KSV1870

CyberRisk Report

THE ANNUAL REPORT OF THE AUSTRIAN CYBERRISK RATING

ISSUE 2022

IT security
An overview of the Austrian critical infrastructure security landscape

Data protection
An interview with OMV data protection expert Manfred Spanner.

IMPRINT: Media owner: KSV1870 Nimbusec GmbH, 4020 Linz, Fadingerstraße 15; www.nimbusec.com/www.cyberrisk-rating.at Publisher: Alexander Mitter; Place of publication: Linz; Editor-in-chief: Elisabeth Hentscholek; Authors of this issue: Alexander Janda, Alexander Mitter, Alen Kocaj, Elisabeth Hentscholek, Gerald Hübsch, Thomas Stubbings, Walter Fraißler; Layout: Elisabeth Hentscholek; Editing: Johannes Payer

Note: For reasons of readability, we have refrained from using gender-specific formulations. Where personal terms are only used in the masculine form, they refer to all genders.

Editorial

We live and work in a world that, thanks to increasingly efficient technology, gives us the highest standard of living in human history. No matter in which direction you look: Information technology is omnipresent. Satellite navigation guides our traffic flows on the roads, on the water and in the air. Computer systems make our X-rays and medical histories available to doctors in original quality. Our companies send invoices digitally, and trade is increasingly taking place in cyberspace even for local goods. Smart meters optimize our power grids, and most of us conduct banking transactions directly on our cell phones. Who could have imagined this less than a generation ago?

But wherever there is light, there is also shadow: Our digitization is built on technology for which new security vulnerabilities are found every hour. Even without active attackers, the reliable functioning of our computers is a major challenge. But since additional criminals and state actors alike have understood that we entrust our most valuable data and processes to this technology, security problems are being exploited systematically and on a grand scale.

How is an IT department supposed to perfectly maintain, secure and monitor all these technologies at any time, on any device and at any company location? And - if this challenge is already huge for our largest companies - how are Austria's small and medium-sized enterprises supposed to meet it?

These questions not only moved the EU Commission when it adopted the NIS Directive[1] and our ministries when they implemented this directive for Austria[2] , but also the cybersecurity experts of the Kompetenzzentrum Sicheres Österreich (KSÖ)[3] , who have created the first Austrian standard for the creation of a CyberRisk Rating[4] since mid-2020. As KSV1870, we use this standard to rate companies worldwide in a uniform, efficient and fair manner. On the following pages, we would like to tell you how this came about, what goals we are pursuing with it, and what insights we have gained as a result.

But I can tell you one thing in advance: Cybersecurity will be one of the most essential factors for the further digitization of our world. No state, no company, no single person will be able to escape this topic. But the opportunities offered by modern technology are too great for us to be discouraged by hackers. So let's remain courageous and innovative! We can master the new challenges together.

I hope you enjoy reading this issue.

Yours Alexander Mitter
CEO of 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

Content

Foto: OMV AG | OMV Zentrale Wien

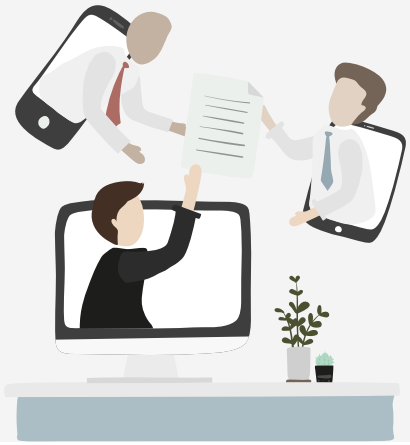

Foto: Freepik

Foto: VERBUND

Foto: Freepik

Foto: Adobe Stock

An overview of Austria's security landscape

In the course of the CyberRisk Rating, a large-scale security scan was carried out across Austria's corporate landscape. The following conclusions were drawn with regard to websites infected with malware: **DATA ANALYSIS:** KSV1870 Nimbusec GmbH | **TEXT:** Elisabeth Hentscholek

28%

MALWARE REMAINS ONLINE FOR AT LEAST 2 MONTHS

28% of infected domains continued to distribute malware to website visitors two months after the malware was discovered.

