KSV1870

CyberRisk Report

DER JÄHRLICHE REPORT ZUM ÖSTERREICHISCHEN CYBERRISK RATING

AUSGABE 2022

IT-Security
Die Security-Landschaft von Österreichs kritischer Infrastruktur im Überblick.

Datenschutz
Im Gespräch mit OMV Datenschützer Manfred Spanner.

IMPRESSUM: Medieninhaber: KSV1870 Nimbusec GmbH, 4020 Linz, Fadingerstraße 15;
www.nimbusec.com/www.cyberrisk-rating.at
Herausgeber: Alexander Mitter; Verlagsort: Linz; Chefredaktion: Elisabeth Hentscholek; Autoren dieser Ausgabe: Alexander Janda, Alexander Mitter, Alen Kocaj, Elisabeth Hentscholek, Gerald Hübsch, Thomas Stubbings, Walter Fraißler; Layout: Elisabeth Hentscholek; Lektorat: Johannes Payer

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

Wir leben und arbeiten in einer Welt, die uns dank immer effizienterer Technologie den höchsten Lebensstandard der Menschheitsgeschichte ermöglicht.
Egal, in welche Richtung man blickt: Informationstechnologie ist allgegenwärtig. Satellitennavigation leitet unsere Verkehrsströme auf den Straßen, am Wasser und in der Luft. EDV-Systeme stellen unsere Röntgenbilder und Krankheitsgeschichten Ärzten in Originalqualität zur Verfügung. Unsere Unternehmen versenden Rechnungen digital, und der Handel findet sogar für lokale Güter immer öfter im Cyberspace statt. Smart Meter optimieren unsere Stromnetze, und Bankgeschäfte tätigen die meisten von uns direkt auf ihrem Mobiltelefon. Wer hätte sich das vor nicht einmal einer Generation vorstellen können?

Doch überall, wo Licht ist, ist auch Schatten: Unsere Digitalisierung baut auf Technologie auf, in der im Stundenrhythmus neue Sicherheitslücken gefunden werden. Selbst ohne aktive Angreifer ist die zuverlässige Funktion unserer Computer eine große Herausforderung. Seit aber zusätzlich Kriminelle und staatliche Akteure gleichermaßen verstanden haben, dass wir unsere wertvollsten Daten und Prozesse dieser Technologie anvertrauen, werden Sicherheitsprobleme systematisch und im großen Stil ausgenützt.

Wie soll eine IT-Abteilung all diese Technologien zu jedem Zeitpunkt, auf jedem Gerät und an jedem Unternehmensstandort perfekt warten, absichern und überwachen? Und – wenn diese Herausforderung für unsere größten Unternehmen bereits riesig ist – wie sollen Österreichs Klein- und Mittelunternehmen sie bewältigen?

Diese Fragen bewegten nicht nur die EU-Kommission, als sie die NIS-Richtlinie[1] verabschiedete, und unsere Ministerien, als sie diese Richtlinie für Österreich umsetzten[2], sondern auch die Cybersicherheitsexperten des Kompetenzzentrum Sicheres Österreich (KSÖ)[3], die seit Mitte 2020 den ersten österreichischen Standard zur Erstellung eines CyberRisk Ratings[4] geschaffen haben. Als KSV1870 nutzen wir diesen Standard, um Unternehmen weltweit einheitlich, effizient und fair zu bewerten. Wie es dazu kam, welche Ziele wir damit verfolgen und welche Erkenntnisse wir dadurch gewinnen konnten, möchten wir Ihnen auf den folgenden Seiten berichten.

Eines kann ich Ihnen aber bereits vorab verraten: Cybersicherheit wird einer der wesentlichsten Faktoren für die weitere Digitalisierung unserer Welt sein. Kein Staat, kein Unternehmen, kein einziger Mensch wird sich diesem Thema entziehen können. Die Chancen moderner Technologie sind aber zu groß, als dass wir uns durch Hacker entmutigen lassen sollten. Also: Bleiben wir mutig und innovativ! Die neuen Herausforderungen können wir gemeinsam meistern.

Ich wünsche Ihnen viel Lesevergnügen.

Ihr Alexander Mitter
Geschäftsführer der KSV1870 Nimbusec GmbH

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016L1148&from=DE
[2] https://www.nis.gv.at/
[3] https://kompetenzzentrum-sicheres-oesterreich.at/
[4] https://cyberrisk-rating.at/cyberrisk-schema-de.pdf

Inhalt

Foto: OMV AG | OMV Zentrale Wien

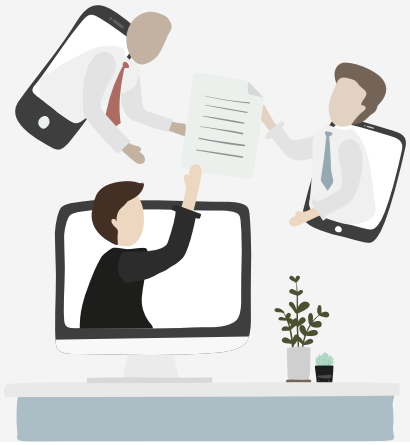

Foto: Freepik

Foto: VERBUND

Foto: Freepik

Foto: Adobe Stock

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:** Elisabeth Hentscholek

28%

MALWARE BLEIBT MINDESTENS 2 MONATE ONLINE

28% der infizierten Domains verteilten zwei Monate nach Entdeckung der Malware weiterhin Schadsoftware an Webseitenbesucher.

17%

INNERHALB EINES MONATS ERNEUT GEHACKT

Von den mit Schadsoftware infizierten Webseiten wurden 17% nach dem Bereinigen nur unzureichend abgesichert und innerhalb eines Monats erneut infiziert.

88%

WORDPRESS ALS MALWARE-EINFALLSTOR

Wordpress ist nicht nur das am weitesten verbreitete Content Management System, sondern auch in 88% der Malware-Fälle das Einfallstor. Gründe dafür sind fehlende Patches, Lücken in Templates und insbesondere Plug-Ins. Diese technischen Probleme werden aufgrund fehlender organisatorischer Prozesse und Verantwortlichkeiten lange nicht gelöst. Wer also nicht schnell patcht, wird gehackt.

