KSV1870

CyberRisk Report

DER REPORT ZUM ÖSTERREICHISCHEN CYBERRISK RATING

AUSGABE 2024

FACHBEITRÄGE:

Caroline Schmidt (BMI) und Vinzenz Heußler über die neue Cybersicherheits-Richtlinie NIS2.

Interview
Mit Verena Becker (WKÖ), Cybersicherheitsexpertin für Information & Consulting.

IT-Security
Im Gespräch mit Generaldirektor Michael Höllerer (Raiffeisen NÖ-Wien).

IMPRESSUM: Medieninhaber: KSV1870 Nimbusec GmbH, 4020 Linz, Kaisergasse 16b; https://cyberrisk-rating.at/
Herausgeber: Alexander Mitter; Verlagsort: Linz; Chefredaktion: Elisabeth Hentscholek; Autoren dieser Ausgabe: Caroline Schmidt, Vinzenz Heußler, Alexander Mitter, Elisabeth Hentscholek, Gerald Hübsch, Alexander Janda, Verena Becker, Martin Klimbacher, Wolfgang Petschko, Georg Beham, Thomas Mann; Layout: Elisabeth Hentscholek; Coverfoto: Unsplash;

Hinweis: Aus Gründen der Lesbarkeit wird darauf verzichtet, geschlechtsspezifische Formulierungen zu verwenden.
Soweit personenbezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf alle Geschlechter.

Editorial

Sind Sie sicher, dass ihr Computer morgen noch funktioniert? Ich nicht.
Zu hoch ist die Anzahl der notwendigen Einzelsysteme, die allesamt funktionieren müssen um moderne Datenverarbeitung zu ermöglichen. Zu viele Hackingangriffe waren in den letzten Jahren erfolgreich, haben Unternehmen zu wochen- und sogar monatelangen Stillständen gezwungen. Zu oft haben mich Nachrichten zu akuten IT-Sicherheitslücken erreicht, die innerhalb weniger Stunden geschlossen werden müssen, um einen Einbruch zu verhindern.
Trotzdem schreitet die Digitalisierung mit immer größeren Schritten voran. Ohne sie verlieren wir an Wettbewerbsfähigkeit gegenüber jenen, die neue Technologien wie künstliche Intelligenz bereits hoch effizient einsetzen. Doch sobald diese Effizienzgewinne erreicht sind und eine Organisation sich daran gewöhnt hat, ist ein Notbetrieb ohne IT plötzlich nicht mehr möglich – unsere Abhängigkeit steigt wieder. Stellen Sie sich einen Büroalltag in einer modernen global verteilten Organisation ohne funktionierendes Internet vor.

Besonders gefährlich wird es, wenn lebenswichtige Einrichtungen wie Krankenhäuser, Stromnetze oder die Regelsysteme eines Verkehrsmittels aufgrund eines Hackingangriffs plötzlich versagen. Der Ukrainekonflikt hat bereits gezeigt, wie IT-Systeme, von denen wir abhängig sind, gegen uns verwendet werden können: VIASAT – der Betreiber eines Satelliten-Internetservices – erkannte am 24. Februar 2022 um 3 Uhr europäischer Zeit, dass zehntausende Modems plötzlich ihre Verbindung verloren hatten[1]. Wie sich später herausstellte, hatte ein Angreifer ein einziges fehlerhaft konfiguriertes Gerät im Netzwerk ausgenutzt, um Kommunikationsverbindungen in ganz Europa, aber besonders in der Ukraine, zu zerstören. Kollateralschäden wurden dabei in Kauf genommen: Deutschlands größter Hersteller von Windkraftanlagen verlor dadurch die Fernsteuerung für mehr als 5800 seiner Windräder[2].
Welche Konsequenzen sollten wir aus solchen Vorfällen ziehen? Die Europäische Union hat mittlerweile klare Antworten: Digitalisierung ohne IT-Sicherheit ist nicht mehr akzeptabel. NIS2 und DORA sind zwei Regularien, die an der Spitze einer ganzen Reihe von Gesetzen stehen, die der gestiegenen Relevanz der Informationstechnologie Rechnung tragen. Sie zwingen Hersteller und Nutzer von IT-Systemen, Verantwortung für ihre Entscheidungen zu übernehmen. Das ist grundsätzlich zu begrüßen, aber wir müssen unbedingt darauf achten, dass diese Maßnahmen Kleinunternehmen nicht überlasten. Wir benötigen nicht nur Strafen, sondern auch Lösungen, um IT-Sicherheit effizient umzusetzen. Genau darum bemühen wir uns als KSV1870: Durch das KSÖ CyberRisk Schema werden jährlich die 25 effektivsten IT-Sicherheitsmaßnahmen von führenden CISOs Österreichs festgelegt. Die Wirtschaftskammer entwickelt dazu kostenlose Vorlagen und bietet sogar Förderungen an, um diese Maßnahmen für jedes Unternehmen erreichbar zu machen. Wir als KSV1870 setzen mit dem CyberRisk Rating eine dazu kompatible externe Überprüfung um, die speziell KMU hilft, ihre Eignung als verlässlicher Lieferant für NIS2 und DORA-Unternehmen zu beweisen.

All dies sind nur die ersten Schritte, aber diese müssen wir jetzt auch gemeinsam umsetzen. Wir unterstützen Sie dabei nach Kräften.

Ich wünsche Ihnen viel Lesevergnügen!

Ihr Alexander Mitter
Geschäftsführer der KSV1870 Nimbusec GmbH

[1] https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview online am 03.05.2024
[2] https://www.sueddeutsche.de/wirtschaft/hack-gegen-satellitennetzwerk-angriff-auf-ka-sat-9a-1.5560370 online am 03.05.2024

Inhalt

Foto: Unsplash

Foto: Freepik

Foto: Roland Rudolf | Michael Höllerer

Foto: Unsplash

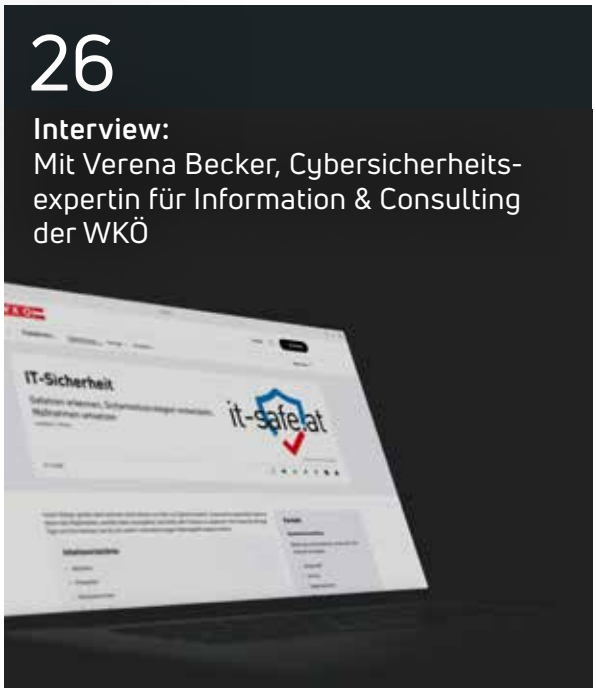


Foto: Unsplash

Foto: Unsplash

Bundesministerium Inneres

FACHBEITRAG:

Das Cybersicherheitspaket der Europäischen Union

Informationstechnologie ist Teil unseres täglichen Lebens geworden. Ihre rasche Entwicklung führt dazu, dass der Austausch von Daten und Ideen die Grenzen von Zeit und Distanz problemlos überwindet. Die Nutzer des Cyberspace sind Teil einer Globalisierung, die neue Möglichkeiten bringt, aber auch Herausforderungen, Bedrohungen und Risiken. Diesen Herausforderungen stellt sich die Europäische Kommission.

TEXT: Mag. Caroline Schmidt M.A., MAS

Die Digitalisierung unseres Alltags und der kritischen Dienste schreitet in einem enormen Tempo voran, damit verbunden ist eine höhere Verwundbarkeit. Die Covid-19 Pandemie beschleunigte die Abhängigkeit von Informationstechnologie und vergrößerte die Angriffsfläche für Cyberkriminelle. Eine Studie des Digitalverbandes Bitkom aus den Jahren 2020 und 2021 in Deutschland stellte fest, dass jedes neunte Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen ist. Statista geht in einer Umfrage aus 2022 davon aus, dass die weltweiten Kosten der Cyberangriffe für das Jahr 2022 etwa 8,4 Billionen US-Dollar kosteten. Die Kosten für Vorfälle, die durch illegale Aktivitäten im Internet verursacht werden, dürften 2023 die 11-Billionen-US-Dollar-Marke überschreiten. Bis 2026 könnten die jährlichen Kosten für Cyberangriffe weltweit 20 Billionen US-Dollar übersteigen.

Besonders risikoreich sind Angriffe auf kritische Einrichtungen wie beispielsweise Krankenhäuser. Solche Angriffe häuften sich in den letzten beiden Jahren. Hinzu kommen geopolitische Aspekte, insbesondere, dass autoritäre Regime immer stärker versuchen ihre Interessen (wirtschaftlicher und politischer Art) im Cyberraum geltend zu machen. Abgesehen von den Risiken wirtschaftlicher Natur hat die Bevölkerung ein sehr hohes Interesse an einem reibungslosen Funktionieren kritischer Einrichtungen.

> **Die Cybersicherheitsstrategie setzt vor allem auf Normsetzung auf europäischer Ebene und eine Stärkung der Kooperation im Gebiet Cybersicherheit.**

Foto: Unsplash

Im Lichte dieser Entwicklungen stellte die Europäische Kommission am 16. Dezember 2020 ein Cybersicherheitspaket vor, das die Abwehrfähigkeit der EU gegen Cyberbedrohungen stärken soll. In weiterer Folge stellte sie am 18. April 2023 ein weiteres Cyberpaket vor. Beide Pakete sollen dazu beitragen, dass man die Vorzüge vertrauenswürdiger und zuverlässiger digitaler Dienste uneingeschränkt nutzen kann. Die Cybersicherheitsstrategie setzt vor allem auf Normsetzung auf europäischer Ebene und eine Stärkung der Kooperation im Gebiet der Cybersicherheit. Im Bereich Normsetzung wurden 2020 zwei konkrete Vorschläge präsentiert: eine Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (überarbeitete NIS-Richtlinie, kurz „NIS 2“) und eine neue Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen (kurz „RKE“). Das Ziel dieser beiden Richtlinien ist ein koordiniertes und komplementäres Vorgehen bei künftigen Online- und Offline-Risiken. Die Europäische Kommission stellte einen Vorschlag für eine NIS2-Richtlinie vor. Dieser Vorschlag baut auf der Richtlinie (EU) 2016/1148 über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) auf, die der erste EU-Rechtsakt über Cybersicherheit war. Die NIS-Richtlinie hatte wesentlich zur Verbesserung der Cybersicherheitskapazitäten auf nationaler/europäischer Ebene beigetragen und verbesserte die Cyberresilienz öffentlicher und privater Einrichtungen. Die Cybersicherheitsanforderungen werden mit NIS 2 ausgebaut. Der Anwendungsbereich wurde in dem Vorschlag angepasst. Die Begriffe wesentliche Dienste und Anbieter digitaler Dienste werden ersetzt durch die Begriffe wesentliche (also besonders kritische) und wichtige Einrichtungen. Kleinst- und Kleineinrichtungen sollen, mit Ausnahmen, aus dem NIS-Anwen-

dungsbereich ausgeschlossen sein. Wichtige Einrichtungen sollen einer weniger strengen Ex-post-Kontrolle, bei Beibehaltung hoher Verpflichtungen zu Sicherheitsvorkehrungen, unterzogen werden. Wesentliche Einrichtungen werden einer Ex-ante-Kontrolle unterzogen. Die bisherigen Ermittlungen Betreiber wesentlicher Dienste entfallen. Durch diese Maßnahme soll der Aufwand für Behörden minimiert werden. Der Aufwand der Unternehmen für die Umsetzung von Sicherheitsmaßnahmen sollte gleichbleibend sein. Der Vorschlag der Europäischen Kommission hat vor allem das Ziel, dass es ein hohes Ambitionsniveau im Bereich Cybersicherheit gibt und die Maßnahmen in die Breite gehen. Die Kooperation und der Informationsaustausch zwischen den Mitgliedsstaaten soll erweitert werden. Die Verbesserung der gemeinsamen Lageerfassung und der kollektiven Vorsorge und Reaktionsfähigkeit wird ausgebaut, insbesondere durch die Festlegung von Regeln und Verfahren im Falle weitreichender Sicherheitsvorfälle oder Krisen.