17%

HACKED AGAIN WITHIN A MONTH

Of the malware-infected websites, 17% were inadequately secured after cleanup and reinfected within a month.

88%

WORDPRESS AS A MALWARE GATEWAY

Wordpress is not only the most widespread content management system, but also the gateway in 88% of malware cases. Reasons for this are missing patches, gaps in templates and especially plug-ins. These technical problems are not solved for a long time due to a lack of organizational processes and responsibilities. So if you don't patch quickly, you will get hacked.

Image: Freepik

CyberRisk Rating: Facts, figures, data

DATA ANALYSIS: Alen Kocaj | **TEXT:** Elisabeth Hentscholek

20%

of the suppliers overestimated themselves on average when answering the assessment. Self-overestimation occurred most frequently in questions B13, A5 and A10.

35%

of the suppliers chose not to select the CyberRisk Rating required by the customer

58%

In 58% of the cases, the verifier had to send a demand to the supplier after completing the assessment because the answer given was not conclusive or detailed enough.

13%

of the companies have a poor basic security level (B rating).

41%

of the companies can only moderately meet the requirement for an advanced security level (A rating).

3 out of 10

suppliers are not able to reliably detect IT security incidents in their company by logging their systems.

Why we need a CyberRisk Rating

As KSV1870, we provide a tool with the CyberRisk Rating, with which we can not only evaluate our business partners, but implicitly also advise them.

For more than 150 years, the Kreditschutzverband von 1870 (KSV1870) has protected the interests of its members by collecting creditworthiness information.

At the time of KSV's founding in 1870, it was credit fraudsters who made life difficult for business people, and as early as the 19th century, the Austrian business community recognized that only by working together across corporate boundaries was a solution possible - just as it is today. TEXT: Alexander Mitter

Technology has evolved dramatically, but fundamentally our members are at the mercy of similar threats today as they were then: Gaps in systems of all kinds are exploited by criminals to gain illegal advantage. Whether information is stolen, money extorted, or identities stolen: In the end, we must defend ourselves against the threats of our time.

The members of KSV1870 form a cross-section of the Austrian economy. In recent years, we have seen the risk of a cybersecurity incident increase for SMEs just as it has for critical infrastructure companies. We now read almost daily of cases where financially sound companies have to stop production because hackers have encrypted their data. Even state actors are using cyberspace to steal knowledge and obtain foreign currency.

In 2020, a jury in the U.S. indicted six officers from a Russian military unit by name, deeming them responsible for thousands of attacks on international businesses, political campaigns, governments and even the Olympics. The details and scope of the indictment provide a rare glimpse into the level of organization of today's hackers.

In light of the war between Russia and Ukraine, we must prepare for these threats to increase further.

As KSV1870, we provide the CyberRisk Rating as a tool to not only assess but implicitly advise our business partners. Each of the 25 requirements of the KSÖ Cyber Risk scheme is a step in the right direction. Now is the time to create security policies for our IT, train employees, test backups and define contingency plans.

Meanwhile, almost every day we read about cases where financially sound companies have to stop production because hackers have encrypted their data.

No company can ignore digitization, and securing our IT is simply necessary for this. We cannot solve this challenge alone - just as we did in 1870: With KSV1870's CyberRisk Rating, we have created a practical tool that builds on the collective knowledge of our country's most experienced IT security and data protection experts.

Feel free to try it for yourself: Our staff at KSV1870 Nimbusec look forward to showing you how to best prepare your business for the cybersecurity challenges of our time. Even SMEs can achieve an excellent CyberRisk rating - with the right measures even without additional costs. ■

The Cyber Risk Advisory Board

What is the role of the Advisory Board in the Austrian CyberRisk Rating, and what makes participation so exciting for experts from the field? Gerald Hübsch spoke with representatives of the industries and public bodies involved about their work on this board:

TEXT: Gerald Hübsch

It was only a short way from the fundamental founding idea in 2019 for a "CyberRisk Rating" in today's KSV1870 Nimbusec GmbH to the involvement of the relevant stakeholders. After all, the new type of rating was intended to specifically address and support the operators of critical infrastructures. And so it was quickly possible to win over a number of recognized top experts from the field for this project and thus to align it stringently with the provisions of the Network and Information System Security Act, NIS for short, and the practical requirements.
So who are these "idea generators" and what aspects do they bring to this innovation project?