Foto: Freepik

CyberRisk Rating: Zahlen, Daten Fakten

DATENANALYSE: Alen Kocaj | **TEXT:** Elisabeth Hentscholek

20%

der Lieferanten haben sich bei der Beantwortung des Assessments im Durchschnitt überschätzt. Bei den Fragen B13, A5 und A10 trat Selbstüberschätzung am häufigsten auf.

35%

der Lieferanten haben sich bei der Auswahl ihres CyberRisk Ratings gegen das vom Auftraggeber geforderte Rating entschieden.

58%

In 58 % der Fälle musste der Verifizierer dem Lieferanten nach Ausfüllen des Assessments eine Nachfrage senden, da die gegebene Antwort nicht schlüssig oder detailliert genug war.

13%

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

41%

der Unternehmen können den Anspruch an ein fortgeschrittenes Sicherheitslevel (A-Rating) nur mäßig erfüllen.

3 von 10

Lieferanten sind nicht in der Lage, IT-Sicherheitsvorfälle in ihrem Unternehmen durch Protokollierung ihrer Systeme zuverlässig zu erkennen.

Warum wir ein CyberRisk Rating brauchen

Als KSV1870 stellen wir mit dem CyberRisk Rating ein Werkzeug zur Verfügung, mit dem wir unsere Geschäftspartner nicht nur bewerten, sondern implizit auch beraten können.

Seit mehr als 150 Jahren schützt der Kreditschutzverband von 1870 (KSV1870) die Interessen seiner Mitglieder durch das Erheben von Bonitätsinformationen.

Zur Zeit der Gründung des KSV1870 waren es Kreditbetrüger, die den Wirtschaftstreibenden ihr Leben schwer machten, und schon im 19. Jahrhundert erkannte die österreichische Wirtschaft, dass nur durch Zusammenarbeit quer über Unternehmensgrenzen hinweg eine Lösung möglich war – genauso wie heute. TEXT: Alexander Mitter

Die Technologie hat sich dramatisch weiterentwickelt, aber grundsätzlich sind unsere Mitglieder heute wie damals ähnlichen Bedrohungen ausgeliefert: Lücken in Systemen aller Art werden von Kriminellen ausgenützt, um sich illegal Vorteile zu verschaffen. Egal, ob Informationen entwendet, Geld erpresst oder Identitäten gestohlen werden: Am Ende müssen wir uns gegen die Bedrohungen unserer Zeit wehren.

Die Mitglieder des KSV1870 bilden einen Querschnitt der österreichischen Volkswirtschaft. Wir konnten in den letzten Jahren beobachten, wie das Risiko eines Cybersicherheitsvorfalls für KMUs genauso wie für Unternehmen der kritischen Infrastruktur immer weiter stieg. Mittlerweile lesen wir fast täglich von Fällen, in denen finanziell gesunde Firmen ihre Produktion stoppen müssen, weil Hacker ihre Daten verschlüsselt haben. Sogar staatliche Akteure nutzen den Cyberspace, um Wissen zu stehlen und Devisen zu beschaffen. 2020 beschuldigte eine Jury in den USA sechs Offiziere einer russischen Militäreinheit namentlich, da sie es als erwiesen ansah, dass diese für tausende Angriffe auf internationale Unternehmen, politische Kampagnen, Regierungen und sogar die Olympischen Spiele verantwortlich waren. Die Details und der Umfang der Anklageschrift geben einen seltenen Einblick in den Grad der Organisation heutiger Hacker.

Im Lichte des Krieges zwischen Russland und der Ukraine müssen wir uns darauf vorbereiten, dass diese Bedrohungen weiter zunehmen.

Als KSV1870 stellen wir mit dem CyberRisk Rating ein Werkzeug zur Verfügung, mit dem wir unsere Geschäftspartner nicht nur bewerten, sondern implizit auch beraten können. Jede der 25 Anforderungen des KSÖ Cyber Risk-Schemas ist ein Schritt in die richtige Richtung. Es ist jetzt an der Zeit, Sicherheitsrichtlinien für unsere IT zu erstellen, Mitarbeiter zu schulen, Backups zu testen und Notfallpläne zu definieren. Kein Unternehmen kann sich der Digitalisierung verschließen, und die Absicherung unserer EDV ist dafür schlicht notwendig.

Wir können diese Herausforderung – genau wie schon im Jahr 1870 – nicht allein lösen: Mit dem CyberRisk Rating des KSV1870 haben wir ein praxisorientiertes Werkzeug geschaffen, das auf dem gemeinsamen Wissen der erfahrensten IT-Sicherheits- und Datenschutzexperten unseres Landes aufbaut.

> **Mittlerweile lesen wir fast täglich von Fällen, in denen finanziell gesunde Firmen ihre Produktion stoppen müssen, weil Hacker ihre Daten verschlüsselt haben.**

Probieren Sie es gerne selbst: Unsere Mitarbeiter bei KSV1870 Nimbusec freuen sich darauf, Ihnen zu zeigen, wie Sie Ihr Unternehmen auf die Cybersicherheitsherausforderungen unserer Zeit am besten vorbereiten. Selbst KMUs können so ein ausgezeichnetes CyberRisk Rating erreichen – mit den richtigen Maßnahmen sogar ohne zusätzliche Kosten. ■

Das Cyber Risk Advisory Board

Welche Rolle hat das Advisory Board im österreichischen CyberRisk Rating inne, und was macht die Mitwirkung für die Experten aus der Praxis so spannend? Gerald Hübsch sprach mit den Vertretern der involvierten Branchen und öffentlichen Stellen über ihre Arbeit in diesem Gremium: TEXT: Gerald Hübsch

Von der tragenden Gründungsidee im Jahr 2019 für ein „CyberRisk Rating" in der heutigen KSV1870 Nimbusec GmbH bis zur Einbindung der dafür maßgeblichen Stakeholder war es nur ein kurzer Weg. Das neuartige Rating sollte ja speziell die Betreiber kritischer Infrastrukturen adressieren und unterstützen. Und so gelang es rasch, eine Reihe anerkannter Top-Experten aus der Praxis für dieses Vorhaben zu gewinnen und dieses somit stringent an den Bestimmungen des Gesetzes für Netz- und Informationssystemsicherheit, kurz NIS, und den Praxisanforderungen auszurichten.

Wer sind nun diese „Ideengeber", und welche Aspekte bringen sie in dieses Innovationsprojekt ein?