> **Beide Pakete sollen dazu beitragen, dass man die Vorzüge vertrauenswürdiger und zuverlässiger digitaler Dienste uneingeschränkt nutzen kann.**

Zweitens hat die Europäische Kommission eine Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen vorgelegt. Diese muss als Gesamtpaket zusammen mit der NIS2 -Richtlinie gesehen werden. Das Ziel beider Richtlinien ist, eine generelle Erhöhung der Widerstandsfähigkeit kritischer physischer und digitaler Einrichtungen zu erreichen. Die Ausrichtung soll weggehen von einer isolierten Betrachtung physischer und digitaler Risiken hin zu einer engen Abstimmung der Maßnahmen und der rechtlichen Grundlagen. Konkret vorgeschlagene Maßnahmen in diesem Zusammenhang sind die Erweiterung der durch die Richtlinie erfassten Sektoren auf insgesamt zehn Sektoren. Die Mitgliedsstaaten müssen in Zukunft verpflichtend nationale Strategien für die Widerstandsfähigkeit kritischer Einrichtungen verfassen. Die Mitgliedsstaaten haben nunmehr die Pflicht, regelmäßige Risikobewertungen und die Identifikation von kritischen Einrichtungen in den Sektoren durchzuführen. Des Weiteren werden Verpflichtungen für kritische Einrichtungen in den Bereichen Risikoanalysen und Sicherheitsvorkehrungen sowie hinsichtlich Meldeverpflichtungen vorgesehen. Die autorisierte nationale Behörde kann die Einhaltung der Verpflichtungen überprüfen und bei Bedarf Sanktionen vorsehen. Die Umsetzung der beiden Richtlinien müssen wir als Chance sehen, um die Resilienz in Österreich und der EU zu erhöhen. Das Cybersicherheitspaket wird neue Aufgaben und Ressourcenbedarf für die betroffenen Behörden und Einrichtungen bedeuten, aber in Summe einen Mehrwert für die Sicherheit Österreichs haben.

Wer Digitalisierung sagt, muss auch Cybersicherheit sagen. Dieses Motto scheint die Europäische Kommission mit ihrem Cybersicherheitspaket konsequent zu verfolgen. Wenn man an den plötzlichen Stillstand kritischer Einrichtungen wegen eines physischen oder digitalen Angriffs denkt, dann ist dies ein düsteres Bild. Es ist wichtig, bereits heute Vorkehrungen zum Schutz wesentlicher und wichtiger Dienste zu treffen und die Kooperation in der EU zu verstärken, um im Fall des Falles gut vorbereitet zu sein. Die Unterstützung und rasche nationale Umsetzung des Cybersicherheitspakets sind daher wichtig. ■

Foto: Privat | Caroline Schmidt

MAG.
CAROLINE SCHMIDT M.A., MAS

Caroline Schmidt (Bundesministerium für Inneres BMI) ist **Programmdirektorin für die Umsetzung des EU-Cybersicherheitspakets**, das die neue Netz- und Informationsrichtline umsetzt.

NIS2 IM DETAIL ››

Foto: Stockvault

FACHBEITRAG:

Oktober 202

Am 16. Dezember 2020 stellte die EU-Ko
welches neben einer neuen Cybersicherh
sicherheitsrichtlinie enthielt. Diese Cyber
Richtlinie" und ersetzt die erste NIS-Rich
Jänner 2023 in Kraft getreten und ist bis

TEXT: Mag. Vinzenz Heußler, LL.M.

Die in diesem Artikel dargelegten Informationen un
Meinung der Europäischen Kommission.

ZIEL

Die NIS2-Richtlinie verfolgt das Ziel, ein hohes gemeinsames Cybersicherheitsniveau in der EU zu erreichen, indem sie den bestehenden Rechtsrahmen modernisiert. Während die NIS-Richtlinie das Fundament legte, baut die NIS2-Richtlinie nun auf diesem auf und verbessert es. Dabei sollen nicht nur die großen Unterschiede zwischen den Mitgliedstaaten beseitigt und aus den Defiziten der NIS-Richtlinie gelernt werden, sondern auch die vorangeschrittene Digitalisierung unserer Gesellschaft und Wirtschaft – nicht zuletzt beschleunigt durch die COVID-19-Pandemie – und die sich rasch weiterentwickelnden Bedrohungen für die Cybersicherheit berücksichtigt werden.

ANWENDUNGSBEREICH

Die wohl größte Änderung der NIS2-Richtlinie liegt in der enormen Ausweitung des Anwendungsbereichs. Um zukunftsfit zu sein und ein großes Spektrum der wirtschaftlich kri-

4: NIS 2.0 kommt

mmission ein neues Cybersicherheitspaket vor,
heitsstrategie auch den Vorschlag für eine neue Cyber-
rsicherheitsrichtlinie firmiert unter dem Namen „NIS2-
tlinie aus dem Jahr 2016. Die NIS2-Richtlinie ist am 16.
17. Oktober 2024 in nationales Recht umzusetzen.

d Ansichten sind die des Autors und repräsentieren nicht die offizielle

tischen Aktivitäten zu schützen, wird die Anzahl der betroffenen Einrichtungen stark erhöht, und zwar EU-weit von derzeit ca. 15.000 sogenannten Betreiber wesentlicher Dienste hin zu mehr als 110.000 Einrichtungen. Denn prinzipiell werden vom

> **Die wohl größte Änderung der NIS2-Richtlinie liegt in der enormen Ausweitung des Anwendungsbereichs.**

Anwendungsbereich der NIS2-Richtlinie alle öffentlichen und privaten Einrichtungen umfasst sein, die einer bestimmten Art von Einrichtung entsprechen und die größer als Kleinunternehmen sind. Durch die Schaffung eines De-facto-Anwendungsbereichs über 18 Sektoren hinweg, der auf objektive Größenkriterien abstellt, soll ein Level-Playing-Field in der EU sichergestellt werden.

WESENTLICHE & WICHTIGE EINRICHTUNGEN

Die NIS2-Richtlinie differenziert beim Anwendungsbereich zwischen sogenannten wesentlichen und wichtigen Einrichtungen. Grundsätzlich gelten alle in den Sektoren des Anhangs I (Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, Verwaltung von IKT-Diensten, öffentliche Verwaltung und Weltraum) genannten 53 Arten von Einrichtungen als wesentliche Einrichtungen, wenn sie Großunternehmen sind. Alle anderen Einrichtungen gelten als wichtige Einrichtungen, also insbesondere mittlere Unternehmen in den oben genannten Sektoren sowie die 14 Arten von Einrichtungen, die in den Sektoren des Anhang II (Post- und Kurierdienste, Abfallbewirtschaftung, Chemie, Lebensmittel, Verarbeitendes und produzierendes Gewerbe, Anbieter digitaler Dienste und Forschung) genannt werden. Während wesentliche Einrichtungen einer strengeren (ex-ante) Aufsicht und höheren Strafdrohungen (Höchststrafe von mindestens 10.000.000 EUR oder 2 % des Umsatzes) unterliegen, sollen für wichtige Einrichtungen eine weniger strenge (ex-post) Aufsicht, verminderter Dokumentationsaufwand und niedrigere Strafdrohungen (Höchststrafe von mindestens 7.000.000 EUR oder 1,4 % des Umsatzes) gelten.

RISIKOMANAGEMENT-MASSNAHMEN & BERICHTSPFLICHTEN

Was jedoch sowohl den wesentlichen als auch den wichtigen Einrichtungen gemein ist, ist die Pflicht, Maßnahmen zur Erhöhung ihrer Cyber-Resilienz zu ergreifen. Konkret müssen

> **Ein weiterer bedeutender Punkt der NIS2-Richtlinie ist, dass Cybersicherheit in Zukunft zur Top Management Sache gemacht wird.**

sie Risikomanagement-Maßnahmen im Bereich der Cybersicherheit umsetzen und Berichtspflichten an das Computer-Notfallteam im Falle von signifikanten Sicherheitsvorfällen nachkommen. Es handelt sich bei diesen beiden Kernpflichten um das Herzstück der NIS2-Richtlinie. Im Gegensatz zur NIS-Richtlinie aus 2016 sind die Sicherheitsanforderungen und Meldepflichten detaillierter gestaltet und stärker harmonisiert, wodurch die Cyberresilienz gesamt europäischen betrachtet auf ein gleiches Niveau gebracht werden soll.

Konkret müssen sie Risikomanagement-Maßnahmen im Bereich der Cybersicherheit umsetzen und Berichtspflichten an das Computer Notfallteam im Falle von signifikanten Sicherheitsvorfällen nachkommen. Es handelt sich bei diesen beiden Kernpflichten um das Herzstück der NIS2-Richtlinie.

SICHERHEIT DER LIEFERKETTE

Was die Risikomanagement-Maßnahmen betrifft, legt die NIS2-Richtlinie einen besonderen Fokus auf das Thema der Sicherheit der Lieferkette. Gerade KMU werden zunehmend zum Ziel von Angriffen auf die Lieferkette. Diese Angriffe auf die Lieferkette können über die KMU hinaus auch eine Kaskadenwirkung auf die von ihnen belieferten Einrichtungen haben. Daher haben alle wesentlichen und wichtigen Einrichtungen sicherheitsbezogene Aspekte der Beziehungen zwischen ihnen und ihren unmittelbaren Lieferanten zu berücksichtigen, was explizit spezifische Schwachstellen der Lieferanten, die Gesamtqualität der Produkte und ihre Cybersicherheitspraxis betrifft. Infolgedessen ist davon auszugehen, dass die NIS2-Richtlinie im mittelbaren Weg positive Auswirkungen auf das Cybersicherheitsniveau nicht nur von den ohnehin schon zahlreichen wesentlichen und wichtigen Einrichtungen, sondern auch auf ihre Lieferanten und Service Provider haben wird.

LEITUNGSORGANE

Ein weiterer bedeutender Punkt der NIS2-Richtlinie ist, dass Cybersicherheit in Zukunft zur Top Management Sache machen wird, weil die Leitungsorgane die Risikomanagement-Maßnahmen genehmigen und spezielle Cybersicherheitsschulungen absolvieren werden müssen. Zweck dieser Bestimmung ist es, das für die Cybersicherheit notwendige Bewusstsein auf der Ebene der Geschäftsführer:innen und der Vorstände zu erzeugen.

FÄHIGKEITEN DER BEHÖRDEN & CYBERSICHERHEITSSTRATEGIEN

Die NIS2-Richtlinie baut zudem die Fähigkeiten der Behörden stark aus und stattet sie mit weitreichenderen Befugnissen aus. Auch werden die Mitgliedstaaten viel umfangreichere und detailliertere nationale Cybersicherheitsstrategien verabschieden müssen, die unter anderem auch

Foto: Freepik

einen Rahmen für die koordinierte Offenlegung von Schwachstellen enthalten werden müssen. Dieser nicht zu vernachlässigende Faktor im Auffinden und Schließen von Schwachstellen fehlt in den meisten Mitgliedstaaten, einschließlich Österreich, aktuell noch. Des Weiteren sieht die NIS2-Richtlinie erstmals auch Mechanismen vor, um auf große Sicherheitsvorfälle mit europäischer Dimension entsprechend reagieren zu können. So werden alle Mitgliedstaaten einen nationalen Rahmen für das Cybersicherheitskrisenmanagement schaffen und nationale Cyberkrisen-Behörden benennen sowie auf europäischer Ebene in einem neuen

MAG.
VINZENZ HEUSSLER, LL. M.

Vinzenz Heußler ist in der EU-Kommission (DG CNECT) als Policy Officer tätig und arbeitet an der Konzeption und Koordinierung politischer Entwicklungen sowie der Weiterverfolgung politischer und legislativer Vorschläge im Rahmen des interinstitutionellen Entscheidungsprozesses, um die Kohärenz bei der Umsetzung der Kommissionspolitik im Bereich der Cybersicherheit und des digitalen Datenschutzes zu gewährleisten. Zuvor war er als Leiter des Büros für strategische Netz- und Informationssystemsicherheit (NIS-Büro) im Bundeskanzleramt als federführender Jurist für die Legistik zur Umsetzung der NIS-Richtlinie in Österreich verantwortlich und vertrat Österreich in zahlreichen europäischen Gremien für Cybersicherheit. In dieser Funktion koordinierte er auch die Verhandlungen zur NIS2-Richtlinie für Österreich.

Was die Risikomanagement-Maßnahmen betrifft, legt die NIS2-Richtlinie einen besonderen Fokus auf das Thema Sicherheit der Lieferkette.

Netzwerk der Verbindungsorganisationen für Cyberkrisen (CyCLONe) zusammenarbeiten müssen. Dadurch sollen die gemeinsame Lageerfassung in der EU sowie die kollektive Vorsorge und Reaktionsfähigkeit verbessert werden. Zusammenfassend kann gesagt werden, dass die NIS2-Richtlinie durch den vereinheitlichten und weiten Anwendungsbereich, die harmonisierten Bestimmungen zu den Sicherheitsmaßnahmen und zu den Berichtspflichten, die Lieferkettensicherheit sowie durch das Schaffen gleicher Fähigkeiten der Behörden einen wichtigen Schritt zur weiteren Erhöhung der gesamteuropäischen Cyberresilienz macht. Von der NIS2-Richtlinie darf daher ein nicht unerheblicher „Boost“ für die österreichische und europäische Cybersicherheit erwartet werden. ■

ZUM NIS2 FACT SHEET ››

NIS2: Anwendungsbereiche

Wesentliche Einrichtungen

Als wesentliche Einrichtungen gelten große Unternehmen aus den Sektoren:

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfra-strukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser*
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten (B2B)*
- Öffentliche Verwaltung*
- Weltraum*

Wichtige Einrichtungen

Als wichtige Einrichtungen gelten mittlere Unternehmen in den oben genannten 11 Sektoren, sowie weitere Arten großer und mittlerer Unternehmen aus den Sektoren:

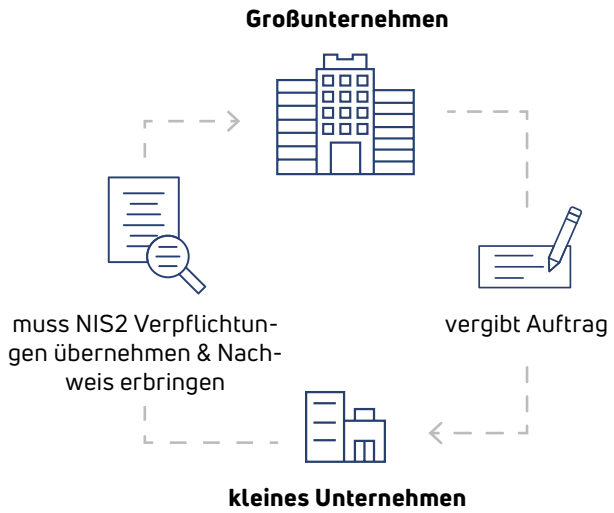
- Post- & Kurierdienste*
- Abfallbewirtschaftung*
- Chemie*
- Lebensmittel*
- Verarbeitendes & herstellendes Gewerbe*
- Anbieter digitaler Dienste
- Forschung*

* Neue Sektoren gegenüber NIS1

Achtung: Indirekte Betroffenheit durch Lieferkette

NIS2 reguliert große Unternehmen

Großunternehmen haften für ihre Lieferanten und können NIS2 Verpflichtungen nicht durch Auslagerung umgehen.



