KSV1870

Es braucht mehr Cyber-Security.

KSV1870 Services zur Minimierung der digitalen Gefahr.

„Mit dem CyberRisk Rating stellen wir ein Werkzeug zur Verfügung, das IT-Security nicht nur bewertet, sondern durch praxisorientierte Anforderungen auch bei der Reduktion von Sicherheitsdefiziten unterstützt.“

Ricardo-José Vybiral
CEO der KSV1870 Holding AG

„Die Gefahr aus dem Web nimmt laufend zu, trotzdem wird das Thema IT-Sicherheit häufig stiefmütterlich behandelt. Es ist definitiv so, dass sowohl KMU als auch die Big Player mehr in Risikominimierung und Prävention investieren sollten.“

Alexander Mitter
Geschäftsführer
KSV1870 Nimbusec GmbH

I. Status quo in Österreich

I.I. Cybergefahr nimmt laufend zu

Die Gefahr von Cyber-Attacken auf Unternehmen befindet sich seit Längerem auf hohem Niveau – und das Risiko ist nicht zuletzt aufgrund der Corona-Krise und dem Ukraine-Krieg nochmals angewachsen. Zahlen des Bundeskriminalamtes für das Jahr 2021 bestätigen die jüngsten Entwicklungen. Demnach gab es damals um knapp 29 Prozent mehr Anzeigen von Internetkriminalität (Gesamt: 46.200) als im Jahr 2020. Fast die Hälfte davon, rund 22.400 Fälle (+ 19,5 %), entfällt auf Betrugsdelikte. Gleichzeitig ist auch die Zahl an Cybercrime-Delikten stark gestiegen – und zwar von 13.000 auf 15.500 Anzeigen innerhalb eines Jahres.

Die Gefahr aus dem Web nimmt laufend zu, trotzdem wird das Thema IT-Sicherheit häufig stiefmütterlich behandelt. Es ist definitiv so, dass sowohl KMU als auch die Big Player mehr in Risikominimierung und Prävention investieren sollten. Auch wenn es heutzutage fast unmöglich ist, sich komplett gegen Hacker zu schützen, so muss das Risiko zumindest auf ein absolutes Minimum reduziert werden.

I.II. Content Management Systeme als „door opener“ für Hacker

Für den CyberRisk Report 2022 hat die KSV1870 Nimbusec GmbH in Österreich rund 45.000 Webseiten unter die Lupe genommen. Wie die aktuellen Ergebnisse zeigen, waren dabei knapp 100 Unternehmenswebseiten mit Schadsoftware infiziert: Das klingt im ersten Moment nicht viel. Wenn man aber bedenkt, dass viele dieser Webseiten täglich zigtausende Zugriffe haben und jedes Mal dabei Schadsoftware verteilen, dann steigt die Zahl an betroffenen IT-Systemen fast schon ins Unermessliche. Unzureichend gewartete Content Management Systeme sind dabei das „Einfallstor“ schlechthin für Cyber-Kriminelle. Bei nahezu allen Fällen bildeten CMS-Systeme die Basis der gehackten Webseiten – in 88 Prozent der Fälle handelte es sich dabei um Wordpress. Besonders erstaunlich: 28 Prozent der infizierten Domains waren zwei Monate nach erfolgter Überprüfung noch immer beschädigt. Und 17 Prozent der betroffenen Domains wurden nach erfolgter Bereinigung nur unzureichend abgesichert, sodass diese innerhalb eines Monats neuerlich Opfer von Hackern wurden.

I.III. Awareness für Cyber-Angriffe stärken

Aktuell gibt es viele Themen, mit denen sich Österreichs Unternehmen bereits jetzt oder in naher Zukunft aufgrund von neuen Richtlinien bzw. Verordnungen intensiv beschäftigen müssen. Neben den Themen ESG und Lieferkettengesetzt u.a. betrifft das auch die IT- und Cyber-Sicherheit. Vonseiten der Gesetzgebung gibt es dazu bereits Maßnahmen, die helfen sollen, das Risiko zu senken – mit der **EU-Richtlinie 2016/1148 („NIS“)** soll etwa das Sicherheitsniveau von Netz- und Informationssystemen gestärkt werden. Dabei bleibt es jedoch nicht: Diese EU-Richtlinie wird ersetzt durch die **NIS-2-Richtlinie**, unter anderem mit strengeren Überwachungsmaßnahmen und Meldepflichten sowie EU-weit harmonisierter Sanktionen. Der Gesetzesentwurf zum European Cyber Resilience Act (CRA) schreibt erstmalig EU-weit verpflichtende Maßnahmen für die Cybersicherheit internetfähiger Geräte und Produkte vor.