Foto: Freepik

Das Kompetenzzentrum Sicheres Österreich (KSÖ) unter der Leitung von Alexander Janda ist „Eigentümer" des Cyber Risk-Schemas und Träger des Advisory Boards.

Die KSV1870 Nimbusec GmbH unter Alexander Mitter – gemeinsam mit Thomas Stubbings von Cyber Trust Austria der Initiator dieses Projektes – betreibt die Rating-Lösung, während Thomas Stubbings das Cyber Trust Label herausgibt.

Vertreter der operativen NIS-Behörde im BMI adressieren die maßgeblichen gesetzlichen Aspekte und lenken den Blick frühzeitig auf künftige Anforderungen, beispielsweise aus NIS 2.0 resultierend.

Die weiteren Mitglieder aus den im NIS-Gesetz gelisteten Branchen bringen ihre umfangreiche praktische Expertise laufend ein, erarbeiten und aktualisieren alljährlich gemeinsam mit KSV1870 Nimbusec das CRR-Schema als Grundlage für das nachfolgende CyberRisk Rating, gestalten die zugehörigen Prozesse rund um den Rating-Vorgang mit und achten strikt auf die Praxisnähe der erarbeiteten Lösung.

Das Cyber Risk Advisory Board 2021/22:

Christian Brennsteiner
Spar Business Services GmbH

Gerald Hübsch
ehemals Energie AG OÖ & nun selbstständiger IT-Experte

Thomas Von der Gathen
Payment Services Austria GmbH (PSA)

Peter Gerdenitsch
Raiffeisen Bank International AG (RBI)

Michael Stephanitsch
IT-Services der Sozialversicherung GmbH (ITSV)

Wolfgang Schwabl
A1 Telekom Austria Group

Manfred Spanner
OMV AG

Walter Fraißler
VERBUND AG

Anton Sepper
Wiener Linien GmbH

Dieses Team unterstützt mit seinem Spirit und Know-How die Einführung des österreichischen CyberRisk Ratings im Interesse einer gesteigerten Sicherheit und Resilienz der Unternehmen und Organisationen in unserem Land. ■

INTERVIEW:

„Daten, Informationen und Wissen sind der ‚Treibstoff' im Unternehmen"

Das **Kompetenzzentrum Sicheres Österreich (KSÖ)** und der **KSV1870** haben ein neuartiges CyberRisk Rating für Österreich als Beitrag zum Basisschutz unserer Unternehmen und Organisationen vor den zahllosen Bedrohungen im Cyberspace entwickelt. Ergänzend zur klassischen Informationssicherheit bietet dieses System auch ein spezifisches Datenschutzmodul. Wir sprachen mit **Manfred Spanner, oberster Konzerndatenschutzmanager in der OMV**, über Inhalt und Nutzen dieses federführend von ihm ausgestalteten Datenschutzmoduls.

TEXT: Gerald Hübsch

Herr Spanner, wie sind Sie zum Datenschutz gekommen, und was fasziniert Sie an Ihrer Tätigkeit?

Nach einer umfassenden Ausbildung in Recht, Wirtschaftsinformatik und Security führte mich mein Weg frühzeitig in das Informationsmanagement und die Informationssicherheit. Berufliche Stationen waren u. a. die Banken- und IT-Branche, ein großer österreichischer Transportkonzern, staatliche Expertengremien und aktuell der OMV Konzern. Mein besonderes Interesse galt dabei immer der organisatorischen und rechtlichen Sicht auf das „Datenuniversum" im Unternehmen. Ich betrachte es als spannende Herausforderung, die Daten = Werte im Unternehmen zu schützen und insbesondere deren Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen (C-I-A = confidentiality + integrity + availability).

Welchen Beitrag leistet ein gutes Datenschutzmanagement im Unternehmen, und wo liegen die größten Herausforderungen?

Daten, Informationen und Wissen sind der „Treibstoff" im Unternehmen. Ein professionelles, durchgängiges Datenschutzmanagement identifiziert und schützt die informatorischen „Juwelen" im Unternehmen, bewertet und reduziert die korrespondierenden Risiken und vermeidet durch die Einhaltung der gesetzlichen Vorgaben finanzielle Strafen. Guter Datenschutz sichert somit Werte, wendet potenziellen Schaden ab und stärkt das Vertrauen der Mitarbeiter, Kunden und Geschäftspartner in eine ordnungsgemäße Behandlung ihrer personenbezogenen Daten.

> **Informationssicherheit und Datenschutz sind ‚Geschwister', die einander ergänzen.**

Welche Schwerpunkte umfasst Ihr Aufgaben- und Verantwortungsbereich in der OMV?

Meine Einheit Group Data Protection Office kümmert sich international um das Datenschutzmanagement im OMV Konzern und stellt in meiner Person auch den obersten Datenschutzbeauftragten. Unser Datenschutzmanagement verfolgt dabei einen integralen Ansatz und deckt nicht nur technische und risikobezogene Aspekte, sondern auch die damit verknüpften wirtschaftlichen und rechtlichen Dimensionen einschließlich der Bewusstseinsbildung unserer Mitarbeiter (Awareness) ab.

Sie haben im Cyber Risk Advisory Board des Kompetenzzentrum Sicheres Österreich (KSÖ) federführend das neue Datenschutzmodul

ZUR PERSON:

Mag. Manfred Spanner, MSc. führt die Konzerneinheit Group Data Protection Office in der Konzernzentrale der OMV, hat den globalen Lead als konzernweiter Datenschutzbeauftragter und leitet die operativen Datenschutzagenden der österreichischen Konzerngesellschaften.

Herr Spanner verfügt über eine breite Ausbildung in Wirtschaftsrecht, Wirtschaftsinformatik und Informationssicherheit. Er blickt auf langjährige Führungserfahrung im Banken-, IT-, Transport- und Industriesektor zurück und hat unter anderem die legislative Umsetzung der NIS-Verordnung und der Datenschutzverordnung in Österreich begleitet.

Fotos: OMV AG - OMV Zentrale Wien, Manfred Spanner

gestaltet. Inwieweit konnten Sie Ihre professionelle Erfahrung einfließen lassen? Können Sie uns Beispiele aus der Praxis nennen?