Image: Freepik

The Kompetenzzentrum Sicheres Österreich (KSÖ), headed by Alexander Janda, is the "owner" of the Cyber Risk Scheme and the responsible entity of the Advisory Board.

KSV1870 Nimbusec GmbH under Alexander Mitter - together with Thomas Stubbings of Cyber Trust Austria the initiator of this project - operates the rating solution, while Thomas Stubbings issues the Cyber Trust Label.

Representatives of the operational NIS authority in the Federal Ministry of the Interior address the relevant legal aspects and direct the view at an early stage to future requirements, for example resulting from NIS 2.0.

The other members from the industries listed in the NIS Act contribute their extensive practical expertise on an ongoing basis, develop and update the CRR scheme every year together with KSV1870 Nimbusec as the basis for the subsequent CyberRisk rating, help to design the associated processes around the rating process and pay strict attention to the practical relevance of the solution developed.

The Cyber Risk Advisory Board 2021/22:

Christian Brennsteiner
Spar Business Services GmbH

Gerald Hübsch
formerly Energie AG OÖ & now self-employed IT expert

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

This team supports with its spirit and know-how the implementation of the Austrian CyberRisk Rating in the interest of increased security and resilience of companies and organizations in our country. ■

INTERVIEW:

"Data, information and knowledge are the 'fuel' in the company"

The Kompetenzzentrum Sicheres Österreich (KSÖ) and KSV1870 have developed a novel CyberRisk Rating for Austria as a contribution to the basic protection of our companies and organizations against the countless threats in cyberspace. In addition to classic information security, this system also offers a specific data protection module. We spoke with Manfred Spanner, Chief Group Data Protection Manager at OMV, about the content and benefits of this data protection module, which he was in charge of designing. TEXT: Gerald Hübsch

Mr. Spanner, how did you get into data protection, and what fascinates you about your job?

After a comprehensive education in law, business informatics and security, my path led me early on to information management and information security. Professional stations included the banking and IT industry, a large Austrian transport group, government expert committees and currently the OMV Group. My special interest has always been the organizational and legal view of the "data universe" in the company. I consider it an exciting challenge to protect the data = assets in the company and in particular to ensure their confidentiality, integrity and availability (C-I-A = confidentiality + integrity + availability).

What is the contribution of good data protection management in the company, and where are the greatest challenges?

Data, information and knowledge are the "fuel" in a company. Professional, end-to-end data protection management identifies and protects the informational "jewels" in the company, assesses and reduces the corresponding risks, and avoids financial penalties by ensuring compliance with legal requirements. Good data protection thus safeguards values, averts potential damage, and strengthens the trust of employees, customers, and business partners in the proper handling of their personal data.

> **Information security and data protection are 'siblings' that complement each other.**

What are the main areas of your duties and responsibilities at OMV??

My unit, the Group Data Protection Office, is responsible for data protection management within the OMV Group on an international level and I am also the Chief Data Protection Officer. Our data protection management takes an integrated approach and covers not only technical and risk-related aspects, but also the associated economic and legal dimensions, including employee awareness.

You played a leading role in designing the new data protection module on the Cyber Risk Advisory Board of the Competence Center Safe Austria (KSÖ). To what extent were you able to incorporate your professional experience? Can you give us some practical examples?

It was with great pleasure that I was able to contribute my many years of experience from practice and for practice. Our primary objective was to

ABOUT:

Manfred Spanner, MSc. heads the Group Data Protection Office at OMV Group headquarters, has the global lead as Group Data Protection Officer and manages the operational data protection agendas of the Austrian Group companies.

