Präsentationsmappe

Schweizer Verband für das Cybersecurity-Gütesiegel :

Sichern Sie Ihre Aktivitäten und machen Sie es bekannt !

Association suisse pour le Label de Cybersécurité
Chemin des Piécettes 2
1052 Le Mont-sur-Lausanne
info@cyber-safe.ch

www.cyber-safe.ch

DER SCHWEIZER VERBAND FÜR DAS CYBERSECURITY-GÜTESIEGEL WURDE 2018 MIT DEM ZIEL GEGRÜNDET, EIN VERANTWORTUNGSBEWUSSTES CYBERSECURITY-MANAGEMENT IN KLEINEN UND MITTLEREN UNTERNEHMEN IN DER SCHWEIZ ZU FÖRDERN.

Zu diesem Zweck entwickelten sie ein Gütesiegel, das es diesen Unternehmen ermöglicht, ein von einer Reihe von öffentlichen und privaten Partnern als akzeptabel definiertes IT-Sicherheitsniveau zu erreichen. Basierend auf einer originellen Bewertungsmethode, die Online-Tools, Fragebögen, Phishing-Tests und menschliche Eingriffe kombiniert, wird das Gütesiegel ein Entscheidungsinstrument und ein detailliertes Wissen über Cyberrisiken in Bezug auf Infrastruktur, Organisation und menschliche Fähigkeiten liefern. So wird es den antragstellenden Organisationen ermöglicht, präventive Maßnahmen mit höherem Mehrwert zur Sicherung ihrer Aktivitäten durchzuführen - und dies bekannt zu machen!

Die zunehmende Verbreitung von Cyberangriffen und -vorfällen, ihre weltweite Mediatisierung und die Entwicklung der schweizerischen und europäischen Gesetzgebung haben in den letzten Jahren in den meisten Unternehmen zu einem neuen Bewusstsein für Cyberrisiken geführt. Während die größten von ihnen in der Regel über die notwendigen Ressourcen und Fähigkeiten verfügen, um mit Cyberrisiken vernünftig umzugehen, sind kleine und mittlere Unternehmen oft anfälliger für diese neuen Risiken. Diese Beobachtung führte zur Gründung des Schweizer Verbands für das Cybersecurity-Gütesiegel.

HABEN SIE GEWUSST?

- 1 von 3 KMU ist bereits Opfer von Cyberangeriffen[1] geworden.
- 15% der Unternehmen schulen ihre Mitarbeiter in guten Cybersicherheitspraktiken, während 100% der Unternehmen Phishing1 –Versuchen ausgesetzt sind.
- Für mehr als 1/4 der Opfer von Cyberangriffen waren die Reparaturkosten hoch; in einem Viertel der Fälle betrug die Rechnung mehr als 10 000 CHF[2].

[1] Mändli Lerch, K. (2017). Cyberrisiken in Schweizer KMUs. Zürich: gfs-zürich. https://gfs-zh.ch/wp-content/uploads/2017/12/Schlussbericht_CyberriskKMU_12122017.pdf

[2] Krähenbühl, J.-F. (2018). Les entreprises vaudoises face aux enjeux de la cybersécurité. Lausanne: Chambre vaudoise du commerce et de l'industrie. https://www.cvci.ch/fileadmin/documents/cvci.ch/pdf/Medias/publications/divers/12315_ENQUETE_CYBERSECURITE_PROD_PP.pdf

EIN GÜTESIEGEL, WARUM ?

Es gibt viele Hindernisse für den Eintritt von KMU und anderen kleinen Strukturen in die Welt der IT-Sicherheit. Das Cyber Safe-Gütesiegel zielt darauf ab, diese Barrieren abzubauen, indem es einen starken Anreiz und die notwendigen Instrumente für Unternehmen bietet, um die Cybersicherheit verantwortungsvoll zu verwalten. Und das alles zu einem erschwinglichen Preis !