Mit großer Freude durfte ich meine langjährigen Erfahrungen aus der Praxis und für die Praxis einbringen. Unsere oberste Zielsetzung war es, Unternehmen und Organisationen beliebiger Größe einen unmittelbar anwendbaren, verständlichen Datenschutzkatalog im Einklang mit dem neuen Datenschutzgesetz zur Hand zu geben. Wie gestalte ich ein effektives Datenschutzmanagement, welche Vorkehrungen und Abläufe sind zu beachten, wie entspreche ich den Betroffenenrechten, und wie reagiere ich auf mögliche Datenschutzverletzungen – dies sind nur einige der konkreten Fragestellungen und Lösungsansätze.

Gibt es beim CyberRisk Rating Gemeinsamkeiten zwischen der Cybersicherheit und dem Datenschutz?

Definitiv. Informationssicherheit und Datenschutz sind „Geschwister", die einander ergänzen. Während Informationssicherheit den Schwerpunkt eher auf technisch-organisatorische Maßnahmen und die gesicherte Verfügbarkeit der Informationsverarbeitung legt, schützt der Datenschutz den Lebenszyklus personenbezogener Daten.

Richtet sich das Datenschutzmodul ausschließlich an IT-Unternehmen?

Keineswegs! Das Modul hilft allen Unternehmen und Organisationen im Interesse eines gesetzeskonformen und wirksamen Datenschutzes. Datenschutz ist auch für Unternehmen ohne (End-)kundenkontakt maßgeblich, insbesondere bei der Verarbeitung von Mitarbeiterdaten. Auch bei der operativen Abwicklung durch beauftragte interne oder externe Dienstleister verbleibt die Gesamt- und Letztverantwortung stets beim eigenen Unternehmen.

Sind die Anforderungen des KSÖ Cyber Risk Advisory Boards in Zukunft auch für Lieferanten der OMV relevant?

> **Sie müssen nicht zum Datenschutzexperten mutieren. Das Grundverständnis und die ‚Awareness' für Datenschutz sollten ausreichen, um eine geeignete Datenschutzorganisation im Unternehmen einzurichten (...).**

Voll und ganz. Auch die OMV beauftragt – als Betreiber wesentlicher, „kritischer" Infrastruktur im Sinne des NIS-Gesetzes – zahlreiche Lieferanten und Dienstleister und trägt dabei die Letztverantwortung für Informationssicherheit und für Datenschutz. In diesem Zusammenhang sind auch verpflichtende Lieferantenaudits durchzuführen (Third Party Risk Assessment/Management). Das neue CyberRisk Rating erleichtert und beschleunigt diese Arbeit und verbessert so den Fokus und die Wirksamkeit der noch verbleibenden, eigenen Audits. Eine umfassende Analyse sämtlicher externer Vertragswerke der OMV hat uns übrigens gezeigt, dass rund ein Viertel davon datenschutzrechtlich relevant ist.

Kann das Datenschutzmodul auch kleineren Unternehmen als Orientierungshilfe dienen, und wie können diese ebenfalls einen guten Datenschutz erreichen?

Auf alle Fälle! Sowohl das grundlegende CyberRisk Rating als auch das Datenschutzmodul sind vom Einpersonen- über Klein- und Mittelstandsunternehmen bis hin zum internationalen Konzern anwendbar und nutzbringend.

Ist die anfängliche Unsicherheit, die bei der Einführung der DSGVO in Österreich geherrscht hat, Ihres Erachtens mittlerweile überwunden?

Österreich besitzt seit dem Jahr 2000 ein Datenschutzgesetz. Die anfängliche Unsicherheit bei der Umsetzung der EU-weiten DSVGO hing wohl eher am unerwartbaren Strafausmaß für (grobe) Datenschutzverletzungen. Die inhaltlichen Anforderungen selbst bis hin zur Verankerung eines Datenschutzmanagementsystems im Unternehmen waren und sind nachvollziehbar und klar im Gesetz geregelt. Die

Einhaltung von Betroffenenrechten, das Einholen von Einverständniserklärungen und die zeitnahe, geeignete Reaktion auf Vorfälle sind zwischenzeitlich zum Selbstverständnis geworden – ein großer Fortschritt!

Was würden Sie Geschäftsführern, die keinen juristischen Hintergrund besitzen, als Überblick und Leitfaden im Bereich Datenschutz empfehlen?

Nun, sie müssen nicht zum Datenschutzexperten mutieren. Das Grundverständnis und die „Awareness" für Datenschutz sollten ausreichen, um eine geeignete Datenschutzorganisation im Unternehmen einzurichten, Verantwortung und Handlungsvollmacht klar zu übertragen und so den wichtigsten Schritt zur Verankerung eines funktionierenden Datenschutzmanagementsystems zu setzen.

Hat die DSGVO den österreichischen Wirtschaftsstandort Ihres Erachtens geschwächt, oder sind österreichische/europäische Unternehmen als Zulieferer nun im Vorteil?

Dies führt in Ansätzen zu einer philosophischen Betrachtung. Nach meiner Einschätzung war bzw. ist die Verankerung eines funktionierenden Datenschutzmanagementsystems mit einem gewissen Aufwand verbunden, schützt aber wie vorhin erwähnt die informatorischen „Juwelen" im Unternehmen, sichert Werte, identifiziert und kontrolliert Risiken und vermeidet Strafen.

Auch bzw. gerade weil Daten zum „neuen Öl" in der globalen Wirtschaft werden, hat die Europäische Union mit ihrer DSGVO den Weg bereitet und dient als Referenz für zahlreiche Länder und mitunter auch globale IT-Konzerne, wie z. B. Apple. Europäische Unternehmen mit DSGVO-Konformität erzielen so einen gewissen Vertrauensvorschuss und -bonus am Weltmarkt.

Wird das Modell des europäischen Datenschutzes angesichts der globalen Digitalisierung haltbar sein, oder sind wir globalen Konzernen aus DSGVO-Drittländern hilflos ausgeliefert?

Ich denke, erst die kommenden Jahre können diese Frage solide beantworten. Globale Unternehmen, welche u. a. auch den europäischen Markt bedienen (wollen), kommen nicht um die Einhaltung der DSGVO herum. International betrachtet ist der „Kampf" zwischen ungehemmter kommerzieller Datensammlung, -analyse und -verwertung einerseits und dem Schutz personenbezogener Daten andererseits noch nicht entschieden.