Best Practices für NIS2 Nachweise

Laut dem "NIS Fact Sheet 9/2022" des Bundeskanzleramt und BMI:

Quelle: https://www.nis.gv.at/dam/jcr:bbe1c393-ba27-43b3-8d38-890610cfcc75/NIS_Factsheet_9_2022_1_0.pdf

- → ÖISHB: Zusammenarbeit mit Externen, Lieferantenbeziehungen
- → ISO/IEC 27001: Information security in supplier relationships
- → IEC 62443 2-1: Supply chain security
- → CIS CSC v8.0: Service Provider Management

BASIS DES CYBERRISK RATINGS BY KSV1870:

- → KSÖ Cyber Risk Rating: Anforderungen für A bzw. B Rating

Foto: Freepik

Kerninhalte

Risikomanagement

FÜR UNTERNEHMEN BESONDERS RELEVANT

- → Maßnahmen wie z. B. Sicherheit der Lieferkette
- → Verantwortlichkeit und Schulung des Top-Managements
- → Berichtspflichten bei erheblichen Sicherheitsvorfällen und Bedrohungen

Fähigkeiten der Mitgliedstaaten

- → Koordinierte Offenlegung von Schwachstellen
- → Aufbau eines nationalen Rahmens für Cyberkrisenmanagement
- → Weiterentwicklung der nationalen Cybersicherheitsstrategien
- → Ausbau der Fähigkeiten und Befugnisse der Cybersicherheitsbehörden

Kooperation & Informationsaustausch

- → Europäische Schwachstellendatenbank
- → Europäisches Netzwerk für die Bekämpfung von Cyberkrisen
- → Austausch von Informationen zur Cybersicherheit zwischen Unternehmen
- → Bericht über den Stand der Cybersicherheit in der EU

Geldbußen

! Natürliche Personen (leitende Angestellte) können für Pflichtverletzungen haftbar gemacht werden.

Für wesentliche Einrichtungen

Bußgeldhöchstbetrag von mindestens
€ 10.000.000,-

ODER

2% des Jahresumsatzes
weltweit, im vorangegangenen Geschäftsjahr getätigt

Für wichtige Einrichtungen

Bußgeldhöchstbetrag von mindestens
€ 7.000.000,-

ODER

1,4% des Jahresumsatzes
weltweit, im vorangegangenen Geschäftsjahr getätigt

Die Security-Landschaft Österreichs im Überblick

Im Zuge des CyberRisk Ratings wurde ein groß angelegter Security Scan quer durch Österreichs Unternehmenslandschaft durchgeführt. Daraus konnten im Bezug auf mit Malware infizierte Webseiten folgende Schlüsse gezogen werden:

DATENANALYSE: KSV1870 Nimbusec GmbH | **TEXT:** Alexander Mitter

~200

Webseiten österreichischer Unternehmen sind durchschnittlich gehackt und stellen ein hohes, aktives Sicherheitsrisiko für Besucher dar. Welche das sind, ändert sich von Monat zu Monat. Seit 2022 enthält deshalb jede KSV1870 Bonitätsauskunft den WebRisk Indicator.

Hacker platzieren auf diesen Webseiten aggressiven Programmcode, der Computerviren installiert oder auch schlicht Cryptominer, die auf (Strom-)Kosten der Webseitebesucher Kryptowährungen erzeugen. Die verantwortlichen Unternehmen werden durch eine unentgeltliche Zusammenarbeit von KSV1870 Nimbusec mit dem österreichischen Cyber Emergency Response Team (CERT.at) aktiv kontaktiert. Dadurch versuchen wir das Internet sicherer zu machen.

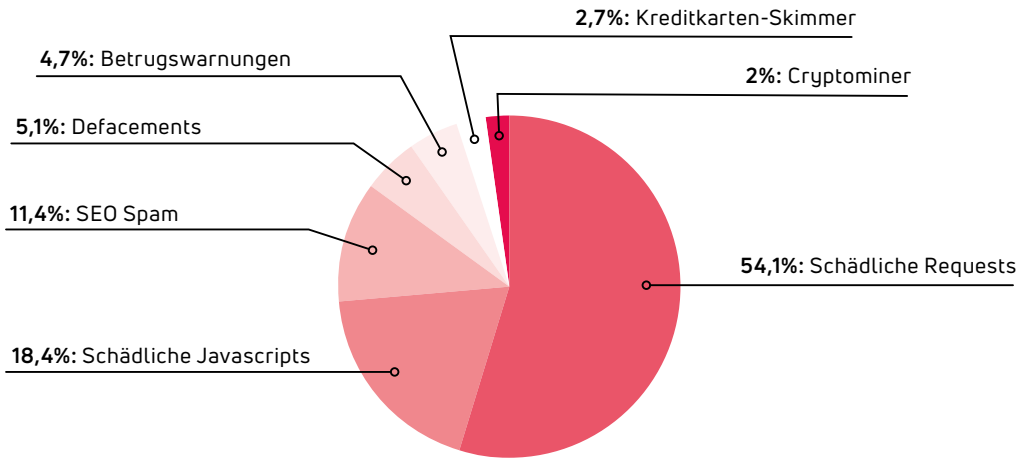
90%

dieser über 200 gehackten Webseiten sind nach einem Monat immer noch nicht durch ihre Inhaber bereinigt und stellen weiterhin ein aktives Sicherheitsrisiko dar.

4.253.411

WebRisk Indicatoren wurden bereits berechnet.

Gefundene Malware nach Kategorie



CyberRisk Rating: Zahlen, Daten, Fakten 2024

DATENANALYSE: Alen Kocaj | **TEXT:** Alexander Mitter, Elisabeth Hentscholek

12.342

Lieferanten sind in der CyberRisk Rating Datenbank bereits enthalten. All diese Lieferanten beliefern Unternehmen, die ab Oktober 2024 unter NIS2 fallen.

Das CyberRisk Rating by KSV1870 ist damit mittlerweile die umfangreichste Datenbank für IT-Sicherheitsnachweise nach NIS. Die Datenbank enthält aber nicht nur CyberRisk Ratings und Cyber Trust Label: Viele Lieferanten nutzen auch die Möglichkeit, proaktiv andere Nachweise wie zum Beispiel ISO27001 zu hinterlegen.
Dieses Angebot ist kostenlos und macht den CyberRisk Manager zur offenen Basis für Third Party Cyber Risk Management nach NIS.

Falls Sie Ihren IT-Sicherheitsnachweis hinterlegen möchten, senden Sie ihn an support@cyberrisk-rating.at.

87,1%

der Unternehmen überschätzen die eigene Cybersicherheit Diese Unternehmen haben bei der Beantwortung des Assessments eine oder mehrere Anforderungen mit "Ja" beantwortet, konnten aber nicht schlüssig darstellen, dass diese Anforderungen im vom KSÖ Schema geforderten Ausmaß umgesetzt wurden.
Bei den Fragen zu Protokollierung, Whitelisting und Betriebskontinuität trat Selbstüberschätzung weiterhin am häufigsten auf.

Diese Zahl unterstreicht, wie wichtig eine professionelle Validierung von Aussagen zur Cybersicherheit ist.

1 VON 3

Unternehmen hat sich bei der Auswahl ihres CyberRisk Ratings gegen das vom Auftraggeber geforderte Rating entschieden.
Die Kunden erwarten oft ein höheres Cybersicherheitsniveau von ihren Lieferanten. In Wirklichkeit ist dieses jedoch nicht vorhanden, was bedeutet, dass die Lieferketten in einem schlechteren Zustand sind, als erwartet.

35%

jener kritischer Lieferanten, für die ein A-Rating angefragt wurde, können den Anforderungen nicht gerecht werden.

16%

der Unternehmen weisen ein mangelndes Basissicherheitslevel (B-Rating) auf.

70%

der Unternehmensantworten mussten von der Validierung rückgefragt werden, da die initiale Antwort nicht schlüssig oder detailliert genug war.

Das bedeutet, dass Aussagen zur Cybersicherheit unbedingt hinterfragt werden müssen, weil unterschiedliche Interpretationen von Fachbegriffen oft zu Missverständnissen führen.

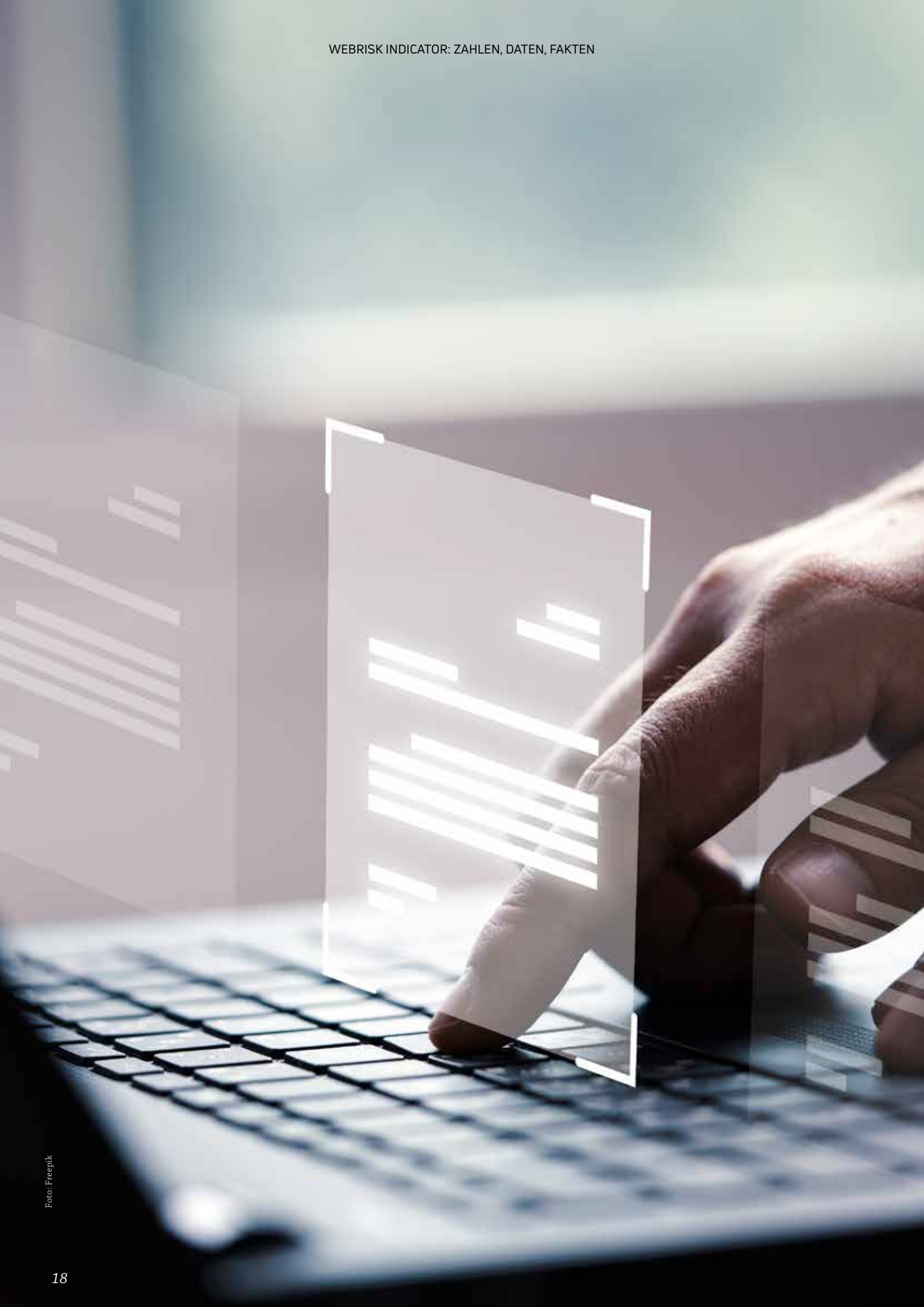


Foto: Freepik

WebRisk Indicator: Zahlen, Daten, Fakten 2024

Im CyberRisk Rating-Prozess dient der WebRisk Indicator als Basisinformation zur Ersteinschätzung der Cyberrisiken eines Unternehmens. Er basiert auf von außen zugänglichen Informationen und kann dank Automatisierung in Kürze für jedes Unternehmen erstellt werden. Der Wertebereich des WebRisk Indicators reicht von 100-700, wobei gilt: je niedriger der Wert, desto besser das Ergebnis. **DATENANALYSE:** KSV1870 Nimbusec GmbH | **TEXT:** Alexander Mitter, Elisabeth Hentscholek

DURCHSCHNITTLICHER WEBRISK INDICATOR FÜR ÖSTERREICH

∅ 219,5

Österreichs Unternehmen schneiden im Durchschnitt mit einem WebRisk Indicator von 219,5 ab. (Wertebereich von 100-700, das Ergebnis wurde um 0-Summen bereinigt und gerundet.)