Trotz zunehmender Mediatisierung über digitale Risiken (Datendiebstahl, Betriebsverlust usw.) und zunehmender Einsicht ist es für kleine und mittlere Unternehmen oft schwierig, Maßnahmen zu ergreifen. Neben den hohen Kosten für IT-Sicherheitsberatung und -auditierung stehen diese Unternehmen vor Fragen, die sie ohne die Hilfe von Spezialisten nur schwer beantworten können. Wie hoch ist das aktuelle Niveau der Cybersicherheit in meinem Unternehmen ? Ist es zufriedenstellend ? Welche Maßnahmen müssen ergriffen werden, um sie zu verbessern, zu welchen Kosten und mit welchen Auswirkungen? Ohne Fachkompetenz ist eine Bestandsaufnahme oder das Wissen, welche Maßnahmen umgesetzt werden sollen, schwierig oder gar unmöglich.

Obwohl es viele IT-Risikomanagementstandards (wie ISO) gibt, sind sie aufgrund ihrer Komplexität, des verwendeten Fachjargons und des von ihnen vorgeschlagenen sektoralen Ansatzes für Cyberrisiken oft nicht an die Bedürfnisse kleiner Organisationen angepasst (z.B. wird sich ein Rahmen ausschließlich auf die organisatorische Dimension, ein anderer auf die Soft- und/oder Hardware-Sicherheit und ein anderer auf die menschlichen Fähigkeiten konzentrieren). Die Einhaltung mehrerer (potenziell widersprüchlicher) Rahmen ist für Unternehmen jedoch nicht einfach, geschweige denn die damit verbundenen Kosten.

EIN GÜTESIEGEL MIT HOHER WERTSCHÖPFUNG

- Detaillierte Kenntnisse über das Cybersicherheits-Niveau.
- Barrierefreie und quantifizierte Entscheidungshilfe.
- Planen Sie, die Anfälligkeit für Cyberangriffe zu reduzieren.
- Optimierung der Cybersicherheitskosten.
- Senkung der Versicherungsprämien.
- Einhaltung guter Praktiken (Element der Haftungsbewertung).
- Mehr Vertrauen bei Partnern und Kunden, Reputationssteigerung.

CYBER SAFE REAGIERT AUF DIESE HERAUSFORDERUNGEN.

Das Cyber Safe-Gütesiegel bietet zunächst einmal ein wesentliches Entscheidungsinstrument, das es kleinen und mittleren Unternehmen ermöglicht, eine Bestandsaufnahme der Situation vorzunehmen, die wahrscheinlichen Kosten eines Cyberangriffs und damit den Mehrwert verschiedener möglicher Abhilfemaßnahmen zu kennen.

Es ermöglicht Unternehmen, ihre Anfälligkeit für zukünftige Cyberangriffe zu reduzieren. Es reagiert dann auf die Bedürfnisse dieser Unternehmen, indem es einen ganzheitlichen, nicht sektoralen Ansatz für Cyberrisiken verfolgt. Schließlich ermöglicht es zertifizierten Unternehmen, Vertrauen aufzubauen und den vollen Nutzen aus ihrem verantwortungsvollen Management der Cybersicherheit zu ziehen.

DER VERBAND : EINE PARTIZIPATIVE DEFINITION DES AKZEPTABLEN NIVEAUS DER CYBERSICHERHEIT

In der IT-Sicherheit gibt es kein Nullrisiko wie anderswo. Der Begriff des akzeptablen Risikos ist daher notwendig, um das Niveau der Anforderungen zu definieren, die ein Unternehmen erfüllen muss, um gekennzeichnet zu werden.