Sehr geehrter Herr Spanner, wir danken für das interessante Gespräch! ■

ZUM INTERVIEWPARTNER:

Das Interview führte **Dipl.-Ing. Dr. Gerald Hübsch**, langjähriger CIO, Konzern-Informationssicherheitsverantwortlicher und aktuell IT Business Angel, in seiner Funktion als Mitglied im Cyber Risk Advisory Board des KSÖ.

Foto: Privat | Dr. Gerald Hübsch

Foto: Freepik

FACHBEITRAG:

Das österreichische CyberRisk Rating – **erste Erfahrungen eines Betreibers kritischer Infrastrukturen**

Gerald Hübsch, Mitglied im Cyber Risk Advisory Board, sprach mit Walter Fraißler, Leiter der Informationssicherheit bei VERBUND AG, und Alexander Mitter, Geschäftsführer der KSV1870 Nimbusec GmbH, über Zielsetzung, Nutzen und die ersten Praxiserfahrungen mit dem österreichischen CyberRisk Rating. TEXT: Gerald Hübsch, Walter Fraißler, Alexander Mitter

Die Innovationsidee:

Das neuartige, österreichische CyberRisk Rating des KSV1870 macht die Risiken in der digitalen Geschäftsabwicklung sicht- & greifbar.

Die branchenübergreifend zunehmende digitale Durchdringung unserer Geschäftstätigkeiten ermöglicht nicht nur hohe Kundenzentrierung, Produktqualität und Prozesseffizienz, sondern erhöht im Gegenzug auch die Abhängigkeit von digitalen Diensten und Systemen. Eine Geschäftsunterbrechung, sei es durch technische Gebrechen oder die Folgen eines Cyberangriffs, kann unsere Unternehmen teuer zu stehen kommen oder sogar in ihrer Existenz bedrohen. Was liegt also näher, als die Risiken in der gesamten Liefer- und Wertschöpfungskette zu analysieren und in einem Rating – wie es die Finanzbranche bereits seit langem kennt – sichtbar zu machen?

Gesagt, getan! Das österreichische Unternehmen Nimbusec GmbH, mittlerweile zur KSV1870 Gruppe zählend, hat unter Patronanz des Kompetenzzentrum, Sicheres Österreich in den vergangenen beiden Jahren gemeinsam mit Top-Experten aus der Praxis ein international beachtetes Rating-System für Cyberrisiken auf die Beine gestellt. Wir haben mit dem Geschäftsführer der KSV1870 Nimbusec GmbH, Alexander Mitter, und mit Walter Fraißler, Konzernverantwortlicher für Informationssicherheit bei VERBUND, gesprochen:

Foto: Freepik

Q **Sehr geehrter Herr Mitter, welches Problem adressiert das neuartige CyberRisk Rating, und welchen Vorteil bietet es Ihren Kunden?**

A Unsere Kunden, vom Kleinstbetrieb bis hinauf zum international tätigen Konzern, müssen die Risiken der digitalen Geschäftsabwicklung kennen, in ihrer Auswirkung auf das eigene Unternehmen beurteilen und geeignete Schutzmaßnahmen ergreifen können. Dies kann natürlich nicht im Inselbetrieb erfolgen, sondern muss die gesamte Lieferkette umfassen. Und genau dabei hilft unser CyberRisk Rating. Es gibt strukturiert Auskunft über die sicherheitstechnische Verfassung eines Geschäftspartners und die Erfüllung adäquater Sicherheitsstandards, auf dem Stand der Technik wie auch gesetzlicher Vorgaben. Gerade hier setzt ja auch die EU-Richtlinie NIS – Netzwerk- und Informationssystemsicherheit – an und verpflichtet in weiterer Folge via nationales NIS-Gesetz die „Betreiber wesentlicher Dienste" zu besonderen Vorkehrungen, u. a. auch zur Überwachung ihrer Lieferkette – Third Party Risk Management. Den geforderten und von den maßgeblichen öffentlichen Stellen akzeptierten Nachweis darüber kann nun unser neues CyberRisk Rating erbringen. Und da wir diesen professionellen Service für alle in Österreich tätigen Unternehmen anbieten, können sich sowohl unsere Kunden als auch deren Lieferanten bzw. Geschäftspartner darauf stützen und sich so viel Ärger, Zeit und Mühe ersparen.

> **„Dies erspart diesem Unternehmen ab nun die vielfache Beantwortung meist geringfügig unterschiedlicher Anfragen potenzieller Kunden in ihren Ausschreibungsverfahren (...)."**

Q **Und wie kommt nun ein interessiertes Unternehmen zum geschäftsrelevanten CyberRisk Rating?**

A Unser Klient beauftragt uns, das CyberRisk Rating für ein bestimmtes Unternehmen in seiner Lieferkette einzuholen bzw. auszuweisen. Wir gehen – falls es sich um die erstmalige Anfrage zu diesem Unternehmen handelt – auf dieses mit einem strukturierten Fragebogen über seinen Zustand im Informationssicherheitsmanagement zu, validieren und bewerten die Antworten und gelangen so zu einem Rating-Index.

Analog dazu kann auch ein Hersteller bzw. Lieferant selbst jederzeit diesen Rating-Prozess durchlaufen, Erkenntnisse über seine Cyberrobustheit gewinnen und nötige Schutzmaßnahmen daraus ableiten. Als Ergebnis erhält dieses Unternehmen einen Rating-Index und – optional – auch ein sichtbares Label von Cyber Trust Austria.

Dies erspart diesem Unternehmen ab nun die vielfache Beantwortung meist geringfügig unterschiedlicher Anfragen potenzieller Kunden in ihren Ausschreibungsverfahren und stellt ein Gütesiegel für die Cybersicherheit seiner Produkte und Dienstleistungen dar.

Q **Sehr geehrter Herr Fraißler, VERBUND ist gewissermaßen Österreichs Rückgrat in der Energieversorgung. Welche Bereiche umfasst dies konkret?**

A VERBUND ist Österreichs führendes Energieunternehmen und einer der größten Stromerzeuger aus Wasserkraft in Europa. Wir sind ein Taktgeber für die Branche und gestalten die Energiezukunft für kommende Generationen mit. Dafür gehen wir neue Wege, ergreifen Marktchancen und entwickeln wegweisende Geschäftsmodelle und Services für unsere Kunden. VERBUND handelt in zwölf Ländern mit Strom und erzielte 2020 mit rund 2.900 Mitarbeiterinnen und Mitarbeitern einen Jahresumsatz von rund 3,2 Milliarden Euro.