FÜR DIE STATISTIK HERANGEZOGENE UNTERNEHMEN

205.326

Mehr als 200.000 Unternehmen und deren Webseiten wurden für diese Statistik ausgewertet.

NIS2: ENERGIE

192,1

Österreichische Unternehmen die dem NIS2 Sektor "Energie" zugeordnet werden können, erzielten durchschnittlich ein WebRisk Indicator Ergebnis von 192,1.
Damit betreiben sie die am besten gewarteten Webseiten.

Ein guter Webrisk Indicator schafft vom ersten Moment der Zusammenarbeit an Vertrauen - das hat sich die Energiewirtschaft offensichtlich zu Herzen genommen. Möglicherweise hat dazu aber auch beigetragen, dass die Energieunternehmen schon seit vielen Jahren IT-Sicherheit leben und entsprechend oft bereits auditiert wurden. In jedem Fall: Gratulation! Unsere Energiewirtschaft nimmt dieses Thema ernst und das ist auch sichbar.

WIE KANN ICH WEBSEITEN UND WEBRISK INDICATOR VERBESSERN?

COOKIES

Noch immer verteilen viele Webseiten Cookies von Drittanbietern, die eigentlich eine Zustimmung benötigen würden. Diese 3rd Party Cookies ermöglichen Tracking von Besuchern über mehrere Webseiten hinweg und dürfen daher nicht ungefragt abgespeichert werden.

BESSERE PRÄVENTIVE SICHERHEITSMASSNAHMEN

Ob Patching, Security Header oder verpflichtende Verschlüsselung: Unternehmen können mit einfachen Mitteln die IT-Sicherheit ihrer Onlineangebote deutlich anheben.

HTTPS/TLS-VERSCHLÜSSELUNG DER ÜBERTRAGUNG

Ohne das "Schloss" in der Adresszeile - dem Indikator für eine funktionierende Verschlüsselung auf dem Weg zwischen Webseitenbesucher und Webserver - sind Datenpakete so einfach auslesbar wie eine Postkarte. Leider vergessen Unternehmen aber nach wie vor, dass diese Verschlüsselung und die damit verbundenen Zertifikate regelmässig aktualisiert und korrekt konfiguriert werden müssen. Zusätzlich sollte eine Webseite unverschlüsselt schlicht gar nicht mehr erreichbar sein. Technisch für Fachleute leicht machbar, wird auch hier oft vergessen, die notwendigen Schritte zu setzen.

BEWERTUNGSABLAUF:

Wie kommen Ratings zustande?

DATENANALYSE: KSV1870 Nimbusec GmbH | **TEXT:** Alexander Mitter, Elisabeth Hentscholek

Ablauf des Assessments – für bewertete Unternehmen

BEANTWORTUNG
Anforderungen beantworten

Das Assessment besteht aus 25 Anforderungen, die mit Ja oder Nein zu beantworten sind. Im Falle einer "Ja"-Beantwortung, muss textuell beschrieben werden, wie die jeweilige Maßnahme im Unternehmen umgesetzt wird.

VALIDIERUNG
Validierung der gegebenen Antworten

Die im Assessment gegebenen Antworten des zu bewertenden Unternehmens werden von qualifizierten Prüfern validiert. Nur schlüssige und fachlich korrekte Antworten werden akzeptiert. Mehr als 70% der Antworten bestehen diese erste Validierung nicht.

KORREKTUR
Unklare Antworten genauer ausführen

Das zu bewertende Unternehmen hat einmalig die Möglichkeit, für den Prüfer unklare Antworten genauer auszuführen und zu korrigieren.

RE-VALIDIERUNG
Finale Validierung der gegebenen Antworten

Auf Basis der korrigierten Antworten berechnen unsere Prüfer nun das CyberRisk Rating des jeweiligen Unternehmens.

VERÖFFENTLICHUNG
A- oder B-Rating auswählen

Das zu bewertende Unternehmen hat nun die Möglichkeit, zwischen der Veröffentlichung des A- (Advanced Security) oder B-Ratings (Basic Security) zu wählen.

Assessmentdauer
am Beispiel von acht Lieferanten

CyberRisk Ratings werden im direkten Austausch mit Personen des bewerteten Unternehmen erstellt. Das erhöht die Aussagekraft gegenüber rein externen Betrachtungen massiv, aber bedeutet auch einen deutlich höheren Zeitaufwand.

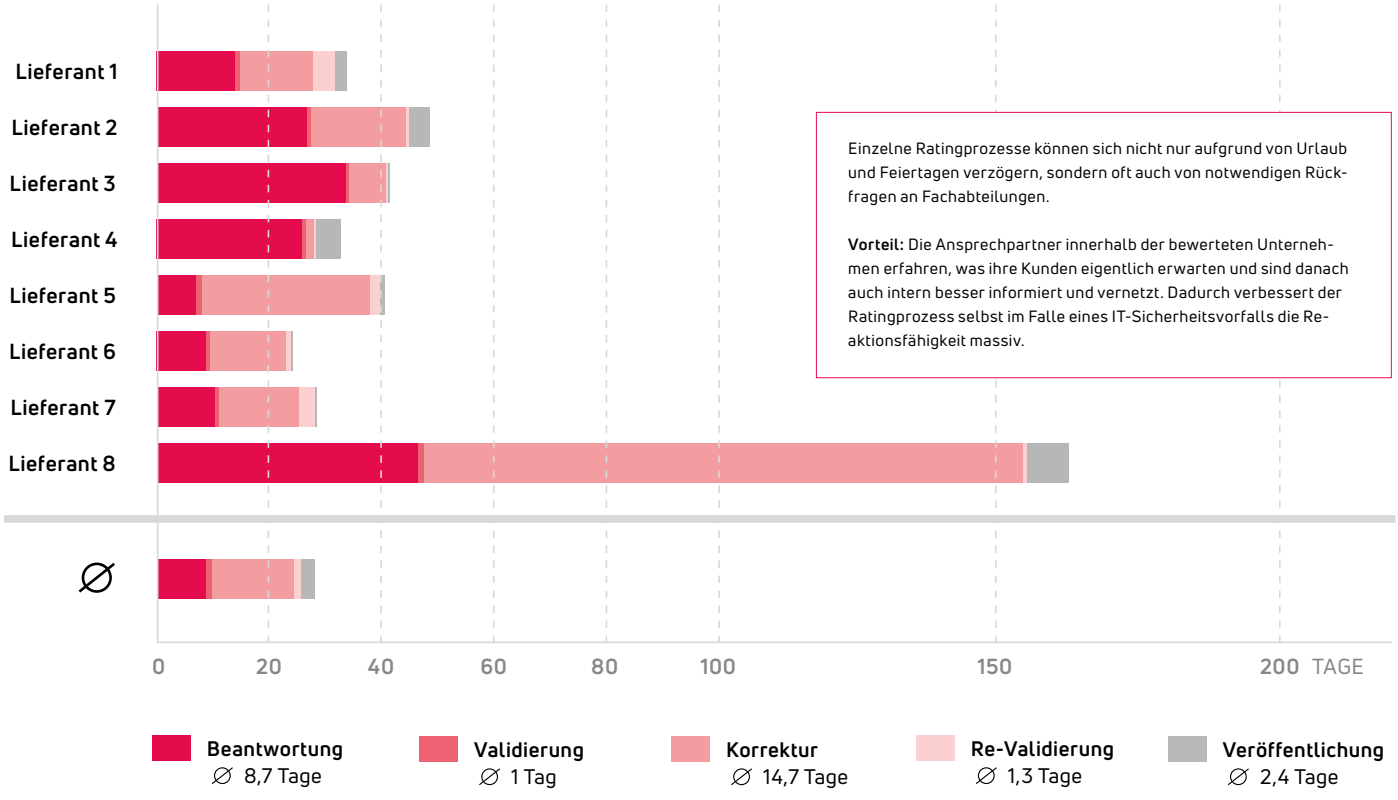
Zu Beginn identifizieren Mitarbeiter von KSV1870 Nimbusec die zuständigen Ansprechpersonen im bewerteten Unternehmen. Dazu wird der Kontakt per E-Mail und Telefon auf Englisch (international) oder Deutsch aufgebaut.

Ist die zuständige Person gefunden, informieren die KSV1870 Mitarbeiter über den Zweck, Ablauf und Hintergrund des Ratings: Kein Unternehmen stimmt einer IT-Sicherheitsbewertung zu, ohne genau verstanden zu haben, wie die erhobenen Daten verwendet werden. Diese Schritte nehmen durchschnittlich über 8 Tage in Anspruch, da Ansprechpartner oft nicht klar definiert oder erreichbar sind - ein Problem im Fall eines echten Hackingangriffs!

Nun beginnt die Kernphase des Ratings: Die 25 Fragen des KSÖ CyberRisk Schemas werden erstmalig beantwortet und an die Validierung übermittelt. Innerhalb von maximal zwei Werktagen erhält das bewertete Unternehmen von IT-Sicherheitsexperten Feedback, ob die Beantwortungen die gestellten Anforderungen erfüllen oder nicht. Bei mehr als 70% der Antworten werden tiefer gehende Rückfragen gestellt, um Sicherheit zu bekommen.

Im letzten Schritt erhält das bewertet Unternehmen die Möglichkeit Antworten zu präzisieren und erneut einzureichen. Dieses Feedback löst Missverständnisse auf und stellt eine korrekte, aber auch faire Bewertung sicher.

Das finale Rating wird gemeinsam mit einer digital signierten Zusammenfassung der Ratingantworten an das bewertete Unternehmen übermittelt. Nach Abschluss dieser Übermittlung löscht der KSV1870 die Detailantworten wieder, um langfristige Datensicherheit sicherzustellen.



Welches CyberRisk Rating-Ergebnis hätte Ihr Unternehmen erzielt?

→ **Die kostenlose Demoversion des CyberRisk Rating by KSV1870 finden Sie hier:**
https://demo.cyberrisk-rating.at

Es handelt sich hier lediglich um das Assessment, ohne Validierung. Ihre Angaben werden nicht gespeichert.

→ Mehr Infos zu Rating und Ablauf erhalten Sie außerdem unter **www.cyberrisk-rating.at** oder per E-Mail an **support@cyberrisk-rating.at**

Foto: Georges Schneider | Raiffeisenhaus Wien

INTERVIEW:

„Innovation ist keine Frage des Alters."

Business Angel Gerald Hübsch und **Alexander Janda, Generalsekretär des KSÖ**, im Gespräch mit **Michael Höllerer, Generaldirektor Raiffeisen NÖ-Wien**.

TEXT: Dr. Gerald Hübsch, Dr. Alexander Janda

Sehr geehrter Herr Höllerer, wie ist die Raiffeisenlandesbank NÖ-Wien heute aufgestellt und wie führen Sie diese traditionsreiche Bank in die digitale Zukunft?

Als Geschäftsbank wollen wir den mehr als 1,2 Millionen Kundinnen und Kunden der Raiffeisen Bankengruppe NÖ-Wien im geschäftlichen und privaten Mittelstand auch im digitalen Zeitalter ein komplettes Dienstleistungsportfolio bieten und weiterhin ihr verlässlicher, sicherer Partner sein. Dies bildet zugleich den Rahmen für unsere Geschäftsstrategie, die sich auf drei Säulen stützt:

1. Kundenzentrierung:

Die Bedürfnisse unserer Kund:innen und Zielgruppen bestimmen das Leistungsangebot.

2. Innovation:

In enger Abstimmung mit unseren Kund:innen und gemeinsam mit führenden Technologieunternehmen unserer Branche – beispielsweise dem österreichischen FinTech Bitpanda – identifizieren wir in einem periodischen Innovationsprozess zahlreiche Ideen für neue Dienste und Lösungen.

3. Unternehmenskultur:

Und nicht zuletzt beeinflusst die digitale Transformation auch unsere DNA, erfordert ein positives Mindset und neue, agile Methoden. Eine wichtige Erkenntnis zeigt übrigens, dass Innovationsfreude keine reine Frage des Alters ist.

Diese drei Eckpfeiler wecken zudem das Interesse junger talentierter Menschen und machen uns als Arbeitgeber attraktiv. Bei Innovationsideen legen wir großen Wert auf die enge Interaktion mit unseren Kund:innen und das frühe, praxisnahe Feedback zu den künftigen Lösungen. Besonders spannend zeigt sich dabei die Zusammenarbeit zwischen jungen „Digital Natives" im Front-End-Bereich und erfahrenen Kennern unserer internen Prozesse und Back-End-Systeme. Nur so gelingen uns intuitiv verständliche und gut integrierte Ende-zu-Ende-Lösungen, die von den Kund:innen auch gerne genützt werden.

„Erst eine durchgängige, monetäre Bewertung und Transparenz über unsere geschäftlichen Cyberrisiken verschafft uns ein klares Bild über die Bedrohungslage."