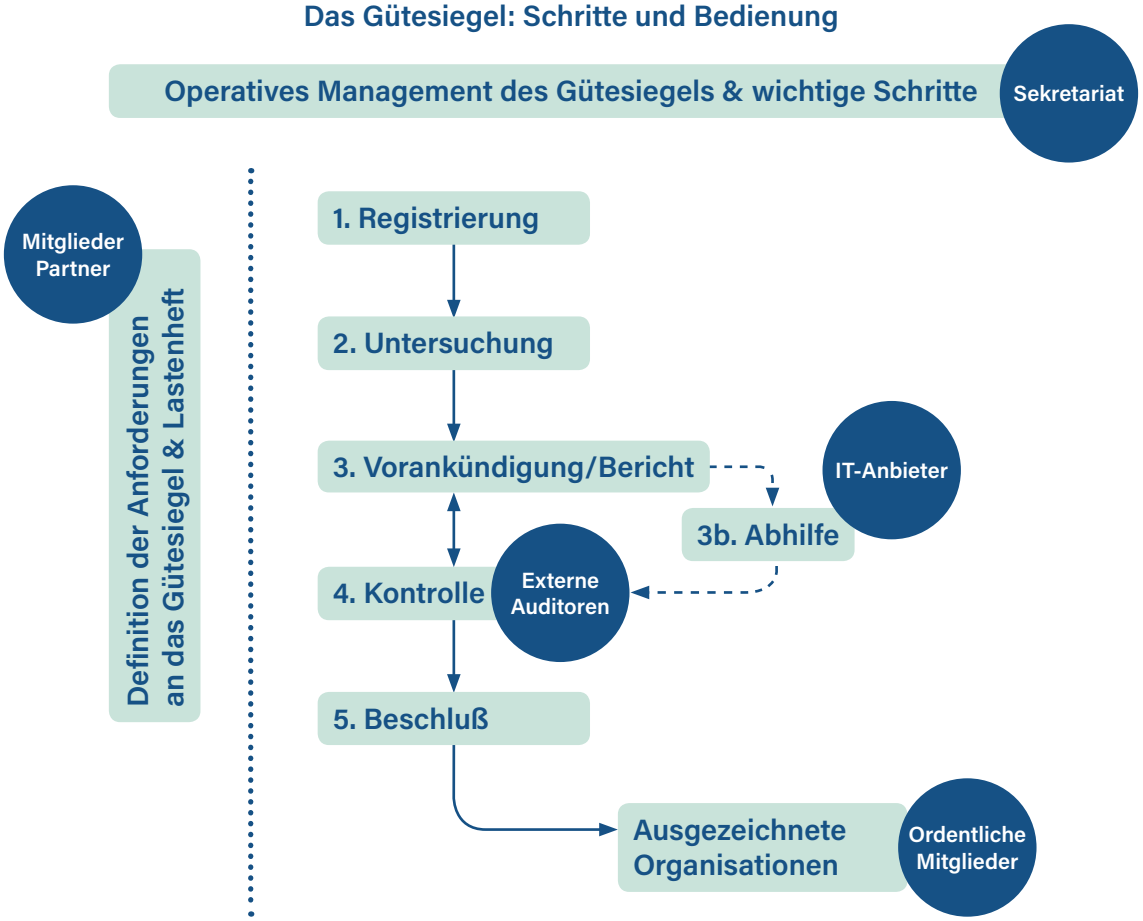
Um ein akzeptables Niveau der Cybersicherheit zu definieren, mobilisiert der Verband das Wissen und die Erfahrung aller relevanten Interessengruppen. Unter der Schirmherrschaft des Verbandes treffen sich IT-Sicherheitsspezialisten, Vertreter aus Wirtschaft und Politik sowie aus Wissenschaft und Gesellschaft. Sie definieren auf einer beschließenden und einvernehmlichen Grundlage das akzeptable Maß an Cybersicherheit, das für das Gütesiegel in Frage kommt. Diese so genannte «Normalisierung» findet jedoch innerhalb eines bestimmten Umfangs statt; die Untergrenze des Anforderungsniveaus wird durch die Konkursgrenze eines Unternehmens vorgegeben (z. B. Konkurs aufgrund der finanziellen und operativen Folgen von Data-Hacking). Die Obergrenze ist erreicht, wenn die Kosten der Investition höher sind als die Kosten für die Erstellung des Cyberrisikos.

DAS GÜTESIEGEL, EIN GLOBALER ANSATZ FÜR CYBERSICHERHEIT

Um das Niveau der Cybersicherheit eines Unternehmens zu bestimmen, basiert das Gütesiegel auf einer innovativen Technologie, die von einem Schweizer Unternehmen entwickelt wurde.

Diese Technologie ermöglicht es, Cyberrisiken global zu erfassen. Bewertet werden sowohl die IT-Infrastruktur, die Datensicherheit (einschließlich Backup- und Wiederherstellungsplan) und die Webseitensicherheit (bekannte Schwachstellen in den Content-Management-Systemen WordPress und Joomla) als auch menschliche und organisatorische Praktiken, die die Cybersicherheit betreffen (z.B. Phishing-Tests). Auf diese Weise können die technischen, menschlichen und organisatorischen Dimensionen bewertet werden, die für die Festlegung einer kohärenten und proaktiven Cyber-Risiko-Strategie erforderlich sind.