In den vergangenen drei Jahren hat die Informationssicherheit einen noch höheren Stellenwert in unserem Unternehmen bekommen. Im Rahmen des „Masterplans Information Security" werden alle Aspekte des Reifegrads in der Cybersecurity weiterentwickelt und vorangetrieben. Seit 2021 laufen die Fäden von IT, Digitalisierung, Informationssicherheit und Telekom in einem Holdingbereich unter Leitung von Thomas M. Zapf und im Vorstandsbereich von Achim Kaspar zusammen.

Die steigenden Bedrohungen durch Cyberangriffe (egal, durch welche Akteure), die Anforderungen von Geschäftsprozessen und Kunden und die steigenden regulatorischen Vorgaben sind unsere Treiber im Gebiet der Informationssicherheit. Das NIS-Gesetz hat bei vielen

> **„Ein wesentlicher Punkt in diesen Vorgaben, übrigens auch in der Norm ISO 27.001, ist die Sicherheit in der Lieferantenkette; dafür stellt das CyberRisk Rating aus unserer Sicht eine sehr gute Lösung dar."**

Foto: VERBUND | Speicherkraftwerk

Foto: VERBUND | Übertragungsnetz

Unternehmen, die wesentliche Dienste für die Gesellschaft bereitstellen, eine zusätzliche und maßgebliche Investition in Cybersecurity ausgelöst. Ein wesentlicher Punkt in diesen Vorgaben, übrigens auch in der Norm ISO 27.001, ist die Sicherheit in der Lieferantenkette; dafür stellt das CyberRisk Rating aus unserer Sicht eine sehr gute Lösung dar.

Q **Nachdem wir nun die Hauptgründe für den Einsatz des CyberRisk Ratings von KSV1870 kennen – wie ist es Ihnen bei der Umsetzung ergangen, und welchen Nutzen ziehen Sie als VERBUND daraus?**

A Im Zuge unseres „Masterplans Information Security" haben wir uns mit dem Third Party and Vendor Risk Management intensiv auseinandergesetzt. Unser erster Zugang zu diesem Thema war das, was bisher allgemein als Best Practice gegolten hat: die Lieferanten zu klassifizieren und dann einen großen Teil der Lieferanten über die Aussendung eines Fragebogens zu bewerten. Ein solcher Fragebogen orientiert sich idealerweise an einer allgemeinen Struktur – besteht letzten Endes aber doch aus sehr vielen Fragen, deren Beantwortung oft nicht ganz einfach ist. Nach dem Erhalt eines beantworteten Fragebogens heißt es dann noch, diesen zu überprüfen und zu verifizieren. Mit dieser allgemein anerkannten Vorgangsweise haben wir zwei Problemfelder identifiziert: Zum einen würden wir einen solchen Fragebogen an relativ viele Lieferanten versenden, erhalten von diesen Rückfragen, die beantwortet werden müssen, und haben die Antworten schließlich zumindest auf Plausibilität zu überprüfen. Mit einem Wort: Wir haben sehr viel Arbeit auf unserer Seite zu erledigen. Zum anderen haben viele Lieferanten nicht nur uns als Kunden. Wenn auch andere Kunden – was zu erwarten ist – ihr Lieferanten-Risikomanagement intensivieren, dann erhalten die Lieferanten eine Reihe von sehr ähnlichen, aber doch nicht identen Fragebögen zur Beantwortung. Resultat: Auch auf der Seite der Lieferanten entsteht sehr viel Arbeit.

PROJEKTORGANISATION

Daher haben wir die Idee des Teams um Alexander Mitter, ein standardisiertes „Cybersecurity Rating“ zu entwickeln, sofort als hervorragend eingestuft. Eine der großen Herausforderungen war es, die doch leicht unterschiedlichen und oft sehr umfangreichen Anforderungen von verschiedenen Betreibern auf einen gemeinsamen Nenner zu bringen. In sehr intensiven Diskussionen im Advisory Board ist es uns letztlich gelungen, diese Anforderungen auf eine sehr überschaubare Anzahl von Fragen zu komprimieren. Genauso wurde ein Prozess für den Ablauf des Ratings und die erforderliche Plausibilisierung der Antworten skizziert.

BETRIEBLICHER NUTZEN

Im Idealfall fordern wir für einen neuen Lieferanten das CyberRisk Rating an, das in der Datenbank schon vorliegt und daher unverzüglich verfügbar ist. Falls das noch nicht vorliegt, muss der Lieferant den Fragebogen ein einziges Mal bearbeiten. Wir können darauf vertrauen, dass die Antworten und somit das Rating qualitätsgeprüft wurden. Für die Großzahl der Lieferanten wird das Rating als Kriterium ausreichen – für wenige besonders kritische Lieferanten ist es jedenfalls eine gute Basis für ein weiterführendes Audit. In diesem Idealfall sieht man sehr rasch die Vorteile in Aufwand und Durchlaufzeit auf unserer Seite – aber auch auf der Seite des Lieferanten.

HERAUSFORDERUNGEN

Die größte Herausforderung bei den ersten Anfragen nach dem Rating war vermutlich, dass dieses völlig neu und daher noch unbekannt war. Die Lieferanten hatten daher eine – verständliche – Zurückhaltung und Rückfragen vor der Durchführung des Ratings. Ich bin zuversichtlich, dass diese Hürde mit zunehmender Bekanntheit des CyberRisk Ratings deutlich niedriger werden wird. Zudem wird durch die beabsichtigte Novellierung der NIS-Regulierung – Stichwort „NIS 2.0“ – der Kreis der vom NIS-Gesetz betroffenen Unternehmen um ein Vielfaches größer werden.

Wir danken für das interessante Gespräch!

Foto: VERBUND | Fischwanderhilfe in Kärnten

Seit 1988 notiert VERBUND an der Börse Wien, 51 % des Aktienkapitals besitzt die Republik Österreich.

Mit Tochterunternehmen und Partnern ist VERBUND von der Stromerzeugung über den Transport bis zum internationalen Handel und Vertrieb aktiv. Mit der Austrian Power Grid AG und der Gas Connect Austria GmbH besitzt VERBUND zu 100 % bzw. 51 % die österreichischen Übertragungsnetzbetreiber für Strom bzw. Gas. Mit der Strategie „Mit unserer Kraft in eine grüne Zukunft" will VERBUND nicht nur der wirtschaftlichen, sondern auch der gesellschaftlichen Verantwortung als führendes Energieunternehmen Österreichs gerecht werden.