Mr. Spanner has a broad education in business law, business informatics and information security. He looks back on many years of management experience in the banking, IT, transport and industry sectors and has, among other things, accompanied the legislative implementation of the NIS Regulation and the Data Protection Regulation in Austria.

Images: OMV AG - OMV headquarter Vienna, Manfred Spanner

provide companies and organizations of all sizes with a directly applicable, comprehensible data protection catalog in line with the new Data Protection Act. How do I design effective data protection management, what precautions and processes must be observed, how do I comply with the rights of data subjects, and how do I react to possible data protection violations - these are just some of the concrete questions and approaches to solutions.

Are there commonalities between cybersecurity and data protection in CyberRisk Rating?

Definitely. Information security and data protection are "siblings" that complement each other. While information security tends to focus on technical and organizational measures and the assured availability of information processing, data protection protects the life cycle of personal data.

Is the data protection module aimed exclusively at IT companies?

Not at all! The module helps all companies and organizations in the interest of legally compliant and effective data protection. Data protection is also crucial for companies without (end) customer contact, especially when processing employee data. Even in the case of operational processing by contracted internal or external service providers, the overall and ultimate responsibility always remains with the company itself.

Will the requirements of the KSÖ Cyber Risk Advisory Board also be relevant for OMV suppliers in the future?

Fully and completely. As an operator of essential, "critical" infrastructure as defined by the NIS Act, OMV also commissions numerous suppliers and service providers and bears ultimate responsibility for information security and data protection. In this context, mandatory supplier audits must also be carried out (Third Party Risk Assessment). The new CyberRisk Rating facilitates and accelerates this work, thus improving the focus and effectiveness of the remaining, in-house audits. Incidentally, a comprehensive analysis of all external contracts at OMV has shown us that around a quarter of them are relevant in terms of data protection law.

Can the data protection module also serve as a guide for smaller companies, and how can they also achieve good data protection?

In all cases! Both the basic CyberRisk Rating and the data protection module are applicable and beneficial from one-person companies to small and medium-sized enterprises to international corporations.

In your opinion, has the initial uncertainty that prevailed when the GDPR was introduced in Austria now been overcome??

Austria has had a data protection law since 2000. The initial uncertainty surrounding the implementation of the EU-wide GDPR was probably due more to the unexpected level of penalties for (gross) data protection violations. The substantive requirements themselves, up to and including the establishment of a data protection management system in the company, were and are comprehensible and clearly regulated in the law. Compliance with data subjects' rights, obtaining declarations of consent, and responding promptly and appropriately to incidents have in the meantime become a matter of course - great progress!

“They do not have to mutate into data protection experts. The basic understanding and "awareness" of data protection should be sufficient to set up a suitable data protection organization in the company.”

What would you recommend as an overview and guide to data protection for managing directors who do not have a legal background?

Well, they do not have to mutate into data protection experts. The basic understanding and "awareness" of data protection should be sufficient to set up a suitable data protection organization in the company, clearly assign responsibility and authority to act,

and thus take the most important step toward anchoring a functioning data protection management system.

In your opinion, has the GDPR weakened the Austrian business location, or are Austrian/European companies now at an advantage as suppliers?

This leads to some philosophical considerations. In my opinion, the establishment of a functioning data protection management system was and is associated with a certain amount of effort, but as mentioned earlier, it protects the informational "jewels" in the company, secures values, identifies and controls risks, and avoids penalties. Also, or precisely because data is becoming the "new oil" in the global economy, the European Union has paved the way with its GDPR and serves as a reference for numerous countries and sometimes even global IT corporations, such as Apple. European companies with GDPR compliance thus achieve a certain trust advantage and bonus on the global market.

Will the European data protection model be sustainable in the face of global digitization, or are we helplessly at the mercy of global corporations from third countries?

I think only the coming years can provide a solid answer to this question. Global companies that (want to) serve the European market, among others, cannot avoid compliance with the GDPR. From an international perspective, the "battle" between unrestricted commercial data collection, analysis and utilization on the one hand and the protection of personal data on the other has not yet been decided.