Foto: Roland Rudolf | Michael Höllerer

„Kundenzentrierung ist oberstes Gebot: Die Bedürfnisse unserer Kundinnen und Kunden bestimmen auch in Hinkunft unser Leistungsangebot."

Foto: Roland Rudolf | Michael Höllerer

Weiters sehen wir, dass die Kund:innen das gewohnte Komplettangebot unserer Bank auch in der digitalen Welt wünschen, unsere Verlässlichkeit schätzen und Sicherheit suchen. Diesen Erfolgsgarant gilt es – gepaart mit innovativen, neuen Lösungen – auch künftig zu bewahren.

Digitalisierung stiftet nicht nur Nutzen und Komfort, sondern erhöht zwangsläufig auch die Abhängigkeit von IT-Systemen. Welche Rolle spielt dabei das Informationssicherheits- und Cyberrisikomanagement in Ihrem Unternehmen?

Eine zentrale. Ein funktionierendes Cyberrisikomanagement ist für unser Institut erfolgskritisch. Erst eine durchgängige, monetäre Bewertung und Transparenz über unsere geschäftlichen Cyberrisiken verschafft uns ein klares Bild über die Bedrohungslage. Dies erlaubt uns, die richtigen Prioritäten zu setzen und Investitionsentscheidungen zu treffen, so dass wir die Risiken effektiv kontrollieren und mit gezielten Gegenmaßnahmen sicher im Griff haben können. Wir stützen uns dabei auf die tiefe Expertise unseres Providers, der Raiffeisen Informatik. Ein weiterer wesentlicher Beitrag kommt von unseren Mitarbeiterinnen und Mitarbeitern. Sie absolvieren regelmäßig Awareness Trainings in Informationssicherheit und nehmen an ausgefeilten, praktischen Übungen teil.

Ist ein zunehmender Austausch zum Thema Informationssicherheit zwischen den in Österreich tätigen Banken erkennbar?

Bei allem Bemühen, unsere sicherheitstechnischen Hausaufgaben bestmöglich zu lösen, gewinnt der Erfahrungsaustausch innerhalb der Banken- und ebenso Versicherungsbranche an Bedeutung. Wir sitzen in dieser Hinsicht alle im selben Boot: Niemand hat ein Interesse daran, dass es einen Branchenkollegen „erwischt" – dies würde das Vertrauen der Kunden in alle Institute schwächen.

Können Ihre Mittelstandskund:innen ebenso ein bedarfsgerechtes

Sicherheitsniveau erreichen oder fehlen Ihnen häufig die personellen Ressourcen dafür?

Wir bemühen uns, auch die im Finanzgeschäft unverzichtbaren Sicherheitsbedürfnisse unserer Kund:innen zu verstehen und sie dabei verstärkt zu begleiten. Sicherheit braucht Partnerschaften und den gemeinsamen Zugriff auf Experten-Know-how.

Kann das CyberRisk Rating dabei einen Beitrag leisten?

Absolut. Wir betrachten das CyberRisk Rating als Einstieg und wertvollen „Puzzle-Stein" auf dem Weg zu sicheren Finanztransaktionen in der digitalen Welt. Ergänzend gewinnt die Abdeckung bestimmter Cyberrisiken bzw. Schadensfälle durch geeignete Versicherungsmodelle zunehmend an Bedeutung.

Werden wir auch in Zukunft noch mit unseren Bankberater:innen sprechen – oder übernimmt die Künstliche Intelligenz das Ruder?

Das Komplettangebot und die Verlässlichkeit einer renommierten Bank werden auch künftig von unseren Kund:innen geschätzt. Wenngleich sie zahlreiche Transaktionen über unsere digitalen Lösungen selbst wahrnehmen, suchen sie gerne das persönliche Gespräch bei wichtigen Investitions- und Finanzierungsfragen, denken Sie nur an den Hausbau oder den Erwerb einer Wohnung. Wir machen sehr gute Erfahrungen mit unserem Omnikanal-Ansatz, bei dem unsere Kund:innen ganz individuell auf ihrem bevorzugten Weg ihre Wünsche mit uns teilen. Künstliche Intelligenz kann dabei künftig unsere Dienstleistungen verstärkt an die individuellen Bedürfnisse unserer Kund:innen anpassen. Insgesamt betrachtet stehen wir vor spannenden Entwicklungen und Herausforderungen. Die Kerntugenden unserer Bank stellen dabei auch im digitalen Zeitalter das Vertrauen unserer Kund:innen sicher.

Sehr geehrter Herr Höllerer, wir danken für das Gespräch! ■

Foto: Georges Schneider | Raiffeisenhaus Wien

ZUM INTERVIEWPARTNER:

MAG.
MICHAEL HÖLLERER

Michael Höllerer ist Generaldirektor der **Raiffeisenlandesbank NÖ-Wien** und der **Raiffeisen-Holding NÖ-Wien**. Die ambitionierte Weiterentwicklung der beiden Unternehmen, insbesondere der aus der Digitalisierung resultierende Kundennutzen, sind ihm ein großes persönliches Anliegen.

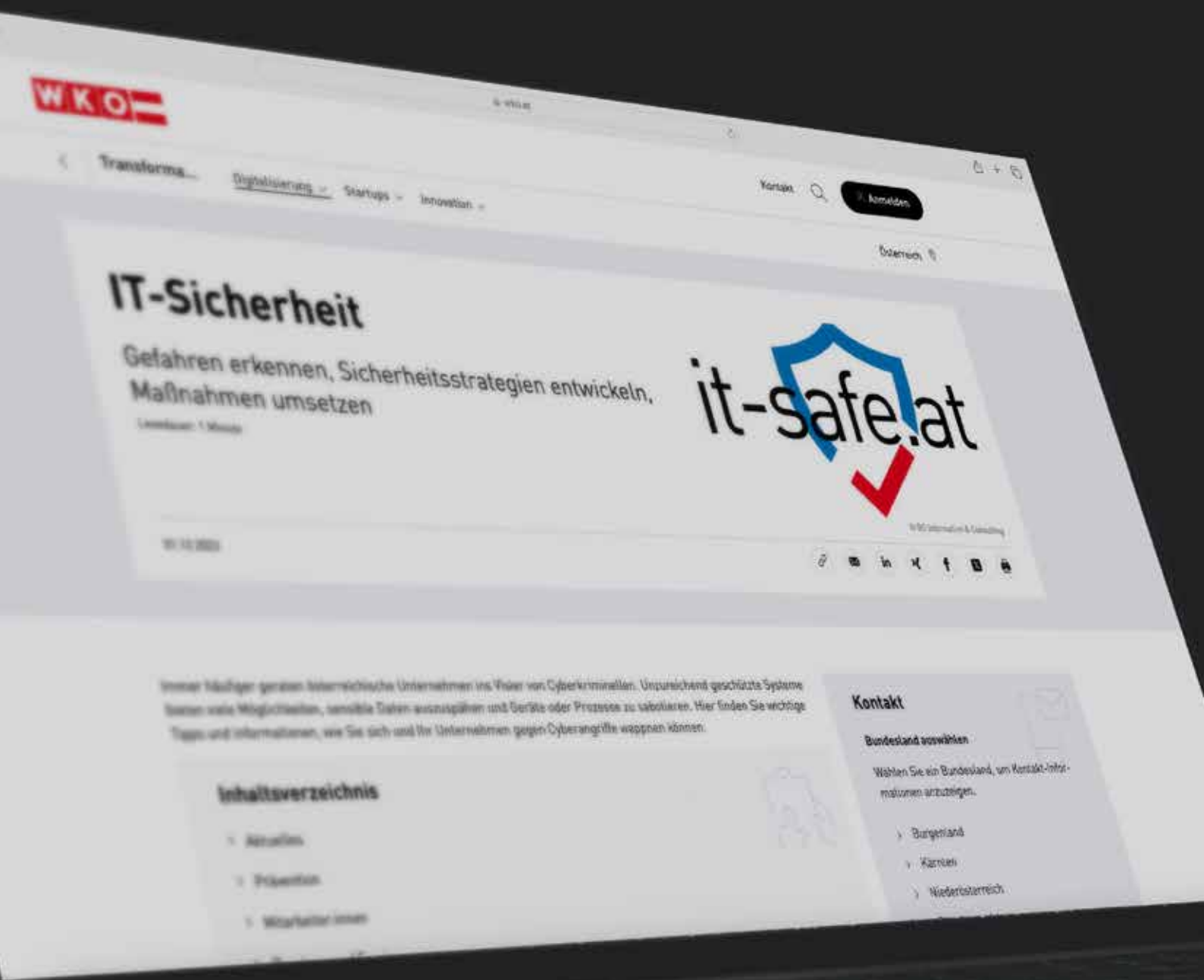


Foto: Unsplash

INTERVIEW:

"Cyberattacken warten nicht bis Oktober 2024."

Verena Becker ist **Cybersicherheitsexpertin** in der Sparte **Information & Consulting der Wirtschaftskammer Österreich** und vertritt darin die Interessen von gut 142.000 wissensbasierten Dienstleistern.
Wir durften Frau Becker zur Entwicklung der Cyberrisiken - und wie die WKÖ ihren Mitgliedern beim erfolgreichen Management dieser Gefahren hilft - sprechen. TEXT: Mag. Verena Becker Msc., Dr. Gerald Hübsch

Sehr geehrter Frau Becker, wie schätzen Sie als ausgewiesene Cybersicherheitsexpertin die Lage der rd. 500.000 österreichischen Unternehmen in Bezug auf Cyber-Bedrohungen ein?

Nun, wenige Bedrohungen sind derart breit gestreut und schwer zu „greifen" wie Cyberrisiken. Diese betreffen jede Sparte und jedes Unternehmen, unabhängig von der Größe: Kein Unternehmen ist zu klein, um nicht Opfer einer Cyberattacke zu werden. Und mittlerweile sind praktisch alle Unternehmen

> **Kein Unternehmen ist zu klein, um nicht Opfer einer Cyberattacke zu werden.**

mehr oder minder von funktionierenden IT-Systemen abhängig, denken Sie nur an die elektronische Planung und Auftragsabwicklung in der Tischlerei oder die IT-gestützte Diagnose von Fahrzeugen in der Kfz-Werkstätte.

Angreifer sind meist einen Schritt voraus, sie wissen sehr gut über die unternehmerische Tätigkeit, Prozesse, IT-Systeme und vor allem auch finanzielle Leistungsfähigkeit ihrer potenziellen Opfer Bescheid und können so gezielt Angriffe vorbereiten, beispielsweise Ransomware-Attacken.

Wie können sich Unternehmen schützen?

Eine hundertprozentige Sicherheit gibt es bekanntlich nicht. Aber mit einem funktionierenden Cyberrisikomanagement und klaren Grundregeln für den IT-Einsatz und alle damit tätigen Personen lässt sich dieses Risiko transparent machen und gezielt beeinflussen.

Sind zahlreiche Unternehmen, speziell KMU, denn nicht mit dieser Thematik ressourcentechnisch überfordert?

Absolut. KMU haben nicht die personellen Möglichkeiten, IT-Security Mitarbeiter:innen zu beschäftigen und ihre Systeme rund um die Uhr zu überwachen, von der wirtschaftlichen Komponente mal ganz abgesehen.

Die Situation erfordert jedoch wirksame Gegenmaßnahmen. Welche Unterstützung bietet die Wirtschaftskammer ihren Mitgliedern?

Das Angebot für unsere Mitglieder ist breit gefächert und soll Unternehmen bei der Bewältigung dieser Herausforderungen gezielt unterstützen.

Auf unserem Portal unter www.it-safe.at finden unsere Mitglieder Hintergrundinformationen, Checklisten, praktische Ratgeber und den direkten Draht zu Expertinnen und Experten in der Region, sei es für ein Beratungsgespräch oder als „Feuerwehr" im Ernstfall. Daneben bieten wir Online-Webinare an und informieren über Veranstaltungen in den Landeskammern und im internationalen Umfeld unserer rund hundert Außenwirtschaftscenter weltweit.

Sollte im Unternehmen ein Sicherheitsvorfall aufgetreten sein, leistet unsere Cyber-Security-Hotline unter 0800 888 133 „Erste Hilfe", nimmt die Eckpunkte strukturiert auf und vernetzt bei Bedarf zeitnah mit Sicherheitsexpertinnen und -experten.

Ein professionelles Informationssicherheits-Risikomanagement leistet wertvolle Dienste.

„Awareness", also die Bewusstseinsbildung in der Unternehmensleitung und bei allen Beschäftigten, gilt als Schlüssel für den erfolgreichen Umgang mit Cyberrisiken.

Wir orten mittlerweile – nicht zuletzt aufgrund der zahlreichen, medial aufgezeigten Vorfälle – breites Interesse und Bereitschaft in den Unternehmen, sich mit dem Thema auseinanderzusetzen. Die Herausforderung liegt aber darin, gerade jene zu erreichen, die den Bedrohungen noch nicht gebührend Augenmerk verleihen.

Wir verstehen dabei aber auch die Lage der Unternehmerinnen und Unternehmer. Sie sind mit unzähligen gesetzlichen Vorschriften und Auflagen aus verschiedensten Bereichen konfrontiert, die per se keinen Mehrerlös generieren, sondern ohnehin knappe Ressourcen zusätzlich binden.

