichermassen betreffen, und zwar unabhängig von ihrer Branche oder Grösse, ist die Kritikalität solcher Ereignisse für jedes Unternehmen einzigartig. So erleidet beispielsweise eine Schreinerei, deren Produktion vollständig computergestützt ist, im Falle eines Cyber-Vorfalls grössere Verluste als eine Schreinerei, die Computersysteme nur für administrative Zwecke (z. B. ein ERP-Buchhaltungssystem) einsetzt. Aus diesem Grund werden mit dem «cyber-safe»-Label spezifische Anforderungen festgelegt, die je nach Bedeutung der IT-Systeme in Ihrem Unternehmen variieren.

Um die Kritikalität der IT-Systeme eines Unternehmens zu ermitteln, verwendet das «cyber-safe»-Label einen pragmatischen Ansatz, mit dem der Wert der digitalen Assets und Daten, die geschützt werden müssen, sowie die erforderliche Cybersicherheit evaluiert werden. Daher besteht der erste Schritt bei jedem Labelling-Prozess darin, die Art von Daten zu identifizieren, über welche die antragstellende Organisation verfügt. In einem zweiten Schritt wird eine Aufschlüsselung der Auswirkungen im Falle eines Cyber-Vorfalls auf drei Achsen vorgenommen, für die jeweils die Höhe des wirtschaftlichen Schadens abgeschätzt werden muss:

1. **Vertraulichkeit (V)**: Welchen wirtschaftlichen Schaden kann die antragstellende Organisation erleiden, wenn ihre Daten weitergegeben werden?
2. **Integrität (I)**: Wie hoch ist der Schaden für die antragstellende Organisation, wenn ihre Daten geändert oder modifiziert werden (z. B. in Bezug auf Inhalt, Format, Genauigkeit usw.)?
3. **Temporäre Nichtverfügbarkeit (TNV)** und **permanente Nichtverfügbarkeit (PNV)**: Welche Kosten entstehen, wenn meine Daten einen Tag lang nicht zugänglich sind bzw. dauerhaft verloren gehen?

Die Antwort auf diese Fragen hängt nicht nur von der Art der Tätigkeit der antragstellenden Organisation ab, die sich auf die Art der ihr vorliegenden Daten auswirkt (z. B. in Bezug auf die Vertraulichkeit wird die Offenlegung medizinischer Daten grössere wirtschaftliche Auswirkungen haben als die Offenlegung von Arbeitszeitnachweisen), sondern auch von der Anzahl Mitarbeitender, deren Tätigkeit von IT-Systemen abhängt (z. B. bei vorübergehender Nichtverfügbarkeit von Daten variieren die Kosten je nach Anzahl der Mitarbeitenden, deren Tätigkeit wegen fehlender IT-Daten nicht mehr möglich ist).

Schliesslich definiert das «cyber-safe»-Label eine Reihe von grundlegenden Anforderungen, die Teil der Good Practices im Bereich Cybersicherheit sind und somit für alle Unternehmen gelten (z. B. Nutzung und Aktualisierung eines Antivirusprogramms, vorhandene Datensicherung usw.). Diese allgemeinen Anforderungen werden entsprechend dem Wert der Daten und der Anzahl der Mitarbeitenden, welche die IT-Systeme nutzen, verfeinert.

1.3 Terminologie

CVSS: Common Vulnerability Scoring System, allgemeines Verwundbarkeitsbewertungssystem. (siehe https://de.wikipedia.org/wiki/CVSS).

Netzwerkausstattung: Alle Elemente für die Verbindung eines Computernetzwerks, einschliesslich WiFi-Zugangspunkte, Router, Switches, Gateways usw.

Geschäftssoftware: Software zur Verwaltung von Unternehmensprozessen, insbesondere Enterprise-Resource-Planning-Systeme (ERP), Customer-Relationship-Management-Systeme (CRM) und Material-Requirement-Planning-Systeme (MRP).

Peripheriegeräte: Alle mit dem Netzwerk verbundenen Geräte, die über eine Benutzeroberfläche verfügen (Computer, Smartphone, Tablet usw.).

Geschäftliches Netz: Computernetzwerk (physisch oder VLAN), in dem die Mitarbeitenden arbeiten.