Dear Mr. Spanner, thank you for the interesting interview! ■

ABOUT THE INTERVIEWER:

The interview was conducted by **Dipl.-Ing. Dr. Gerald Hübsch**, long-time CIO, Group Information Security Officer and currently IT Business Angel, in his function as member of the Cyber Risk Advisory Board of KSÖ.

Image: Private | Dr. Gerald Hübsch

Image: Freepik

FEATURE ARTICLE:

The Austrian CyberRisk Rating – **First Experiences of a Critical Infrastructure Operator**

Gerald Hübsch, member of the Cyber Risk Advisory Board, spoke with Walter Fraißler, Head of Information Security at VERBUND AG, and Alexander Mitter, Managing Director of KSV1870 Nimbusec GmbH, about the objectives, benefits and initial practical experience with the Austrian CyberRisk Rating. TEXT: Gerald Hübsch, Walter Fraißler, Alexander Mitter

The innovation idea:

KSV1870's new, Austrian CyberRisk Rating makes the risks in digital business visible & tangible.

The increasing digital penetration of our business activities across industries not only enables high customer centricity, product quality and process efficiency, but in return also increases dependency on digital services and systems. A business interruption, whether due to technical failures or the consequences of a cyber-attack, can cost our companies dearly or even threaten their very existence

So what could be more obvious than analyzing the risks in the entire supply and value chain and making them visible in a rating - as the financial sector has long been familiar with?

No sooner said than done! The Austrian company Nimbusec GmbH, now part of the KSV1870 Group, has worked with top experts from the field over the past two years under the patronage of the Competence Center, Secure Austria to set up an internationally respected rating system for cyber risks. We spoke to Alexander Mitter, Managing Director of KSV1870 Nimbusec GmbH, and Walter Fraißler, Group Manager for Information Security at VERBUND:

Image: Freepik

Q **Dear Mr. Mitter, what problem does the new CyberRisk Rating address, and what advantage does it offer your customers?**

A Our customers, from the smallest business all the way up to the internationally active corporation, must be aware of the risks of digital business transactions, be able to assess them in terms of their impact on their own company, and take appropriate protective measures. Of course, this cannot be done in an isolated operation, but must encompass the entire supply chain. And this is exactly where our CyberRisk Rating helps. It provides structured information on the security status of a business partner and the fulfillment of adequate security standards, based on the state of the art as well as legal requirements. This is precisely where the EU directive NIS - Network and Information System Security - comes in and subsequently

> **From now on, this saves this company from having to answer multiple, mostly slightly different inquiries from potential customers in their bidding processes (...).**

obliges the "operators of essential services" to take special precautions via the national NIS law, including monitoring their supply chain - Third Party Risk Management. Our new CyberRisk Rating can now provide the proof required and accepted by the relevant public authorities. And since we offer this professional service to all companies operating in Austria, both our customers and their suppliers or business partners can rely on it and save themselves a lot of trouble, time and effort.

Q **So how does an interested company get a business-relevant CyberRisk rating?**

A Our client asks us to obtain or report the CyberRisk rating for a specific company in its supply chain. We approach this company - if it is the first time we have been asked to do so - with a structured questionnaire about its state in information security management, validate and evaluate the answers and thus arrive at a rating index.

Similarly, a manufacturer or supplier can also go through this rating process itself at any time, gain insights into its cyber robustness and derive necessary protective measures from it. As a result, this company receives a rating index and - optionally - also a visible label from Cyber Trust Austria.

From now on, this saves this company from having to answer multiple, mostly slightly different inquiries from potential customers in their bidding processes and represents a seal of quality for the cyber security of its products and services.

Q **Dear Mr. Fraißler, VERBUND is, in a way, Austria's backbone in energy supply. Which areas does this cover in concrete terms?**

A VERBUND is Austria's leading energy company and one of the largest producers of electricity from hydropower in Europe. We set the pace for the industry and help shape the future of energy for generations to come. To this end, we are breaking new ground, seizing market opportunities and developing pioneering business models and services for our customers. VERBUND trades in electricity in twelve countries and generated annual sales of around €3.2 billion in 2020 with around 2,900 employees.