Aber gerade das Thema Cybersecurity ist ein leuchtendes Beispiel dafür, dass es nicht um die Einhaltung von Vorschriften und Vermeidung allfälliger Strafen allein geht, sondern ein echter Mehrwert für die Unternehmen entsteht. Cyberattacken verursachen enorme Schäden, beispielsweise bei Betriebsunterbrechungen, wenn es zu Lieferverzögerungen kommt. Diese kosten viel Geld – und auch Nerven! - und gefährden mitunter sogar die Existenz von Unternehmen. Die Erfüllung gesetzlicher Vorgaben und der Schutz des eigenen Unternehmens gehen hier Hand in Hand. Unternehmen, die im Bereich Cybersecurity noch am Anfang stehen, empfehlen wir als ersten Schritt, eine geförderte individuelle Beratung über die Initiative „KMU Digital" der Wirtschaftskammer Österreich gemeinsam mit dem Bundesministerium für Arbeit und Wirtschaft in Anspruch zu nehmen. Oft gibt es auch zu Umsetzungsmaßnahmen in den Bundesländern attraktive Förderungen.

Welche Erfolgsfaktoren für die wirksame Vorbeugung sehen Sie noch?

Der wichtigste Punkt: Die Chefetage muss hinter dem Informationssicherheitsmanagement stehen. Betriebliches Risikomanagement, was im Unternehmen unbedingt zu schützen ist und wo die erfolgskritischen Prozesse sind, ist Aufgabe der Unternehmensleitung. Sie muss die nötigen Entscheidungen treffen und auch für die personellen und finanziellen Ressourcen sorgen. Überdies bedarf Cybersecurity einer entsprechenden Unternehmenskultur, die Unternehmensleitung hat hier eine wichtige Vorbildfunktion.

Die Chefetage muss hinter dem Informationssicherheitsmanagement stehen.

Welche Rolle spielt NIS2 und die kommende gesetzliche Vorgabe?

Eine sehr wichtige. Wenngleich der Gesetzestext noch nicht im Detail bekannt ist, liegt die zugrunde liegende NIS2-Richtlinie der Europäischen Union bereits vor. Ich empfehle betroffenen Unternehmen dringend, den bis zur Umsetzung bis Oktober 2024 verbleibenden Zeitraum für die Vorbereitung und professionelle Umsetzung eines Informationssicherheitsmanagements gut zu nützen. Die Wirtschaftskammer bietet auch hier umfangreiches Material und Veranstaltungen unter https://wko.at/nis2 an. Wer nicht weiß, ob sein Unternehmen betroffen ist, kann dies mit unserem Online-Ratgeber testen: https://ratgeber.wko.at/nis2/.

In Österreich werden – verglichen mit rd. 100 betroffenen Unternehmen der kritischen Infrastruktur aus NIS1 – nun etwa 2.000 - 4.000 Unternehmen betroffen sein. Dies umfasst auch zahlreiche KMU, zum Beispiel einen Lebensmittelverarbeitungsbetrieb mit mehr als 50 Mitarbeiter:innen oder ein Maschinenbauunternehmen mit mehr als 10 Mio. EUR Jahresumsatz.

Wichtig ist, dass sich die betroffenen Unternehmen rechtzeitig um ein professionelles Informationssicherheitsmanagementsystem kümmern. Das ist auch im eigenen Interesse jedes Unternehmens, denn klar ist, dass Cyberkriminelle jederzeit zuschlagen können. Als Interessenvertretung ist es uns ein wichtiges Anliegen, dass die Umsetzung der Richtlinie einen tatsächlichen Nutzen in Richtung mehr Cybersicherheit bringt und den Unternehmen dabei keine unnötigen Belastungen auferlegt werden.

NIS2 adressiert auch die Sicherheit der Lieferketten und sieht in logischer Konsequenz verpflichtende Lieferanten-Audits rund um Infor-

mationssicherheit vor. Wie sehen Sie in diesem Zusammenhang den Beitrag eines Cyber-Rating-Systems in Österreich bzw. darüber hinaus?

Hintergrund der gesetzlichen Vorgabe der Sicherheit der Lieferkette ist, dass sich Angriffe auf kleine und mittlere Unternehmen mitunter nicht nur auf deren eigene Geschäftstätigkeit auswirken, sondern auch eine Kaskadenwirkung auf die von ihnen belieferten Einrichtungen haben können.

> **NIS2 wird rund 2.000-4.000 Unternehmen in Österreich betreffen, die Lieferketten noch nicht mitgezählt.**

Die Frage ist nun, wie ein von NIS2 betroffenes Unternehmen den Nachweis der Sicherheit seiner Lieferkette erbringen kann. Es ist wichtig, dass keine überbordenden Sicherheitsvorkehrungen verlangt werden, die nur wenige große Unternehmen erfüllen können und dadurch eine Vielzahl kleiner Lieferanten aus dem Markt gedrängt werden. Der Nachweis muss ohne unnötige Bürokratie erfolgen und sich – natürlich in Abhängigkeit davon, welche Dienstleistungen erbracht werden und wie kritisch diese sind - auf die jeweils absolut notwendigen Sicherheitsvorkehrungen beziehen. Das Horrorszenario ist, dass mit NIS2 kleine Lieferanten mit zig unterschiedlichen Fragebögen und Auditvorgaben seitens ihrer Auftraggeber konfrontiert werden.

Die Kommission und die Cybersicherheitsagentur ENISA sprechen sich ausdrücklich für eine Anpassung an internationale Normen und bewährte Verfahren bei der Bewertung der Sicherheit der Lieferkette aus. Selbstverständlich kann aber nicht jedes kleine Unternehmen eine aufwendige ISO 27001-Zertifizierung durchmachen. Niederschwellige Cyber-Ratings stellen hier eine praktikable Lösung dar und sind für den Markt sehr von Vorteil. Es muss jedenfalls jedem Unternehmen überlassen bleiben, welcher Nachweis im jeweiligen Bereich sinnvoll ist.

Sehr geehrte Frau Becker, wir danken für das Gespräch! ■

ZUR INTERVIEWPARTNERIN:

Foto: Privat | Verena Becker

MAG.
VERENA BECKER, BSC

Verena Becker ist **Cybersicherheitsexpertin in der Bundessparte Information & Consulting in der Wirtschaftskammer Österreich**, die rund 142.000 Unternehmen in den Sektoren Information, Kommunikation und Consulting vertritt. Frau Becker ist auch **Vorsitzende von „Women4Cyber Austria"**, einer Initiative, welche die Förderung von Frauen im Bereich Cybersecurity zum Ziel hat.

Cyber Security für KMUs:

- → **Infos, Checklisten, praktische Ratgeber & direkter Draht zu Experten:**
  www.it-safe.at
- → **CyberSecurity Hotline für den Akutfall:**
  0800 888 133

Infos zu NIS2

- → **Material & Veranstaltungen zum Thema:**
  www.wko.at/nis2
- → **Ist mein Unternehmen betroffen?**
  ratgeber.wko.at/nis2

Foto: Unsplash

DORA & NIS:

Drei Fragen mit: Martin Klimbacher

CISO mit Schwerpunkt Finanzwirtschaft

Seit mehr als einem Jahrzehnt entwickelt Martin Klimbacher IT-Sicherheit in Finanzunternehmen weiter. Wir haben mit ihm über die Herausforderung DORA gesprochen.

TEXT: Alexander Mitter, Martin Klimbacher

Welche Herausforderungen stellen sich aktuell und wie beeinflusst NIS2 bzw. DORA Ihre Arbeit?

DORA ist für Banken natürlich die grundlegende Richtlinie, an der sich Strategien und Maßnahmen orientieren. Als CISO muss man dabei eine holistische Sicht auf den gesamten Themenkomplex bewahren, um zielsicher und effektiv Cybersicherheit entsprechend den Erwartungen der Kunden und der regulatorischen Anforderungen zu gewährleisten.

> **„(...) Cybersicherheit muss für die gesamte Lieferkette sichergestellt werden."**

Welche Maßnahmen setzen Sie aktuell um und wie überprüfen Sie Effektivität?

Beispielsweise kann eine Zertifizierung nach ISO27001 für ein Großunternehmen die Basis darstellen. Die eigenen Ansprüche sind aber noch deutlich höher: Dazu prüft man beispielsweise Lieferanten mit dem CyberRisk Rating, um auch über das Unternehmen hinaus klar zu kommunizieren, dass Cybersicherheit für die gesamte Lieferkette sichergestellt werden muss.

Was muss also passieren, damit Cybersicherheit nachhaltig sichergestellt wird?

Zuerst muss das Thema richtig positioniert sein: Die erste Voraussetzung ist die Unterstützung der Geschäftsführung, damit wir unabhängig und bevollmächtigt die richtigen Maßnahmen setzen können. Das ermöglicht uns, durchgängige Steuerungsmechanismen im eigenen Haus, aber auch für externe Stakeholder zu implementieren. Letztendlich ist Cybersicherheit dann nachhaltig sichergestellt, wenn vom Hersteller bis zum Endkunden alle Beteiligten Wissen aufbauen und damit koordiniert und aufeinander abgestimmt zusammenarbeiten. Diesen langfristigen Prozess gilt es zu unterstützen um die Digitalisierung langfristig abzusichern. ■

Foto: Privat | Martin Klimbacher

MARTIN KLIMBACHER

Martin Klimbacher ist mit über einem Jahrzehnt Erfahrung in **namhaften österreichischen Finanzunternehmen ein führender Experte im Bereich IT-Sicherheit**. Seine langjährige Führungserfahrung umfasst die Leitung von Gruppen und Abteilungen sowie die Beratung in der Raiffeisenbankengruppe im Bereich Business Continuity Management. Seine Expertise erstreckt sich über die Implementierung und den Betrieb von ISMS, Information Security & Resilience Management, Cyber & IT-Risikomanagement sowie Information Security Governance & Auditmanagement.

Foto: Freepik

25. PWC GLOBAL SURVEY:

Cybersecurity in der Supply Chain

Cybersecurity und Cybercrime sind aktuelle Themen, welche die heimische Wirtschaft beschäftigen und fordern. Im 25. PwC Global CEO Survey sehen österreichische CEOs Cyberrisiken als deren größte Sorge. Die Ausnutzung von Schwachstellen in der IT oder Ransomware-Angriffe sind nur zwei aktuelle Cybercrime Beispiele.

TEXT: Georg Beham, MSc.

Cyberrisiken resultieren aus verschiedenen Faktoren, wie beispielsweise Schwachstellen in der IT-Landschaft und nicht ausreichender Sensibilisierung der Mitarbeiter. Häufig noch kaum betrachtet sind Cyberrisiken in der Supply Chain. Gerade in Zeiten der zunehmenden Digitalisierung und Vernetzung nimmt die Abhängigkeit unserer digitalen Prozesse von jenen unserer Lieferanten und Kunden zu. Ausfälle einzelner kritischer Systeme in der Supply Chain können signifikante Folgen für den gesamten Betrieb des eigenen Unternehmens bedeuten. Gleichzeitig öffnet die zunehmende Vernetzung Eintrittsmöglichkeiten in die IT von Unternehmen, die, bei nicht ausreichenden Schutzmaßnahmen Ihrer Partner, von Cyberkriminellen als Tor in ihr Unternehmen genutzt werden können.

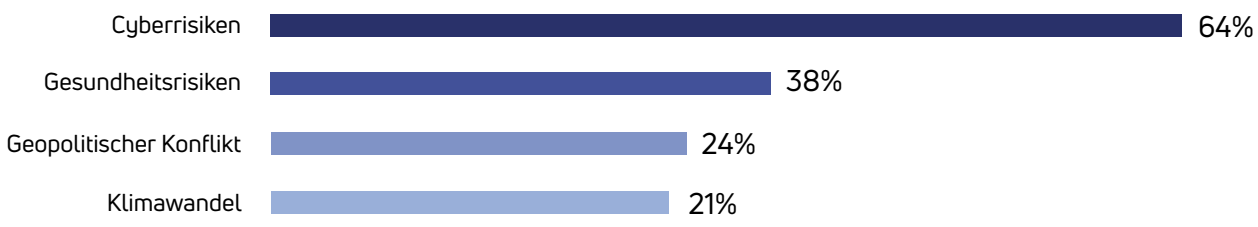
Beschäftigen Sie diese Fragen? Das Unternehmen verfügt über einen hohen Schutzlevel? Es werden IT-Produkte verschiedener Hersteller eingesetzt? Werden diese Produkte von Dienstleistern gewartet? Wer stellt ausreichende Schutzmaßnahmen dieser Dienstleister sicher?

Wir sehen die laufende Überprüfung der Informationssicherheitsmaßnahmen Ihrer vernetzten Partner als eine wesentliche Maßnahme zum Schutz Ihres Unternehmens. Dabei gilt es angemessene Prüfungsmaßnahmen anzusetzen, um Aufwand und Kritikalität der Lieferanten in Relation zu halten. Diese Maßnahmen reichen von der Einholung nachweisbarer Zertifizierungen über die Validierung der Sicherheitsvorkehrungen bis zur Durchführung gezielter schwerpunktbezogener Audits und Security Tests.

Wir bei PwC unterstützen unsere Kunden mit unserem PwC Supplier Risk Assessment powered by KSV1870 in der Kategorisierung der Lieferanten, der Definition angemessener Kontrolltätigkeiten sowie der Durchführung dieser mit entsprechenden Audits, Security Tests sowie dem KSV1870 CyberRisk Rating. ■

25. PwC Global CEO Survey - Auszug:

Folgend die Kernergebnisse der 25. Global CEO Survey von PwC, bei der 4.446 CEOs in 89 Ländern – darunter 42 Entscheidungsträger:innen aus Österreich – zwischen Oktober und November 2021 befragt wurden.



