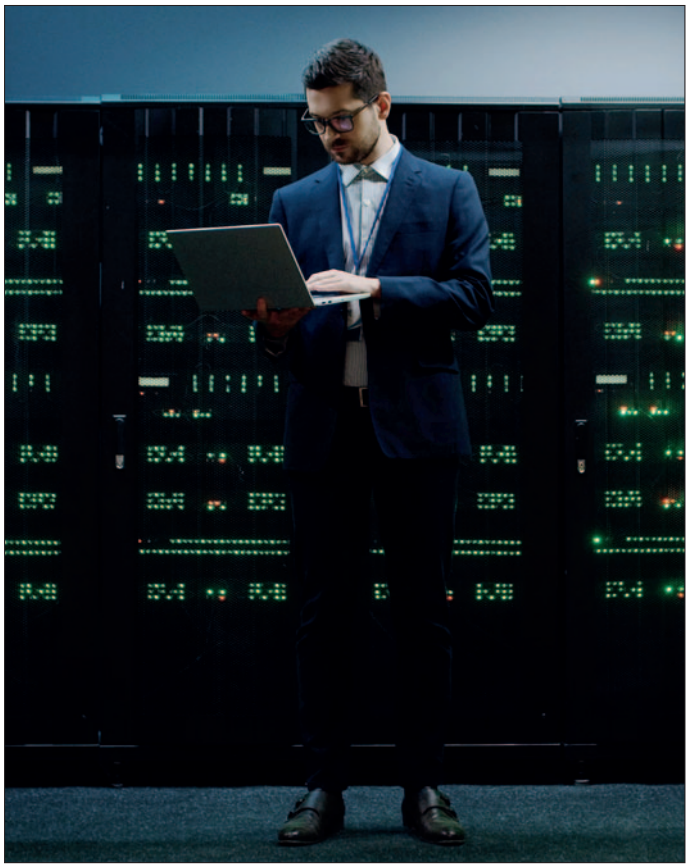
Labels für mehr Sicherheit

Das „Cyber Trust Austria Label“ bietet eine Auszeichnung für die unternehmensweite Cyber-Sicherheit. Es soll auch kleinen Unternehmen die Chance bieten im Wettbewerb zu bestehen.

Internetkriminalität ist die in Österreich am stärksten steigende Kriminalitätsform. Das österreichische Gütesiegel für Cyber-Sicherheit soll die Sicherheit in der Lieferkette erhöhen, mehr Transparenz in der österreichischen Cyber-Sicherheitslandschaft schaffen und somit die Wettbewerbsfähigkeit des österreichischen Wirtschaftsstandorts im Digitalisierungszeitalter stärken“, sagte Mag. Erwin Hameseder, Präsident des *Kuratoriums Sicheres Österreich (KSÖ),* bei der Präsentation des *Cyber Trust Labels Austria* am 27. Jänner 2021 im Raiffeisen-Haus in Wien.



Das Cyber Trust Austria Label soll den Nachweis der Cyber-Sicherheit von Unternehmen bescheinigen.

Hacker-Angriff auf die westliche Welt. „Wie allgegenwärtig und gefährlich Hacker-Angriffe sind, verdeutlicht der Angriff auf den amerikanischen IT-Dienstleister Solarwinds“, gab Dr. Thomas Stubbings, MBA, Geschäftsführer der *Cyber Trust Services GmbH* zu bedenken. Wie die *New York Times* berichtete, soll die Attacke auf *Solarwinds* Hackern im Handstreich einen Zugang in die Systeme von mehr als 250 amerikanischen Behörden, Ministerien und prominenten Unternehmen eröffnet haben – somit sei auch die kritische Infrastruktur unterwandert worden. Durch die automatisch heruntergeladenen Aktualisierungen sollen die Kriminellen Zugriff auf rund 18.000 Netzwerke von Unternehmen und Regierungsbehörden erlangt haben. *Microsoft* gab bekannt, dass die Hacker in das Netzwerk des Unternehmens eingedrungen seien und Zugriff auf den *Windows*-Quellcode gehabt hätten. Jedoch hätten sie diesen nicht verändern können, was ein sicherheitspolitisches Desaster gewesen wäre, da das Betriebssystem von Milliarden Systemen weltweit eingesetzt werde.