In the past three years, information security has become even more important in our company. All aspects of cybersecurity maturity are being further developed and driven forward as part of the "Information Security Master Plan".

Since 2021, the threads of IT, digitization, information security and Telekom have come together in a holding area headed by Thomas M. Zapf and in the Board of Management area of Achim Kaspar.

The increasing threats from cyber attacks (no matter by which actors), the requirements of business processes and customers, and the rising regulatory requirements are our drivers in the field of information security. The NIS Act has triggered an additional and significant in-

> **A key point in these requirements, incidentally also in the ISO 27.001 standard, is security in the supply chain; for this, the CyberRisk Rating is a very good solution in our view.**

Image: VERBUND | Storage power plant

Foto: VERBUND | Übertragungsnetz

vestment in cybersecurity for many companies that provide essential services to society. A key point in these requirements, incidentally also in the ISO 27.001 standard, is security in the supply chain; for this, the CyberRisk Rating is a very good solution in our view.

Q **Now that we know the main reasons for using KSV1870's CyberRisk Rating - how did you fare during implementation, and what benefits do you derive from it as VERBUND?**

A In the course of our "Information Security Master Plan", we took a close look at Third Party and Vendor Risk Management. Our first approach to this topic was what has generally been considered best practice up to now: classifying suppliers and then evaluating a large proportion of them by sending out a questionnaire.

Such a questionnaire ideally follows a general structure - but ultimately consists of a large number of questions, which are often not easy to answer. After receiving of a completed questionnaire, it is then a matter of checking and verifying it.

With this generally accepted procedure, we have identified two problem areas: First, we would send such a questionnaire to a relatively large number of suppliers, receive queries from them that have to be answered, and finally have to check the answers at least for plausibility. In a word, we have a lot of work to do on our side. On the other hand, many suppliers have more than just us as customers. If other customers - which is to be expected - also intensify their supplier risk management, then the suppliers receive a number of very similar, but not identical questionnaires to answer. Result: A great deal of work is also generated on the supplier side.

PROJECT ORGANIZATION

That's why we immediately rated the idea of Alexander Mitter's team to develop a standardized "Cyber security rating" as excellent. One of the major challenges was to bring the slightly different and often very extensive requirements of different operators down to a common denominator. In very intensive discussions in the Advisory Board, we ultimately succeeded in compressing these requirements into a very manageable number of questions. In the same way, a process for the rating procedure and the necessary plausibility check of the answers was outlined.

OPERATIONAL BENEFIT

Ideally, we request the CyberRisk Rating for a new supplier, which is already in the database and therefore available immediately. If it is not yet available, the supplier must complete the questionnaire once. We can trust that the answers and thus the rating have been quality checked. For the majority of suppliers, the rating will be sufficient as a criterion - for a few particularly critical suppliers, it is in any case a good basis for a further audit. In this ideal case, the advantages in terms of effort and processing time can be seen very quickly on our side - but also on the supplier's side.

CHALLENGES

The biggest challenge with the first inquiries about the rating was probably that it was completely new and therefore still unknown. Suppliers therefore had an - understandable - reluctance and queries before the rating was carried out. I am confident that this hurdle will become much lower as awareness of the CyberRisk Rating increases. In addition, the intended amendment of the NIS regulation - keyword "NIS 2.0" - will increase the circle of companies affected by the NIS law many times over.

We thank you for the interesting conversation!

Image: VERBUND | Fresh Migration Aid in Carinthia

VERBUND has been listed on the Vienna Stock Exchange since 1988; 51 % of the share capital is owned by the Republic of Austria.
With its subsidiaries and partners, VERBUND is active in everything from electricity generation and transmission to international trading and sales. With Austrian Power Grid AG and Gas Connect Austria GmbH, VERBUND owns 100 % and 51 % respectively of the Austrian transmission grid operators for electricity and gas. With its strategy "With our power into a green future", VERBUND aims to live up not only to its economic but also to its social responsibility as Austria's leading energy company.