Quelle: PwC, 25. Global CEO Survey (2022), Ergebnisse für Österreich

RATING & VERSICHERUNG:

Wie kann ich mein Unternehmen vor Cyberbedrohungen schützen?

Die Geschwindigkeit der Digitalisierung in einer durch das Internet verbundenen Welt bringt große Chancen für Unternehmen. Die damit entstehenden Risiken müssen jedoch technisch und finanziell abgedeckt werden. **TEXT:** Dr. Wolfgang Petschko

Schon das fünfte Jahr in Folge werden Cyberrisiken für Unternehmen in einschlägigen Befragungen unter die Top 3 Risiken gereiht. Das Thema der Auseinandersetzung mit diesen Risiken kann von sorgfältigen Geschäftsführern nicht mehr ignoriert oder verniedlicht werden.

In den letzten Jahren hat sich in Österreich auch eine umfassende Community auf der Anbieterseite etabliert, die den in den Unternehmen verantwortlichen CISO's und CIO's ein breites Angebot an Vorgehensweisen, Tools und Services anbietet.
Aber wo anfangen und wo aufhören? Und wie viel ist genug? Diese Aufgabenstellung verbleibt bei den Verantwortlichen im Unternehmen, verbunden mit einer entsprechenden, individuellen Abschätzung der Risikolage.

Wie viel Produktionsausfall kann ich mir leisten, wie lange ist es tragbar für mein Unternehmen, meine Dienstleistung nicht erbringen zu können? Welche Verpflichtungen bin ich Dritten gegenüber eingegangen? Oft geht es bei den zu treffenden Einschätzungen auch um das wirtschaftliche Überleben eines Unternehmens.

Einschlägige Zertifizierungen wie etwa ISO 27001 helfen, die entsprechenden Mindeststandards im Unternehmen zu etablieren, sind jedoch aufwendig und oft aufgrund der Kundenstruktur des Unternehmens nicht die richtige Wahl. Hier hilft die unabhängige Einschätzung der Cyber-Bedrohungslage mit Ratings durch Spezialisten das richtige Maß geeigneter Sicherheitsmechanismen zu finden.
Eine klare Klassifizierung hilft nicht nur dem CIO bei der Argumentation, welche Maßnahmen umzusetzen sind, sondern vor Allem auch Geschäftspartnern und Kunden, eine profunde und transparente Aussage zum Thema der Informationssicherheit eines Unternehmens zu erlangen.

Versicherungen unterstützt dieses Rating bei der Einschätzung des Risikos für den Abschluss einer Cyberversicherung, die zur Abdeckung des Vermögensschadens (auch eines Betriebsunterbrechungsschadens) hilft, der einem Unternehmen nach einem Cyberangriff entsteht. Darüber hinaus bietet eine Cyberversicherung Soforthilfe durch Spezialisten bei der Abwehr eines möglichen Cyber-Angriffs und Aufräumarbeiten danach. Durch den Mix aus geeigneten Maßnahmen im Unternehmen, unabhängige Einschätzung durch ein Rating und die Abdeckung des verbleibenden Risikos durch eine Cyberversicherung sind Österreichs Unternehmen bestens gewappnet für die Herausforderungen des Geschäftslebens. ■

Foto: Ian Ehm | Wolfgang Petschko

DR.
WOLFGANG PETSCHKO

Dr. Wolfgang Petschko ist **Vorstandsmitglied** bei der DONAU Versicherung AG – Vienna Insurance Group.

Warum eine **Cyberversicherung?**

- Abdeckung des Vermögensschadens
- Abdeckung eines Betriebsunterbrechungsschadens
- Soforthilfe durch Spezialisten bei der Abwehr eines möglichen Cyber-Angriffs und den Aufräumarbeiten danach

Foto: Freepik

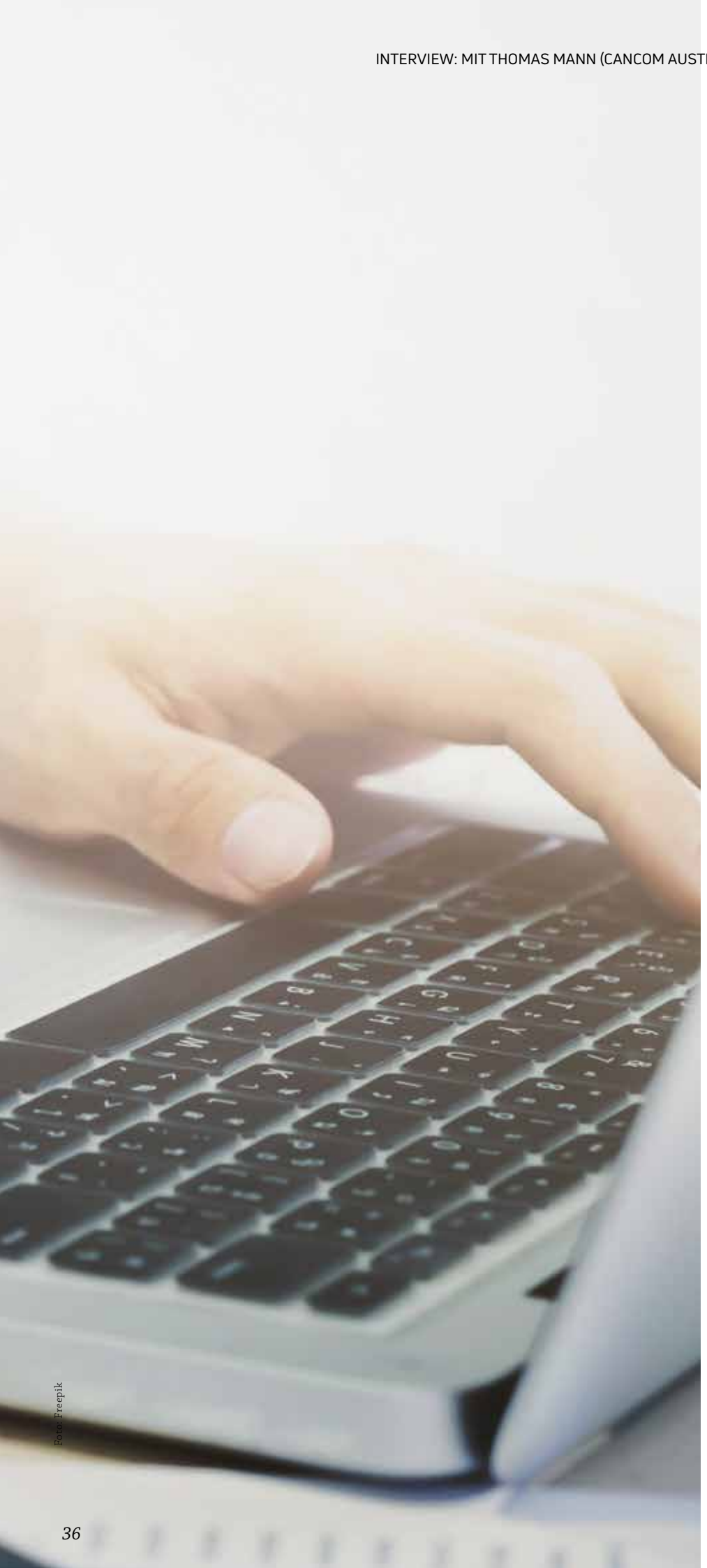


Foto: Freepik

INTERVIEW:

„Cyberbedrohu Unternehmen b führenden Ges

Wir sprachen mit **Thomas Mann, CISO u** heit aus Sicht eines führenden österreic

TEXT: Dr. Gerald Hübsch, Thomas Mann

Sehr geehrter Herr Mann, wie würden Sie das Leistungsportfolio Ihres Unternehmens kurz beschreiben?

CANCOM Austria AG erbringt für ihre Kunden in Österreich und der DACH-Region umfassende IT-Dienstleistungen, von der IT-Strategieentwicklung und technologischen Planung bis hin zum 7x24-Betrieb. Zunehmend an Bedeutung gewinnt darüber hinaus das Gebiet der Cybersicherheit. CANCOM deckt auch hier den gesamten Lebenszyklus ab, sei es Strategieplanung, Risikoanalyse, Audits bis hin zum „Red Teaming", Errichtung und Betrieb von Sicherheitslösungen. Ein Erfolgsmodell ist dabei zweifellos unser Cyber-DefenseCenter.

Welche Entwicklungen rund um Cybersicherheit sehen Sie in der heimischen Wirtschaft?

Cyberbedrohungen werden von vielen Unternehmen bereits als eines der 3 führenden Geschäftsrisiken eingestuft. Die Entwicklung geeigneter Strategien rückt daher immer stärker in den Mittelpunkt. Zuvor eher technisch ausgerichtete IT-Sicherheitskonzepte weichen einer umfassenden,

ungen werden von vielen bereits als eines der drei chäftsrisiken eingestuft."

und Chief BCM Officer der CANCOM Austria AG, über Cybersicher-chischen IT-Dienstleisters auf diesem Gebiet.

geschäftsorientierten Informationssicherheitsstrategie. Die Sicherheit von OT-Systemen (Operational Technology, also Automatisierungs- und Leittechnik, *Anm.*) erhält einen immer größeren Stellenwert, um Produktions- und Betriebsausfällen vorzubeugen. Zahlreiche Unternehmen verfügen jedoch nicht über die erforderliche Personalausstattung, um den gesamten Sicherheitszyklus und -betrieb intern abzudecken. „Security as a Service" wird zur unverzichtbaren Unterstützung, um die Herausforderungen meistern zu können.

> **Die Sicherheit von Automatisierungs- und Leittechniksystemen erhält einen immer größeren Stellenwert, um Produktions- und Betriebsausfällen vorzubeugen.**

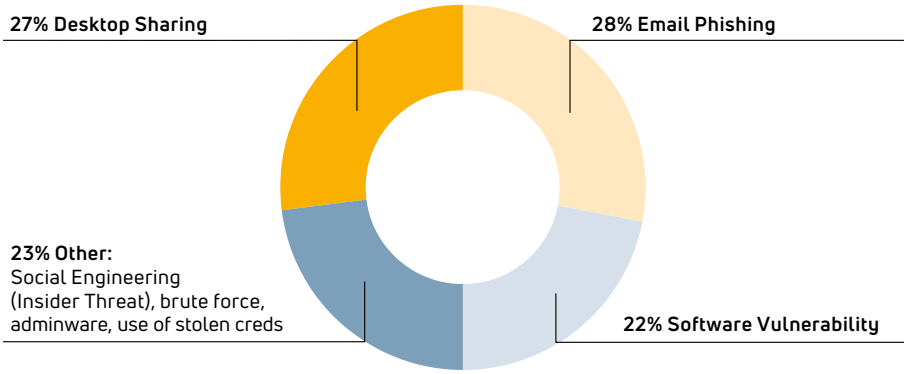
Damit schließt sich für CANCOM der Kreis?

Exakt. Unsere Kunden profitieren vom Komplettangebot seitens CANCOM. Wir leben quasi Informationssicherheit und teilen unser Know-How und unsere Praxiserfahrungen gerne mit unseren Kunden, sei es die Bereitstellung und der Betrieb von Sicherheitslösungen oder die Entwicklung geeigneter Sicherheitsstrategien. Immer häufiger fragen speziell Industriebetriebe auch die Erbringung der CISO-Funktion als „Trusted Advice & Service" bei uns an – ein Zeichen besonderen Vertrauens und Verantwortungsbewusstseins.

Wie stellen Sie hohe Sicherheitsstandards im eigenen Unternehmen sicher?

Mehrschichtig. Dazu zählt eine ausgeprägte Awareness des gesamten Teams ebenso wie strikte Security Policies und leistungsfähige Sicherheitslösungen. Einen besonderen Stellenwert nehmen in diesem Zusammenhang Zertifizierungen und Ratings ein, beispielsweise nach ISO 27001 und das

Schwachstellenübersicht / Einfallstore 2022



www.coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting#vectors
www.verizon.com/business/resources/T651/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

CyberRisk Rating des KSV1870, welche nicht nur zur Einhaltung des NIS-Gesetzes immer häufiger von Kunden und Geschäftspartnern bei uns nachgefragt werden.

> **Gesetze und Normen fokussieren zunehmend auf "Supply Chain Security", also die Sicherstellung einer auch in Cyber-Fragen funktionierenden Lieferkette.**

Wo sehen Sie die Stärken und Vorteile des CyberRisk Ratings des KSV1870?

Nun, das zugehörige Schema (das ist der rund 25 Themen umfassende CyberRisk Rating-Fragenkatalog, *Anm.*) deckt wesentliche Bereiche eines zeitgemäßen Informationssicherheits-Managementsystems ab und gibt Auskunft über die zu erwartende Resilienz gegenüber Cyberbedrohungen im Unternehmen. Gesetze und Normen fokussieren zunehmend auf „Supply Chain Security", also die Sicherstellung einer auch in Cyber-Fragen funktionierenden Lieferkette. Würden die geforderten wechselseitigen Gespräche bzw. Audits nicht orchestriert erfolgen, hätten wir mittelfristig einen immensen Aufwand und Wildwuchs an unterschiedlichsten Zugängen und Evaluierungsfragen. Dies würde die Kosten ins Unermessliche treiben und die Qualität und Aussagekraft der Lieferantenüberprüfungen schmälern. Dank des österreichischen CyberRisk Ratings können wir den sonst exponentiellen Aufwand hin zu einer linearen Entwicklung drastisch reduzieren und gleichzeitig einheitliche Qualitätsstandards sicherstellen. Dies ist einer der Gründe, weshalb wir frühzeitig dieses Rating erfolgreich absolviert haben und nun unseren Geschäftspartnern zur Verfügung stellen. Wir runden unser Rating künftig auch durch ein Label als sichtbares Zeichen dieses Qualitätsanspruches ab.