Zu den Opfern des Angriffs gehören bekannte Unternehmen wie *Intel, Fireeye, Cisco* oder *Nvidia*. Bundesbehörden in Deutschland und Unternehmen haben die kompromittierte Netzwerk-Plattform von *Solarwinds* ebenfalls genutzt.

Einzigartig innerhalb der EU. Das österreichische Gütesiegel für Cyber-Sicherheit ist die erste Auszeichnung ihrer Art innerhalb der Europäischen Union. Sie basiert auf dem frei verfügbaren „KSÖ Cyber Risk Schema“, das von einem Expertengremium bestehend aus CISOs großer Unternehmen unter Beteiligung des Bundesministeriums für Inneres entwickelt worden ist und somit auch auf die Anforderungen des NIS-Gesetzes abgestimmt ist. CISO steht für Chief Information Security Officer und bezeichnet eine Position in einer Organisation oder einem Unternehmen, die für die Sicherheit von Informationen und der Informationstechnologie verantwortlich ist.

Alternative zu aufwändigen Zertifizierungsverfahren. Das *Cyber Trust Austria Label* stellt nach Ansicht des *KSÖ* eine einfache und kostengünstige Möglichkeit dar, nach außen sichtbar zu machen, dass die Sicherheit im eigenen Unternehmen einen wichtigen Stellenwert hat und wesentliche Sicherheitsmaßnahmen umgesetzt wurden.

Cyber Risk Rating. Das *Cyber Trust Austria Label* basiert auf dem „Cyber Risk Rating Schema“, das vom *KSÖ* in Zusammenarbeit mit dem *Kreditschutzverband 1870* erarbeitet wurde. Das „Cyber Risk Rating“ und das darauf basierende *Cyber Trust Label* stellen ein Schema zur Bewertung des Cyber-Risikostatus von Unternehmen oder Vereinen dar. Das „Cyber Risk Rating“ unterscheidet drei Bewertungsschemata, die sich in Bezug auf ihren Anspruch (Security Claim) wie auch in Bezug auf die Rigorosität der Überprüfung (Assurance Level) unterscheiden: das „B-Rating“, das „A-Rating“ und das „A-Plus“-Rating. Aufbauend auf diesen Ratings wird das *Cyber Risk Label* angeboten. Es soll nach außen ein sichtbares Qualitätsmerkmal für ein angemessenes Cyber-Sicherheitsniveau signalisieren. Für jedes Unternehmen, das die Vertrauenswürdigkeit seiner Lieferanten in Bezug auf die Cyber-Sicherheit prüfen möchte, stellt das *Cyber Risk Rating* eine effiziente Methode dar, der Sorgfaltspflicht beim „Third Party Risk Management“ nachzukommen.

Zwei Qualitätsstufen, zwei Labels. Es gibt zwei Qualitätsstufen und dazu passende Labels. Das einfachere Basis-Label wendet sich vor allem an kleinere Unternehmen und Organisationen. Die Anforderungen sind Basissicher-

Foto: VAKSMANV/Stock.adobe.com

heitskriterien, die jedes Unternehmen erfüllen sollte. Der Aufwand dafür ist überschaubar. Die Bewertung erfolgt mit einer validierten Selbstdeklaration. Der Prozess ist einfach und rasch durchführbar. Bei der Selbstdeklaration bewerten sich die Unternehmen selbst – inwiefern sie die vom Schema vorgegebenen Anforderungen im Rahmen der definierten Kriterien erfüllen und dies anhand der definierten Nachweise (Evidenzen) im Bedarfsfall nachweisen können. Dabei sind Fragen wie – „Gibt es in Ihrem Unternehmen eine oder mehrere Personen, die für das Thema Informationssicherheit und Datenschutz zuständig sind" oder „Verlangen Sie von Ihren Mitarbeitern für alle Anwendungen Passwörter mit einer sicheren Mindeststärke zu verwenden" – zu beantworten.

Um eine Nachvollziehbarkeit und Plausibilisierung der Selbstbewertung gewährleisten zu können, 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. Das fortgeschrittene Label *(Cyber Trust Austria Label Gold)* wendet sich an Unternehmen und Organisationen, die ein höheres Sicherheitsniveau erfüllen müssen oder wollen. Es umfasst die 14 Basissicherheitskriterien sowie 11 zusätzliche Kriterien. Die Erfüllung der Anforderungen erfordert Vorbereitung und einen gewissen Aufwand. Die Bewertung erfolgt durch ein externes Audit. Dieser Prozess nimmt etwas mehr Zeit in Anspruch.