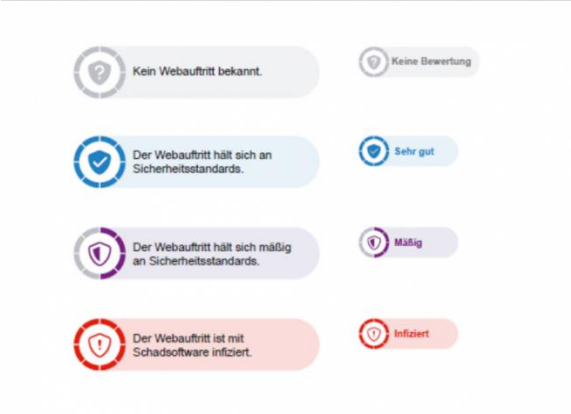
Big Change: Ab Herbst 2024 muss die kritische Infrastruktur selbst bzw. deren Geschäftspartner Maßnahmen zur Wahrung der IT-/Cyber-Sicherheit nachweisen. Ist das nicht der Fall, können Betriebe kein Geschäftspartner der kritischen Infrastruktur mehr sein. Das würde für viele Unternehmen einen massiven wirtschaftlichen Verlust bedeuten.

II. Bedeutung von Risikomanagement steigt

II.I. KSV1870 prüft Cyber-Risiko von Unternehmen

Die steigenden Zahlen in Sachen Cyber-Kriminalität sprechen eine deutliche Sprache. Umso verständlicher ist es demnach, dass Unternehmen heutzutage genau wissen wollen, wie es um die IT-Security eines potenziellen Geschäftspartners bestellt ist. Selbstverständlich noch bevor dieser an das eigene IT-System „andockt“ und digitale Daten fließen.

II.I.I. Soft Check mit vier Klassifizierungen



Seit März 2022 ist in allen UnternehmensProfilen des KSV1870 der WebRisk Indicator integriert. Dabei handelt es sich um eine Risikobewertung für den Webauftritt eines Unternehmens. Konkret wird das öffentlich sichtbare Cyberrisiko von Unternehmenswebseiten klassifiziert. Gemessen an den geltenden Sicherheitsstandards wird die Unternehmenswebsite als sehr gut, mäßig oder infiziert (mit Schadsoftware) eingeteilt. Ist kein Webauftritt bekannt, so gibt es auch keine Bewertung. Die Information ist ein Add-on für bestehende Kunden und hat keinen Einfluss auf das klassische KSV1870 Rating. Mit diesem neuen Service gehen wir darauf ein, dass Unternehmen neben der klassischen Bonitätsprüfung immer häufiger auch noch andere Needs haben. Und wir als Informationsdienstleister haben den Anspruch, Antworten auf diese aktuellen Fragestellungen von Unternehmen zu liefern.

II.I.II. Für Fortgeschrittene: das CyberRisk Rating

Doch viele Betriebe wollen mehr wissen, bevor sie ihre IT-Systeme für einen Geschäftspartner öffnen und Schnittstellen einrichten. In diesem Fall kann ein CyberRisk Rating über den potenziellen Partner beantragt werden, wobei dieser seine Systeme und digitalen Daten für die Prüfung beschreiben muss. Optimalerweise wird dies im Vorfeld besprochen, damit der Prozess effizient und schnell abgeschlossen werden kann. Ein weiterer Vorteil bei dieser Prüfung ist, dass sie der EU-Richtlinie 2016/1148 („NIS“) entspricht. Ziel der Richtlinie ist ein höheres Sicherheitsniveau von Netz- und Informationssystemen in der gesamten EU zu schaffen. Das CyberRisk Rating hat der KSV1870, ebenso wie den WebRisk Indicator gemeinsam mit einer seiner Beteiligungen, der KSV1870 Nimbusec GmbH, umgesetzt.

II.I.III. IT-Sicherheit als Eigenwerbung

Doch viele Unternehmen möchten sich schon im Vorfeld eines Geschäftsabschlusses als sicherer Partner deklarieren. Hier gibt es die Möglichkeit, dass Unternehmen die Sicherheit der eigenen IT-Landschaft proaktiv auszeichnen lassen. All jene, die öffentlich deklarieren möchten, dass sie essenzielle Mindestsicherheitsmaßnahmen für Cybersicherheit umgesetzt haben, können auf das Cyber Trust Austria Label zurückgreifen. Es basiert auf dem CyberRisk Rating Schema, das vom Kompetenzzentrum Sicheres Österreich (kurz KSÖ) in Zusammenarbeit mit dem KSV1870 erarbeitet wurde. Es gibt drei Qualitätsstufen und dazu passende Labels. Es ist also für jeden etwas dabei.

Mehr dazu:
Cyber-Risiko-Lösungen vom KSV1870 auf einen Blick.

KSV1870

www.ksv.at

Rückfragehinweis:
Markus Hinterberger
KSV1870 Unternehmenskommunikation
Telefon: 050 1870-8205
E-Mail: hinterberger.markus@ksv.at
www.ksv.at