Datenträger: Der Datenträger ist ein physisches Element, das Informationen dauerhaft empfangen, speichern und wiedergeben kann.

Wert der Auswirkungen eines Vertraulichkeitsproblems: Geschätzter Wert der Kosten in Schweizer Franken, die durch die Offenlegung der Daten, die von der antragstellenden Organisation verwaltet werden entstehen.

Wert der Auswirkungen eines Integritätsproblems: Geschätzter Wert der Kosten in Schweizer Franken, die durch die Änderung von sämtlichen oder Teilen der Daten, die von der antragstellenden Organisation verwaltet werden, durch einen unbefugten Dritten entstehen.

Wert der Auswirkungen einer temporären Nichtverfügbarkeit: Geschätzter Wert der Kosten in Schweizer Franken, die durch die temporäre Nichtverfügbarkeit der Daten über einen bestimmten Zeitraum entstehen.

Wert der Auswirkungen einer permanenten Nichtverfügbarkeit: Geschätzter Wert der Kosten in Schweizer Franken für die Wiederherstellung der Daten, die für den reibungslosen Betrieb des Unternehmens erforderlich sind.

Wert der Daten: stellt den kumulierten Wert der Auswirkungen von Vertraulichkeits-, Integritätsproblemen, temporärer Nichtverfügbarkeit für einen Zeitraum von 10 Tagen und dauerhafter Nichtverfügbarkeit dar.

2 Bedingungen für den Erhalt des Labels

2.1 Allgemeines

Die Anforderungen gelten für Unternehmen mit maximal 250 Mitarbeitenden, die auf drei verschiedene geografische Standorte verteilt sind. Unternehmen, die diese Kriterien nicht erfüllen, haben dennoch die Möglichkeit, das Label zu erhalten. Die Anforderungen, die sie erfüllen müssen, werden dann von der Labelling-Kommission des Verbandes individuell und unter Beachtung der Grundsätze des Labels definiert.

2.2 Wert der Daten

Der Wert der Daten wird auf Einzelfallbasis mit der antragstellenden Organisation und unter Berücksichtigung jeder V-/I-/TNV-/PNV-Achse berechnet.
Der Gesamtwert der Daten GWD wird durch Summierung der Werte auf den verschiedenen Achsen berechnet.

2.3 Expositionskategorien

Die antragstellende Organisation wird in eine Kategorie eingestuft, die auf dem relativen Wert der Daten *RWD* basiert. Dieser wird definiert durch den Gesamtwert der Daten *GWD* dividiert durch die Anzahl Mitarbeitender *AM* (ausgedrückt in Vollzeitäquivalenten).

$$RWD = GWD / AM$$

***RWD*<=10k**	**10k<*RWD*<=20k**	**20k<*RWD*<=50k**	**50k<*RWD*<=100k**	**100k<*RWD***
nicht kritisch	wenig kritisch	leicht kritisch	kritisch	sehr kritisch
Kat. 1	Kat. 2	Kat. 3	Kat. 4	Kat. 5

3 Voraussetzungen für den Erhalt des Labels

Damit die antragstellende Organisation für die Vergabe des Labels in Frage kommt, muss sie alle Anforderungen erfüllen für:

- ihre Kategorie gemäss Punkt 2.3

  ODER

- die Anzahl der von der antragstellenden Organisation verwendeten Geräte, mit Ausnahme von Netzwerkgeräten.

Es muss nur eine der beiden Bedingungen erfüllt sein, damit die Voraussetzung für die antragstellende Organisation gültig ist.

Der Sachverständige kann ausnahmsweise und auf Basis einer schriftlichen Begründung die Vergabe des Labels empfehlen, wenn höchstens zwei Kriterien nicht erfüllt sind.