As the largest electricity company in Austria and as the leading hydropower plant operator in Bavaria
VERBUND is aware of its responsibility. It reliably supplies millions of people with vital electrical energy. The plants are managed efficiently and the environment and climate are protected in the generation of electricity. The extent to which crisis management and resilience are VERBUND have been established was not only demonstrated in the past two years. ■

ABOUT THE PEOPLE:

Image: VERBUND | Walter Fraißler

DIPL.-ING. DR.
WALTER FRAISSLER

Dipl.-Ing. Dr. Walter Fraißler holds a doctorate in mathematics (Vienna University of Technology) and has been an executive at VERBUND for many years. His career path took him from the IT department to the role of assistant to the Chairman of the Managing Board to responsibility for the group organization and to the position of CIO and Head of IT Services. Over the past four years, he has been tasked with establishing and developing the area of information security across the Group. Together with his dedicated team, he is pursuing these goals in the interests of his company's increased cyber resilience and Austria's security of supply.

Image: Private | Alexander Mitter

MAG.
ALEXANDER MITTER

Alexander Mitter is Managing Director of KSV1870 Nimbusec GmbH. After graduating from HTL and studying business administration, he gained practical experience in a globally active technology company before joining the management team at Nimbusec and managing the market launch of the security product range. Subsequently, he developed the founding idea for a "CyberRisk Rating Austria" and now - as a member company of the KSV1870 Group - manages its market launch.

Image: Private | Dr. Gerald Hübsch

DIPL.-ING. DR.
GERALD HÜBSCH

Dipl.-Ing. Dr. Gerald Hübsch, long-time CIO, Group Information Security Officer and current IT Business Angel, conducted the interview in his capacity as a member of the KSÖ Cyber Risk Advisory Board.

Image: Freepik

INTERVIEW:

Austria's seal of quality for cyber security

The Cyber Trust Austria label gives organizations the opportunity to visibly demonstrate to the outside world that they have implemented essential minimum security measures for cyber security and that the topic has a corresponding priority in the organization. The Secretary General of the Kompetenzzentrum Sicheres Österreich (KSÖ), Dr. Alexander Janda, and Managing Director of Cyber Trust Austria, Dr. Thomas Stubbings, in conversation.

TEXT: Alexander Janda, Thomas Stubbings

Dr. Janda, why did KSÖ decide to develop a seal of approval for cybersecurity?

DR. JANDA: Cybersecurity is a challenge that does not stop at a company's borders. Critical infrastructure companies in particular need a reliable and secure supply chain. Therefore, it is and was our concern to make the reliability and security also visible to the outside world in a seal of approval.

Dr. Stubbings, as Managing Director of Cyber Trust Services GmbH, you are responsible for awarding the seals of approval to applicants, according to the KSÖ scheme. Who are your target groups?

DR. STUBBINGS: Basically, any company that works with IT and electronic data in any way is a target group - and who doesn't these days? Anyone who operates computers and networks or has them operated and uses them to process and store data, whether their own and/or those of customers, must pay attention to the cyber hygiene of their infrastructure and processes. In their own interest and that of their customers and partners.

Why in the interest of customers and partners?

DR. STUBBINGS: Close networking with our customers and partners creates more opportunities for attackers and also malware to move from one company to the next. This is even easier than penetrating from the outside - because companies that do business with each other usually trust each other. I would just like to remind you of NotPetya, the biggest cyber incident in history to date: The malware entered the network of a supplier directly via a software update.

Dr. Janda, how does KSÖ assess the current risk situation for Austrian companies, in general and in particular with regard to supplier risk?

DR. JANDA: Over the past year and a half, cybercrime has increased by more than 25%. In addition to government institutions and a growing number of private individuals, the main targets are companies. The attackers make no distinction between a large bank and a small, medium-sized business. At the same time, the amount of damage is constantly rising - in many cases, a cyber attack threatens the very existence of a company.