Welche Anregung möchten Sie dem CyberRisk Advisory Board für die Weiterentwicklung dieses Ratings geben?

Als Betreiber eines CyberDefenseCenters und mehrerer Hochsicherheits-Rechenzentren sind wir natürlich in weiten Bereichen nach internationalen Sicherheitsnormen zertifiziert, beispielsweise die genannte ISO 27001. Dies sollte auch in das CyberRisk Rating gebührend einfließen und kann so den erforderlichen Zeitaufwand für uns weiter reduzieren.

Abschließend tätigen wir noch einen Ausblick. Wo sehen Sie weitere künftige Herausforderungen in der Cybersicherheit?

Wir kämpfen auch im Bereich Cybersecurity mit dem viel zitierten Fachkräftemangel. Das Angebot an CISOs kann mit dem Bedarf kaum Schritt halten. Dies liegt auch daran, dass eine CISO-Funktion nicht einfach „kopier- und skalierbar" ist, jedes Unternehmen benötigt eine individuelle Risikoanalyse und Informationssicherheitsstrategie. Eine weitere Herausforderung liegt in der Einfachheit und Akzeptanz von Sicherheitslösungen durch die Anwender. Wir erproben hier Konzepte und Dienste, welche die ungeliebten Passwörter ersetzen können, beispielsweise durch biometrische Verfahren und die Vernetzung von Geräten und Sicherheitsfunktionen. Unser Ziel ist es, sowohl den Komfort – und damit auch die Benutzerakzeptanz – als auch die Sicherheit Hand in Hand zu steigern.

Besonderen Fokus richten wir auch auf die sogenannte Endpoint Security auf mobilen wie auch stationären Endgeräten, denn im Zuge der Cloud-Transformation kommunizieren viele dieser Clients vorrangig mit den in der Cloud angebotenen Anwendungen und nicht mehr ausschließlich

Foto: Freepik

mit jenen im eigenen Rechenzentrum gehosteten. Eine altbekannte Risikoquelle stellt bekanntlich der Einsatz nicht gepatchter, also nicht auf dem letzten Software- und Sicherheitsstand befindlicher Systeme dar. Auch Threat Intelligence und die Verknüpfung unterschiedlichster Sicherheitsforen kann uns zusätzlich vor Angriffen schützen bzw. zumindest warnen. Künstliche Intelligenz für die Überwachung und Erkennung von Anomalien und möglichen Sicherheitsattacken gewinnt zunehmend an Bedeutung und kann verdächtige Abweichungen aus immensen Datenmengen nahezu in Echtzeit erkennen.

Eine altbekannte Risikoquelle stellt bekanntlich der Einsatz nicht gepatchter, also nicht auf dem letzten Software- und Sicherheitsstand befindlicher Systeme dar.

Die Komplexität des IT-Einsatzes stellt in Summe eine große Herausforderung dar – und steigt stetig weiter. Speziell Cloud-Dienste können einfach durch Fachbereiche bestellt und aktiviert werden, mit entsprechenden Schnittstellen ergeben sich oft neue, unsichtbare Risiken. Ein professionelles Informationssicherheitsmanagement und ein weitblickendes Enterprise Architecture Management sind deshalb unerlässlich.

Und schließlich kann die Vernetzung unserer Sicherheitseinrichtungen – über Unternehmensgrenzen hinweg – frühzeitig wertvolle Informationen und Maßnahmen bereitstellen, allen voran die Computer Emergency Response Teams (CERT) und Mitwirkung in der Security Community.

Sehr geehrter Herr Mann, wir danken für das Gespräch! ■

ZUM INTERVIEWPARTNER:

THOMAS MANN

Thomas Mann ist als **Informationssicherheitsexperte** seit 2009 für **CANCOM Austria AG** (bisher bekannt als K-Businesscom) tätig und bekleidet seit 2015 die Funktion des CISOs und des Chief BCM Officers in der Gruppe. Herr Mann ist darüber hinaus Auditor für ISO27001 und EN50600 Zertifizierungen und berät zahlreiche Unternehmen in der DACH-Region rund um Cybersicherheitsstrategien.

NIS2 NACHWEIS:

Der CyberRisk Manager: Kostenlos für KSV1870-Mitglieder, die das Cyber-Risk Rating akzeptieren*

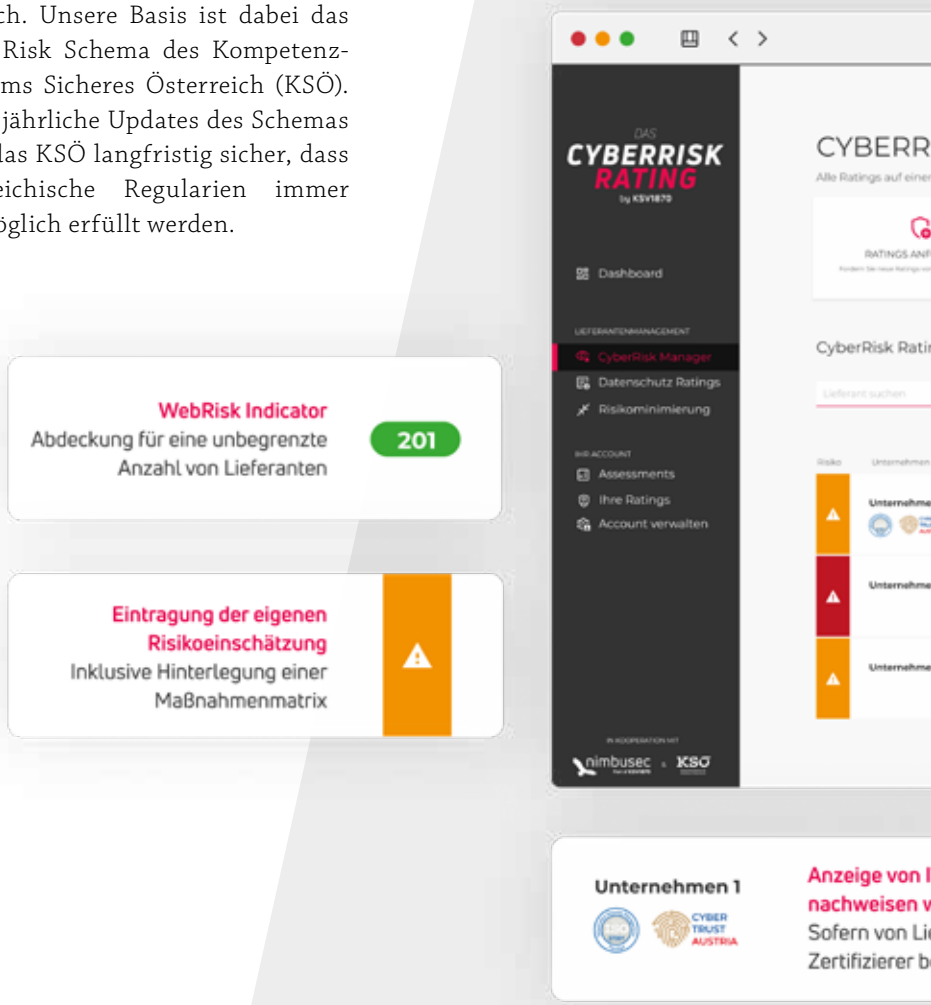
Der CyberRisk Manager ermöglicht KSV1870 Mitgliedern durch die Führung des Lieferantenverzeichnisses die Grundlage für Ihr Lieferantenmanagement nach NIS2 zu legen. TEXT: Alexander Mitter

Seit 2020 bewertet das CyberRisk Rating by KSV1870 Cyberrisiken von Dienstleistern, Lieferanten und Dritten.

Die Basis für jedes CyberRisk Rating stellt ein Dialog zwischen dem bewerteten Unternehmen und Analysten dar. Wir sind aufgrund unserer Praxiserfahrung überzeugt und wurden auch durch die österreichischen Aufsichtsbehörden darin bestätigt, dass nur durch einen direkten Austausch mit dem Lieferanten Cyberrisiken korrekt bewertet und langfristig gesenkt werden können. Pro Rating nehmen wir uns durchschnittlich einen Personentag Zeit, um zu informieren, aufzuklären und nachzufragen.

Zusätzlich nutzen wir modernste Technologien und Ihre eigene Risikoeinschätzung, um die richtigen Teile Ihrer Lieferkette zu bewerten. Dadurch erreichen wir eine Vollabdeckung all Ihrer Lieferanten, setzen aber wertvolle Ressourcen nur dort ein, wo es Sinn macht.

Selbstverständlich bewerten wir Unternehmen weltweit auf Deutsch und Englisch. Unsere Basis ist dabei das Cyber Risk Schema des Kompetenzzentrums Sicheres Österreich (KSÖ). Durch jährliche Updates des Schemas stellt das KSÖ langfristig sicher, dass österreichische Regularien immer bestmöglich erfüllt werden.

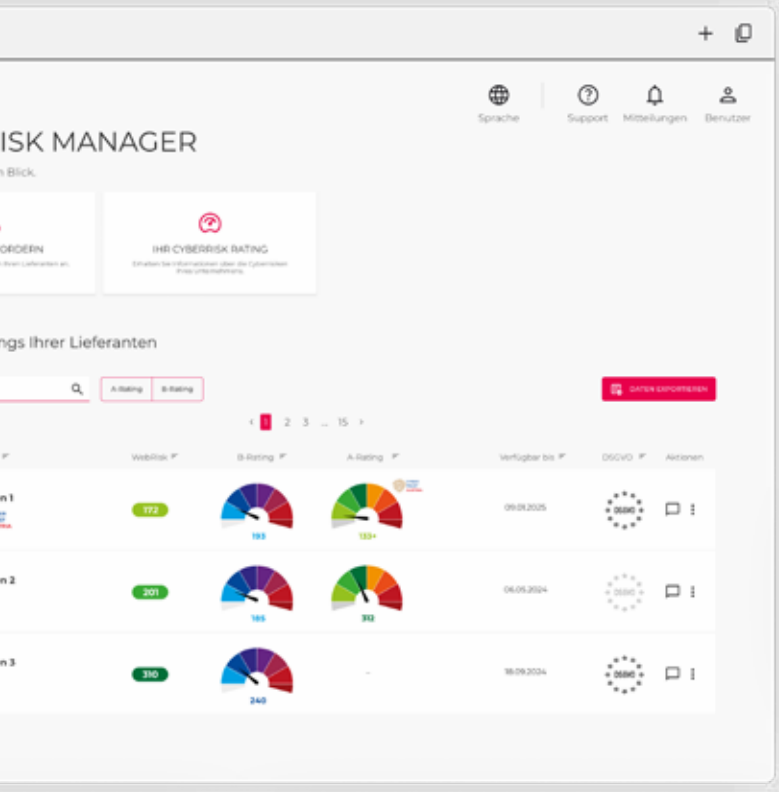


*480€ Jahresgebühr exkl. MwSt. wird rückerstattet bzw. erlassen, wenn in öffentlich einsehbaren Einkaufsbedingungen das CyberRisk Rating by KSV1870 bzw. das Cyber Trust Gütesiegel als Sicherheitsnachweis für Lieferanten akzeptiert wird.

AUF EINEN BLICK:

Vorteile & Nutzen

- Alle **bereits hinterlegten Cybersicherheits-nachweise** aller Lieferanten **sofort einsehbar**.
- Interne **Risikobewertung NIS-konform** für alle Lieferanten hinterlegen.
- **WebRisk Indicator für alle Lieferanten** als objektive Zusatzinformation **sofort verfügbar**.
- **Maßnahmen** entsprechend der Risikoklasse **hinterlegen**.
- **Automatisch Aufgaben** zur **Cyberrisiko-minimierung** erstellen.
- Lieferanten zum **Hinterlegen** von **Cybersicher-heitsnachweisen auffordern**.
- **Unbegrenzte User für Fachabteilungen** und Prozesse über **API automatisieren**.
- Schnell und effizient **CyberRisk Ratings beauftragen**.



Zusätzlich zur Basisversion bieten wir folgende Services an:

- Erstellung von Einzelratings für beliebige Lieferanten weltweit
- Direkte Kontaktierung der Cyber-Security verantwortlichen Person bei Ihrem Lieferanten

AB 40 CYBERRISK RATINGS JÄHRLICH:

- API-Integration
- Quartalsweises Review
- Individuelle Fragen/Module

DSGVO

DSGVO-Modul
Klärt Basisanforderungen der DSGVO bereits vorab

T-Sicherheits-
vie z. B. ISO27001
eferant oder
ereits hinterlegt

Anzeige von Cyber Trust® Austria Gütesiegeln
Inklusive vollem CyberRisk Rating

DAS CYBERRISK RATING by KSV1870

Kontaktinformationen

KSV1870 Nimbusec GmbH
Kaisergasse 16b, 4020 Linz
+43 (0) 732 860 626
support@cyberrisk-rating.at

www.cyberrisk-rating.at

nimbusec
Part of KSV1870