Das Gütesiegel: Schritte und Bedienung



1. Registrierung: Die Organisation stellt ihren Antrag an das Sekretariat, das sie nach formalen Kriterien (Anzahl der Mitarbeiter, Sitz in der Schweiz, Tätigkeiten außerhalb der FINMA) annehmen kann oder auch nicht. Die Registrierungsphase endet mit der Annahme des Antrags und der Zahlung der Registrierungsgebühr.

2. Untersuchung: Dann beginnt die Untersuchungsphase, in der eine erste Bewertung des Cybersicherheitsniveaus des antragstellenden Unternehmens mit spezialisierten Tools (externe und interne Scans der IT-Infrastruktur und der Website), Fragebögen (Datensicherungsrichtlinie und Wiederherstellungsplan, Zuweisung von Verantwortlichkeiten innerhalb des Unternehmens usw.) und Phishing-Versuchen (Bewertung der menschlichen Fähigkeiten) durchgeführt wird.

3. Vorankündigung/Bericht: Die antragstellende Organisation erhält dann einen detaillierten Bericht über ihr Cybersicherheitsniveau, ihre Schwachstellen und den möglichen Kosten; gleichzeitig wird ein Zertifizierungsbescheid versandt. Dieser Bericht, der sowohl im PDF-Format als auch in einem interaktiven Dashboard verfügbar ist, stellt auch mögliche Abhilfemaßnahmen und deren Auswirkungen auf das allgemeine Niveau der Cybersicherheit (Kosten-Nutzen-Verhältnis) dar. Das Dashboard ermöglicht es dem Unternehmen, die verschiedenen Maßnahmen und ihre Auswirkungen auf die verschiedenen Komponenten (Infrastruktur, Organisation, menschliche Fähigkeiten) zu simulieren, die bei der Beurteilung des Niveaus der Cybersicherheit berücksichtigt werden.

3b. Abhilfe: Abhängig vom Grad der Cybersicherheit der antragstellenden Organisation kann diese die notwendigen Abhilfemaßnahmen durchführen, um das für den Erhalt des Gütesiegels festgelegte Anforderungsniveau zu erreichen. Je nach Fall können die Abhilfemaßnahmen entweder direkt von dem Unternehmen oder von seinem IT-Dienstleister durchgeführt werden. Für jede der möglichen Maßnahmen werden potenzielle Anbieter an die antragstellende Organisation kommuniziert.

4. Kontrolle: Wenn die antragstellende Organisation der Ansicht ist, dass sie die Anforderungen des Gütesiegels erfüllt, informiert sie das Sekretariat des Verbands, das dann einen unabhängigen externen Auditor (d.h. nicht an Sanierungsmaßnahmen beteiligt) beauftragt, bei der antragstellenden Organisation die Richtigkeit der gesammelten Daten und gegebenenfalls deren Aktualisierung nach Durchführung der Sanierungsmaßnahmen zu überprüfen. Der externe Auditor erstellt dann einen Bewertungsbericht, den er an das Sekretariat des Verbandes sendet.

5. Beschluss: Auf der Grundlage des vom externen Auditor übermittelten Bewertungsberichts fasst das Sekretariat des Verbandes einen formellen Beschluss über die Vergabe oder Vertagung. Eine Entscheidung über die Verschiebung kann nur einmal getroffen werden, damit das Unternehmen, das die Anforderungen des Gütesiegels nicht erfüllt, die Schritte 2 bis 5 ohne zusätzliche Kosten wiederholen kann. Wenn das Unternehmen am Ende der Vertagung die Anforderungen immer noch nicht erfüllt, weigert sich der Verband, das Gütesiegel zu vergeben.

ASSOCIATION SUISSE POUR
LE LABEL DE CYBERSÉCURITÉ

Association suisse pour
le Label de Cybersécurité
Chemin des Piécettes 2
1052 Le Mont-sur-Lausanne
info@cyber-safe.ch

www.cyber-safe.ch