3.1 Kompetenzen und Verantwortlichkeiten

3.1.1 Human Resources

Voraussetzung	Kat.	Anz. Geräte
a) Die antragstellende Organisation muss eine interne Ansprechperson für IT-Fragen ernannt haben.	2	20
b) Die antragstellende Organisation muss über eine im IT-Bereich geschulte Ansprechperson (*mindestens EFZ*) verfügen, die mindestens eine Schulung zur Sensibilisierung für Cybersicherheit absolviert hat.	3	50
c) In der Geschäftsleitung der antragstellenden Organisation muss eine Person für die Cybersicherheit verantwortlich sein.	4	150

3.1.2 Phishing-Test

Für die Leistungsbewertung werden E-Mails mit unterschiedlichem Inhalt an jede angegebene E-Mail-Adresse gemäss den folgenden Regeln gesendet:

- Jede gesendete E-Mail enthält mindestens ein Element, an dem der Mitarbeitende erkennen kann, dass es sich um eine betrügerische E-Mail handelt.
- Die gesendeten E-Mails sind generisch und leicht als betrügerisch erkennbar.
- An jede Adresse werden mindestens fünf E-Mails gesendet.
- Der Testzeitraum beträgt je nach Anzahl der Adressen zwischen zwei und sechs Wochen.
- Jede E-Mail enthält ein Bild, das nach dem Anzeigen in der Phishing-Statistik aufgeführt wird.
- Jede E-Mail enthält einen Link, der nach dem Anklicken in der Phishing-Statistik aufgeführt wird.

Voraussetzung	Kat.	Anz. Geräte
a) Die durchschnittliche Klickrate für alle gesendeten E-Mails muss weniger als 25 % betragen.		
b) Die durchschnittliche Klickrate für alle gesendeten E-Mails muss weniger als 20 % betragen.	2	
c) Die durchschnittliche Klickrate für alle gesendeten E-Mails muss weniger als 17 % betragen.	3	
d) Die durchschnittliche Klickrate für alle gesendeten E-Mails muss weniger als 15 % betragen.	4	
e) Die durchschnittliche Klickrate für alle gesendeten E-Mails muss weniger als 12 % betragen.	5	

3.2 IT-Infrastruktur

3.2.1 Bestand

Voraussetzung	Kat.	Anz. Geräte
a) Das antragstellende Unternehmen muss ein umfassendes Bestandsverzeichnis der ICT-Infrastruktur und aller mit dem/den geschäftlichen Netz(en) verbundenen Elemente (Computer, Smartphone, Tablet, Internetobjekt usw.) führen.	3	20
b) Das antragstellende Unternehmen muss ein umfassendes Bestandsverzeichnis der Cloud-Dienste mit Daten führen.	2	

3.2.2 Verschlüsselung

Voraussetzung	Kat.	Anz. Geräte
a) Externe Kommunikationskanäle (inkl. VPN) werden verschlüsselt.	3	
b) Es ist zu ermitteln, welche Daten verschlüsselt werden müssen (während der Übertragung und/oder Speicherung), und sicherzustellen, dass diese auch tatsächlich verschlüsselt werden.	4	
c) Daten auf mobilen Geräten (Computer, Smartphone, Tablet, Internetobjekt usw.) werden systematisch verschlüsselt.	3	

3.2.3 WiFi

Voraussetzung	Kat.	Anz. Geräte
a) WiFi-Netzwerke müssen verschlüsselt (mindestens WPA2) und durch ein Passwort geschützt sein, bei dem es sich nicht um das Standardpasswort handeln darf (mindestens 16 Zeichen).		
b) Das WiFi-Netz für Gäste muss vom geschäftlichen Netz getrennt sein.	2	
c) Das interne WiFi-Netzwerk muss vom geschäftlichen Netz getrennt sein, wenn Mitarbeiter sich mit nicht im Bestandsverzeichnis aufgeführten Geräten verbinden können (z. B. Smartphones, private Geräte usw.), die das geschäftliche Netz unter keinen Umständen nutzen dürfen.	3	
d) Es muss ein logisches Netzwerk (VLAN) für IP-Telefone (IP-Phones) eingerichtet sein, das vom geschäftlichen Netz getrennt ist.	4	

3.2.4 Physischer Zugang

Voraussetzung	Kat.	Anz. Geräte
a) Sämtliche Anlagen, in denen Daten untergebracht sind, müssen gegen physischen Zugriff durch Unbefugte geschützt sein.		
b) Der Zugriff auf das Rechenzentrum durch externe Personen wird kontrolliert (z. B. Liste mit Angaben zu den Personen, die das Rechenzentrum betreten, Uhrzeit, von welchem Lieferanten usw.).	3	
c) Nicht mehr benutzte Datenträger werden so entsorgt, dass die darauf enthaltenen Daten dauerhaft vernichtet werden.		