Als größtes Stromunternehmen in Österreich und als führender Wasserkraftwerksbetreiber in Bayern ist sich VERBUND seiner Verantwortung bewusst. Er versorgt Millionen Menschen sicher mit lebensnotwendiger elektrischer Energie. Die Anlagen werden effizient geführt und bei der Stromgewinnung Umwelt und Klima geschützt. Wie stark Krisenmanagement und Resilienz bei VERBUND etabliert sind wurde nicht nur in den vergangenen zwei Jahren unter Beweis gestellt. ■

ZU DEN PERSONEN:

Foto: VERBUND | Walter Fraißler

DIPL.-ING. DR.
WALTER FRAISSLER

Dipl.-Ing. Dr. Walter Fraißler ist promovierter Mathematiker (TU Wien) und langjährige Führungskraft bei VERBUND. Sein beruflicher Weg führte ihn von der IT-Abteilung über die Rolle als Assistent des Vorstandsvorsitzenden zur Verantwortung für die Konzernorganisation und zur Funktion des CIO und Leiters der IT-Services. In den vergangenen vier Jahren war er damit beauftragt, den Bereich der Informationssicherheit konzernweit aufzubauen und weiterzuentwickeln. Er verfolgt mit seinem engagierten Team diese Ziele im Interesse der gesteigerten Cyberresilienz seines Unternehmens und der österreichischen Versorgungssicherheit.

Foto: Privat | Alexander Mitter

MAG.
ALEXANDER MITTER

Mag. Alexander Mitter ist Geschäftsführer der KSV1870 Nimbusec GmbH. Nach Absolvierung der HTL und Studium der Betriebswirtschaft sammelte er Praxiserfahrungen in einem global tätigen Technologieunternehmen, bevor er bei Nimbusec in die Geschäftsführung wechselte und die Markteinführung der Security-Produktpalette leitete. In weiterer Folge entwickelte er die Gründungsidee für ein „CyberRisk Rating Austria" und steuert nun – als Mitgliedsunternehmen der KSV1870 Gruppe – dessen Markteinführung.

Foto: Privat | Dr. Gerald Hübsch

DIPL.-ING. DR.
GERALD HÜBSCH

Dipl.-Ing. Dr. Gerald Hübsch, langjähriger CIO, Konzern-Informationssicherheitsverantwortlicher und aktuell IT Business Angel, führte das Gespräch in seiner Funktion als Mitglied im Cyber Risk Advisory Board des KSÖ.

Foto: Freepik

INTERVIEW:

Österreichs Qualitätssiegel für Cybersicherheit

Das Cyber Trust Austria Label gibt Organisationen die Möglichkeit, nach außen sichtbar zu zeigen, dass sie essenzielle Mindestsicherheitsmaßnahmen für Cybersicherheit umgesetzt haben und das Thema einen entsprechenden Stellenwert in der Organisation hat. Der Generalsekretär des Kompetenzzentrum Sicheres Österreich (KSÖ), Dr. Alexander Janda, und Geschäftsführer der Cyber Trust Austria, Dr. Thomas Stubbings, im Gespräch.

TEXT: Alexander Janda, Thomas Stubbings

Herr Dr. Janda, warum hat sich das KSÖ dazu entschlossen, ein Gütesiegel für Cybersicherheit zu entwickeln?

DR. JANDA: Cybersicherheit ist eine Herausforderung, die nicht an den Grenzen eines Unternehmens Halt macht. Gerade Unternehmen der kritischen Infrastruktur brauchen eine verlässliche und sichere Lieferkette. Daher ist und war es unser Anliegen, die Verlässlichkeit und Sicherheit auch in einem Gütesiegel nach außen sichtbar zu machen.

Herr Dr. Stubbings, als Geschäftsführer der Cyber Trust Services GmbH sind Sie dafür verantwortlich, die Gütesiegel an die Antragsteller, gemäß KSÖ-Schema zu vergeben. Wer ist Ihre Zielgruppen?

DR. STUBBINGS: Grundsätzlich ist jedes Unternehmen Zielgruppe, das in irgendeiner Weise mit IT und elektronischen Daten arbeitet – und wer tut das heutzutage nicht mehr? Jeder, der Computer und Netzwerk betreibt oder betreiben lässt und damit Daten verarbeitet und speichert, egal, ob seine eigenen und/oder jene von Kunden, muss auf die Cyberhygiene seiner Infrastruktur und seiner Prozesse achten. Im eigenen Interesse und dem seiner Kunden und Partner.

Warum im Interesse der Kunden und Partner?

DR. STUBBINGS: Durch die enge Vernetzung mit unseren Kunden und Partnern ergeben sich für Angreifer und auch Schadsoftware vermehrt Möglichkeiten, von einem Unternehmen ins nächste zu gelangen. Das ist sogar leichter, als von draußen einzudringen – denn Unternehmen, die miteinander Geschäfte machen, vertrauen sich üblicherweise gegenseitig. Ich erinnere nur an NotPetya, den bisher größten Cybervorfall der Geschichte: Da kam die Schadsoftware über ein Software-Update eines Lieferanten direkt ins Netzwerk seiner Kunden.

Herr Dr. Janda, wie schätzen Sie seitens des KSÖ die aktuelle Risikosituation für österreichische Unternehmen ein, im Allgemeinen und im Speziellen hinsichtlich Lieferantenrisiko?

> **Die Angreifer machen dabei keinen Unterschied, ob es sich um eine große Bank oder einen kleinen, mittelständischen Betrieb handelt.**

DR. JANDA: Während der vergangenen eineinhalb Jahre ist die Cyberkriminalität um mehr als ein Viertel angestiegen. Angriffsziele sind dabei neben staatlichen Einrichtungen oder einer wachsenden Zahl von Privatpersonen vor allem Unternehmen. Die Angreifer machen dabei keinen Unterschied, ob es sich um eine große Bank oder einen kleinen, mittelständischen Betrieb handelt. Zugleich steigt die Schadenssumme permanent

Foto: Redtenbacher | Alexander Janda

DR. ALEXANDER JANDA
KOMPETENZZENTRUM
SICHERES ÖSTERREICH (KSÖ)

Foto: Privat | Thomas Stubbings

DR. THOMAS STUBBINGS
CYBER TRUST AUSTRIA

an – in vielen Fällen ist ein Cyberangriff existenzbedrohend.