> **The attackers make no distinction between a large bank a nd a small, medium-sized business.**

Image: Redtenbacher | Alexander Janda

DR. ALEXANDER JANDA
KOMPETENZZENTRUM
SICHERES ÖSTERREICH (KSÖ)

Image: Privat | Thomas Stubbings

DR. THOMAS STUBBINGS
CYBER TRUST AUSTRIA

Do you share this opinion?

DR. STUBBINGS: Yes, we are seeing more and more attacks on SMEs in Austria. Cases are constantly making the news: from Palfinger to Salzburgmilch to the incident the other day in Upper Austria, in which an IT operator "took down" 34 of its customers. Unfortunately, today it is no longer enough to look at one's own cybersecurity; one must also make sure to work with trustworthy and secure companies.

Dr. Janda, why did KSÖ enter into a cooperation with KSV1870 for the implementation of the CyberRisk Rating? What makes this partnership so special?

DR. JANDA: As Austria's leading creditor protection association, KSV1870 has been a reliable partner of the Austrian economy for many years. With its high orientation towards innovation, KSV1870 is the ideal partner to map the dynamics of technological developments in the field of digitalization, which manifests itself among other things in the challenge of cyber security, in a new CyberRisk Rating.

Dr. Stubbings, could you please explain briefly what the main differences are between the standard label and the gold label?

DR. STUBBINGS: The Standard Label stands for basic safety. The underlying 14 criteria are designed in such a way that any organization - even a very small one - can achieve them with manageable effort. Basic security does not cost vast sums of money. But you do have to take a focused look at the subject and invest a little time. There is really no longer any justification for any company not meeting the basic security criteria - it should be as self-evident as washing your hands or locking up your apartment. The Gold Label sets a higher standard - it is aimed primarily at larger companies that operate in sensitive areas and have already done more for their cybersecurity. Incidentally, a third-party audit is also required for the Gold Label, while a validated self-declaration is sufficient for the Standard Label.

What is a "validated self-declaration"?

DR. STUBBINGS: This means that the company itself provides information on how the individual requirements are met within the company. A validator, an expert with relevant experience, then checks this information for completeness, plausibility and consistency with other information. If there are any ambiguities, the validator has the opportunity to ask questions. The validation step brings a lot of quality to the process.

Dr. Janda, in conclusion, what are your further plans regarding the Cyber Trust Label?

DR. JANDA: We got off to a very good start with our Cyber Trust Label and received a lot of positive feedback. Now we want to address as many companies as possible in Austria and win them over for this new quality seal. Acceptance by the Austrian market is then a prerequisite for taking this

issue to the European stage as well. Cyber challenges do not stop at national borders. We want to take the know-how we have developed in Austria and with Austrian partners to our neighboring countries and beyond to the European Union. At the same time, we will continue to develop the content of our scheme in order to keep pace with security developments and challenges. ■

For more information on Austria's cybersecurity quality seal, visit **www.cyber-trust.at**

3 questions about the Cyber Trust Label with Geldservice Austria

Q **Why did you acquire the Cyber Trust Label?**

A Geldservice Austria has acquired the Cyber Trust Label because it allows us to document our high level of security. Our customers and partners are forced by various regulations and requirements to obtain appropriate confirmations, which we can provide in a practical way, especially in the area of cyber security with the Cyber Trust Label.

Q **What is the importance of cybersecurity seals of approval for you?**

A Particularly in a complex and rapidly evolving topic such as cybersecurity, the use of qualitative and meaningful seals of approval is a significant facilitator. The confirmation of a defined security level by independent third parties creates the (trust) basis for business relationships in a simple way.

Q **What do you look for in your own suppliers with regard to cyber security?**

A As Geldservice Austria ensures Austria's cash supply on behalf of the parent company Oesterreichische Nationalbank, a correspondingly high level of security is required. The availability of relevant certifications is therefore a basic requirement, and coordination with the OeNB's IT experts is very close, especially in the area of cyber security.

THE
CYBERRISK
RATING
by KSV1870

Contact information

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

www.cyberrisk-rating.at

nimbusec
Part of KSV1870