3.2.5 Interne Scans

Voraussetzung	Kat.	Anz. Geräte
a) Schwachstellen mit einem CVSS-Wert von 9,0 oder höher dürfen nicht durch Scannen aus dem Innern der geschäftlichen Netze* heraus gemeldet werden.	2	

*Ein Host mit einer Schwachstelle mit einem CVSS-Wert von 9,0 oder höher kann nur in einem separaten logischen Netzwerk ohne Internetzugang toleriert werden.

3.2.6 Externe Scans

Voraussetzung	Kat.	Anz. Geräte
a) Schwachstellen mit einem CVSS-Wert von 7,0 oder höher dürfen nicht durch Scannen der öffentlichen IP-Adressen der Infrastruktur ab externem Standort gemeldet werden.		
b) Ein öffentlich zugänglicher Host, der eine Schwachstelle mit einem CVSS-Score von 7,0 oder höher, aber weniger als 9,0 aufweist, kann nur toleriert werden, wenn eine Firewall-Regel den Zugriff von ausserhalb der für die ordnungsgemässe Geschäftstätigkeit erforderlichen geografischen Gebiete einschränkt.		

3.3 Organisation

3.3.1 Datenschutz

Voraussetzung	Kat.	Anz. Geräte
a) Die antragstellende Organisation erklärt, dass sie die Datenschutzbestimmungen einhält (siehe Anhang 1).		

Die Datenschutzgrundsätze gemäss DSG (für alle Unternehmen in der Schweiz verbindlich) sowie gegebenenfalls gemäss DSGVO.

3.3.2 Drittanbieter

Voraussetzung	Kat.	Anz. Geräte
a) Wenn die Erfüllung bestimmter Anforderungen von einem oder mehreren Zulieferern abhängt, verlangt die antragstellende Organisation eine Verpflichtung zur Umsetzung von Sicherheitsmassnahmen, die mindestens denjenigen des «cyber-safe»-Labels entsprechen.	3	

Die Nutzung der «Cloud» gilt als Dienstleistung, die von einem Zulieferer erbracht wird.

3.3.3 Human Resources

Voraussetzung	Kat.	Anz. Geräte
a) Die antragstellende Organisation muss eine aktuelle Liste der Zugriffsberechtigungen für alle Datenkategorien und Arten von Mitarbeitenden führen (Berechtigungsplan).	3	30
b) Die antragstellende Organisation muss mindestens einmal jährlich überprüfen, ob die Liste der Zugangsberechtigungen den tatsächlich gewährten Rechten entspricht.		20
c) Kein Mitarbeitender darf an seinem lokalen Arbeitsplatz über Administratorenrechte verfügen, mit Ausnahme von IT-Mitarbeitern.	3	
d) Die antragstellende Organisation hat jeden Mitarbeitenden aufgefordert, ein Dokument zu unterzeichnen, in dem die Rechte und Pflichten in Bezug auf IT-Ressourcen festgelegt sind.		
e) Die antragstellende Organisation verfügt über eine Sicherheitsstrategie für Informationssysteme.		30

3.3.4 Verfahren, Routinen

Voraussetzung	Kat.	Anz. Geräte
a) Betriebssysteme von Geräten und Servern werden regelmässig aktualisiert.		
b) Softwareprogramme (ausser Geschäftssoftware) von Geräten und Servern werden regelmässig aktualisiert.		
c) Die Netzwerkausstattung wird regelmässig aktualisiert.	3	
d) Auf allen Geräten wird regelmässig überprüft, ob ein Antivirusprogramm vorhanden ist, das zudem regelmässig aktualisiert wird.		
e) Sicherheitswarnungen werden zentralisiert und regelmässig verarbeitet.	3	30
f) Zwischen dem geschäftlichen Netz und dem externen Netz besteht eine Firewall.	2	
g) Die Funktion, Konfiguration und Aktualisierung der Firewall wird regelmässig überprüft.	3	