Teilen Sie diese Ansicht?

DR. STUBBINGS: Ja, wir sehen in Österreich immer mehr Angriffe auf KMUs. Ständig gehen Fälle durch die Medien: von Palfinger über Salzburgmilch bis hin zu dem Vorfall neulich in Oberösterreich, bei dem ein IT-Betreiber 34 seiner Kunden „mitgerissen" hat. Es ist leider heute nicht mehr genug, auf seine eigene Cybersicherheit zu schauen, sondern man muss auch darauf achten, mit vertrauenswürdigen und sicheren Unternehmen zusammenzuarbeiten.

Herr Dr. Janda, warum ist das KSÖ für die Umsetzung des CyberRisk Ratings in eine Kooperation mit dem KSV1870 gegangen? Was macht diese Partnerschaft so besonders?

DR. JANDA: Der KSV1870 ist als Österreichs führender Gläubigerschutzverband seit vielen Jahren ein verlässlicher Partner der österreichischen Wirtschaft. Mit seiner hohen Innovationsorientierung ist der KSV1870 der ideale Partner, um die Dynamik der technologischen Entwicklungen im Bereich der Digitalisierung, die sich unter anderem in der Herausforderung der Cybersicherheit manifestiert, in einem neuen CyberRisk Rating abzubilden.

Herr Dr. Stubbings, können Sie uns bitte noch kurz erklären, was die wesentlichen Unterschiede zwischen dem Standard-Label und dem Gold-Label sind?

DR. STUBBINGS: Das Standard-Label steht für Basissicherheit. Die zugrundeliegenden 14 Kriterien sind so konzipiert, dass jede – auch sehr kleine – Organisation diese mit überschaubarem Aufwand erreichen kann. Basissicherheit kostet keine Unsummen. Aber man muss sich fokussiert mit dem Thema auseinandersetzen und ein bisschen Zeit investieren. Es gibt eigentlich keine Rechtfertigung mehr dafür, warum irgendein Unternehmen nicht die Basissicherheitskriterien erfüllt – das sollte so selbstverständlich sein wie Händewaschen oder die Wohnung zusperren. Das Gold-Label legt schon einen höheren Anspruch an – es richtet sich vor allem an größere Unternehmen, die in sensiblen Bereichen tätig sind und schon mehr für ihre Cybersicherheit getan haben. Beim Gold-Label kommt übrigens noch ein Third Party Audit dazu, für das Standard-Label reicht eine validierte Selbstdeklaration.

Was ist eine „validierte Selbstdeklaration"?

DR. STUBBINGS: Das bedeutet, dass das Unternehmen selbst Angaben dazu macht, wie die einzelnen Anforderungen im Unternehmen erfüllt sind. Ein Validierer, das ist ein Experte mit einschlägiger Erfahrung, überprüft diese Angaben dann auf Vollständigkeit, Plausibilität und Konsistenz mit anderen Angaben. Wenn es Unklarheiten gibt, hat der Validierer die Möglichkeit Rückfragen zu stellen. Der Validierungsschritt bringt viel Qualität in den Prozess.

Herr Dr. Janda, abschließend, was sind Ihre weiteren Pläne hinsichtlich des Cyber Trust Label?

DR. JANDA: Wir sind mit unserem Cyber Trust Label sehr gut gestartet und haben viele positive Rückmeldungen bekommen. Jetzt wollen wir möglichst viele Unternehmen in Österreich ansprechen und für dieses neue Gütesiegel gewinnen. Die Akzeptanz des österreichischen Marktes ist dann Voraussetzung dafür, dieses Thema auch auf die europäische Bühne zu tragen. Cyberherausforderungen machen an nationalen Grenzen keinen Halt. Wir wollen unser Know-how, das wir in Österreich und mit österreichischen Partnern entwickelt haben, auch in unsere Nachbarländer und darüber hinaus in die Europäische Union tragen. Zugleich werden wir unser Schema inhaltlich weiterentwickeln, um mit den Entwicklungen und Herausforderungen der Security Schritt zu halten. ■

Mehr Informationen zu Österreichs Cybersicherheits-Qualitätssiegel finden Sie unter **www.cyber-trust.at**

3 Fragen zum Cyber Trust Label mit Geldservice Austria

Q **Warum haben Sie das Cyber Trust Label erworben?**

A Die Geldservice Austria hat das Cyber Trust Label erworben, weil wir damit unser hohes Sicherheitsniveau dokumentieren können. Unsere Kunden und Partner werden durch diverse Vorschriften und Vorgaben gezwungen, entsprechende Bestätigungen einzuholen, die wir speziell im Bereich Cybersicherheit mit dem Cyber Trust Label auf praktikable Weise zur Verfügung stellen können.

Q **Welche Bedeutung haben Gütesiegel für Cybersicherheit für Sie?**

A Gerade bei einem komplexen und sich rasch entwickelnden Thema wie Cybersicherheit ist die Verwendung von qualitativen und aussagekräftigen Gütesiegeln eine wesentliche Erleichterung. Die Bestätigung eines definierten Sicherheitslevels durch unabhängige Dritte schafft auf einfache Weise die (Vertrauens-)Basis für Geschäftsbeziehungen.

Q **Worauf achten Sie bei Ihren eigenen Lieferanten hinsichtlich Cybersicherheit?**

A Da die Geldservice Austria die Bargeldversorgung Österreichs im Auftrag der Konzernmutter Oesterreichische Nationalbank sicherstellt, wird ein entsprechend hohes Sicherheitsniveau gefordert. Das Vorliegen einschlägiger Zertifizierungen ist somit eine Grundvoraussetzung, und speziell im Bereich Cybersicherheit ist die Abstimmung mit den IT-Experten der OeNB sehr eng.

DAS
CYBERRISK
RATING
by KSV1870

Kontaktinformationen

KSV1870 Nimbusec GmbH
Fadingerstraße 15, 4020 Linz
+43 (0) 732 860626
cr@nimbusec.com

www.cyberrisk-rating.at

nimbusec
Part of KSV1870