Zielgruppen. Das Basis-Label richtet sich an Klein- und Mittelbetriebe, die Cyber-Sicherheit ernst nehmen und das auch nach außen hin zeigen wollen, oder an Zulieferer von Betreibern wesentlicher Dienste (gemäß NIS-Gesetz) in weniger kritischen Bereichen. Das Gold-Label richtet sich an große Unternehmen und Zulieferer von Betreibern wesentlicher Dienste (gemäß NIS-Gesetz) in kritischeren Bereichen – wie etwa Verarbeiter von sensiblen Daten.

Unkompliziert und praktikabel. Das Gütesiegel bietet Unternehmen im Unterschied zu bereits bestehenden, teils aufwändigen Zertifizierungsschemata im Cyber-Sicherheitsbereich, einen praktikableren und kostengünstigeren Zugang zu diesem Thema. Dadurch

Thomas Stubbings, Cyber Trust Services GmbH, und KSÖ-Präsident Erwin Hameseder übergeben das Cyber Trust Austria Gold Label an Oliver Albl von Fabasoft.

wird es auch kleineren Unternehmen ermöglicht, mit überschaubarem Aufwand die Umsetzung von Basissicherheitsanforderungen nachzuweisen und sich somit am Markt zu differenzieren.

NIS-Gesetz und Lieferkette. Das NIS-Gesetz verlangt von Betreibern wesentlicher Dienste, dass sie eine adäquate Cyber-Sicherheit bei ihren Zulieferern sicherstellen. Das *Cyber Trust Austria Label* soll zukünftig genau dafür eine gute Grundlage bieten.

Der Generalsekretär der Industriellenvereinigung, Christoph Neumayer, erklärte dazu: „Die Industriellenvereinigung vertritt mit ihren mehr als 4.500 Mitgliedern viele Unternehmen der kritischen Infrastruktur und wesentliche Produzenten und Dienstleister für Österreichs Wirtschaft. Jedes dieser Unternehmen ist darauf angewiesen, sich auf die Cyber-Sicherheit ihrer Zulieferkette verlassen und dies auch nachvollziehen zu können. Das Cyber Trust Austria Label bietet dafür eine sehr gute Grundlage, weil es auch für kleinere Lieferanten geeignet und mit vertretbarem Aufwand umsetzbar ist."

Ausgezeichnete österreichische Unternehmen. Im Zuge der Veranstaltung im Raiffeisen-Haus wurden die ersten Gold-Labels an österreichische Unternehmen vergeben: an die *Fabasoft AG* mit Hauptsitz in Linz und an die in Tirol ansässige *MED-EL Elektromedizinische Geräte GmbH*. „Das Cyber Trust Austria Gold Label ergänzt unsere bestehenden Sicherheits- und Qualitätszertifikate perfekt. Als Softwarehersteller und Cloud-Anbieter haben für uns Datenschutz und Datensicherheit höchste Priorität", erklärte Oliver Albl von *Fabasoft*.

Kein Privileg der Großen. „Cyber-Sicherheit darf kein exklusives Merkmal großer Unternehmen sein. Jeder braucht Basissicherheit – das wird zukünftig ein Hygienefaktor sein, wie das Einhalten der Datenschutz- oder Compliance-Regeln. Mit dieser Initiative soll ein nachhaltiger Beitrag zur Stärkung der Cyber-Sicherheit in Österreich und ein wertvoller Beitrag zur Stärkung des Wirtschaftsstandorts in Zeiten der Digitalisierung geleistet werden", erklärte Stubbings. „Es handelt sich um eine österreichische Initiative von Unternehmen für Unternehmen. Dazu hat ganz wesentlich das „Cyber Risk Advisory Board" des „KSÖ Cyber Risk Schemas" beigetragen, das sich aus Unternehmen der kritischen Infrastruktur zusammensetzt (je eines pro NIS-Sektor) und das vom Innenministerium begleitet wurde, um die Konsistenz mit den NIS-Erfordernissen – darunter fallen die Anforderungen an Cybersicherheit bei Lieferanten, Dienstleistern und Dritten – sicherzustellen".

Das Cyber Risk Rating Schema ist abrufbar unter: *https://kuratorium-sicheres-oesterreich.at/cyber-trust-austria/* *Gernot Burkert*

FOTO: ALEXANDER FELTEN