3.3.5 Sicherung

Voraussetzung	Kat.	Anz. Geräte
a) Die antragstellende Organisation muss über ein Datensicherungssystem verfügen.		
b) Die Sicherung wird mindestens einmal pro Woche durchgeführt.		
c) Die Sicherung wird mindestens einmal pro Tag durchgeführt.	3	10
d) Die antragstellende Organisation muss in der Lage sein, den Status ihres Systems und ihrer Daten wieder auf den Status von vor einem Monat zurückzusetzen.		
e) Die antragstellende Organisation muss in der Lage sein, den Status ihres Systems und ihrer Daten wieder auf den Status von vor drei Monaten zurückzusetzen.	3	50
f) Die antragstellende Organisation muss in der Lage sein, den Status ihres Systems und ihrer Daten wieder auf den Status von vor sechs Monaten zurückzusetzen.	5	200
g) Die ordnungsgemässe Funktion der Sicherung wird mindestens einmal pro Woche überprüft.	2	
h) Eine Kopie der Daten befindet sich an einem zweiten Standort, der mindestens 10 km entfernt ist.	2	
i) Es ist nicht möglich, dass eine Person (einschliesslich des Administrators) alle Sicherungsdaten löschen kann.	4	100
j) Ein Test zur Wiederherstellung der neusten und ältesten Sicherungsdaten muss mindestens einmal pro Jahr durchgeführt werden.	3	50

3.3.6 Resilienz

Voraussetzung	Kat.	Anz. Geräte
a) Es gibt einen Plan bzw. Verfahren für die Wiederherstellung im Falle einer Unterbrechung der IT-Produktion.	4	150
b) Die Verfahren für die Wiederherstellung werden mindestens einmal pro Jahr getestet.	5	200

3.3.7 Passwörter

Passwortrichtlinien müssen so implementiert werden, dass jeder Mitarbeitender zu ihrer Einhaltung verpflichtet ist.

Voraussetzung	Kat.	Anz. Geräte
a) Passwörter müssen aus mindestens 10 Zeichen bestehen und Gross- und Kleinbuchstaben, Zahlen sowie Sonderzeichen enthalten.		

4 Anhang 1 – Datenschutzgrundsätze:

Die antragstellende Organisation verpflichtet sich zur Einhaltung der anerkannten Datenschutzgrundsätze:

- Zulässigkeit (oder Rechtmässigkeit): Die Verarbeitung personenbezogener Daten darf nicht gegen Gesetze verstossen (DSG und gegebenenfalls DSGVO). Sie muss auf einer Rechtsgrundlage, einer Einverständniserklärung oder einem übergeordneten öffentlichen oder privaten Interesse beruhen.
- Treu und Glauben: Grundsätzlich dürfen Daten nicht ohne Wissen der betroffenen Person oder gegen ihren Willen erhoben und verarbeitet werden. Sie dürfen auch nicht durch absichtliche Täuschung erhoben werden.
- Verhältnismässigkeit: Die Verarbeitung personenbezogener Daten muss notwendig, angemessen und so wenig aufdringlich wie möglich sein.
- Zweck: Personenbezogene Daten dürfen nur zu dem zum Zeitpunkt der Erhebung angegebenen Zweck verarbeitet werden, der gesetzlich vorgesehen ist (DSG und gegebenenfalls DSGVO oder gesetzliche Verpflichtung) oder der sich aus den Umständen ergibt.
- Genauigkeit: Die Person, die personenbezogene Daten verarbeitet, muss sicherstellen, dass sie korrekt sind, und gegebenenfalls alle geeigneten Massnahmen ergreifen, um sie zu aktualisieren, sodass unrichtige oder unvollständige Daten gelöscht oder korrigiert werden können.
- Sicherheit: Personenbezogene Daten müssen durch geeignete organisatorische und technische Massnahmen vor unbefugter Verarbeitung geschützt werden.
- Transparenz der Erfassung: Die Erfassung personenbezogener Daten und ihr Zweck müssen für die betroffene Person erkennbar sein.
- Alle anderen gesetzlichen Verpflichtungen, die für den Tätigkeitsbereich der antragstellenden Organisation gelten.