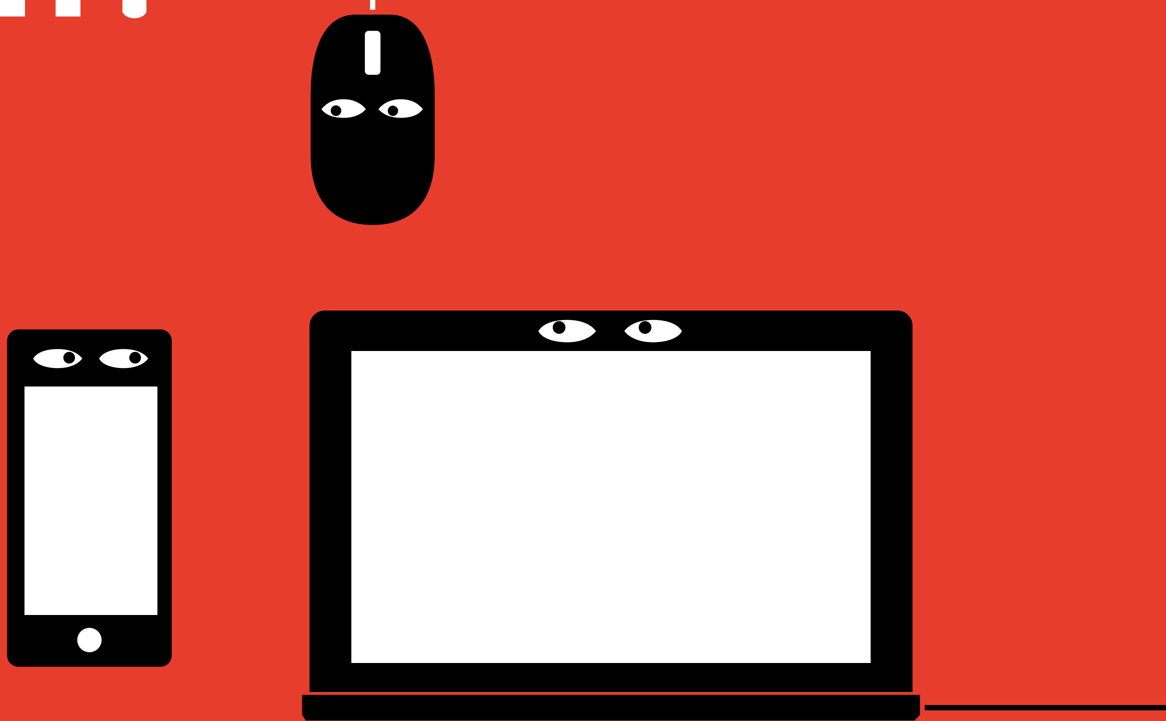
IT Security

Know-how for the Corporate Management

Do you trust in the security of your IT?



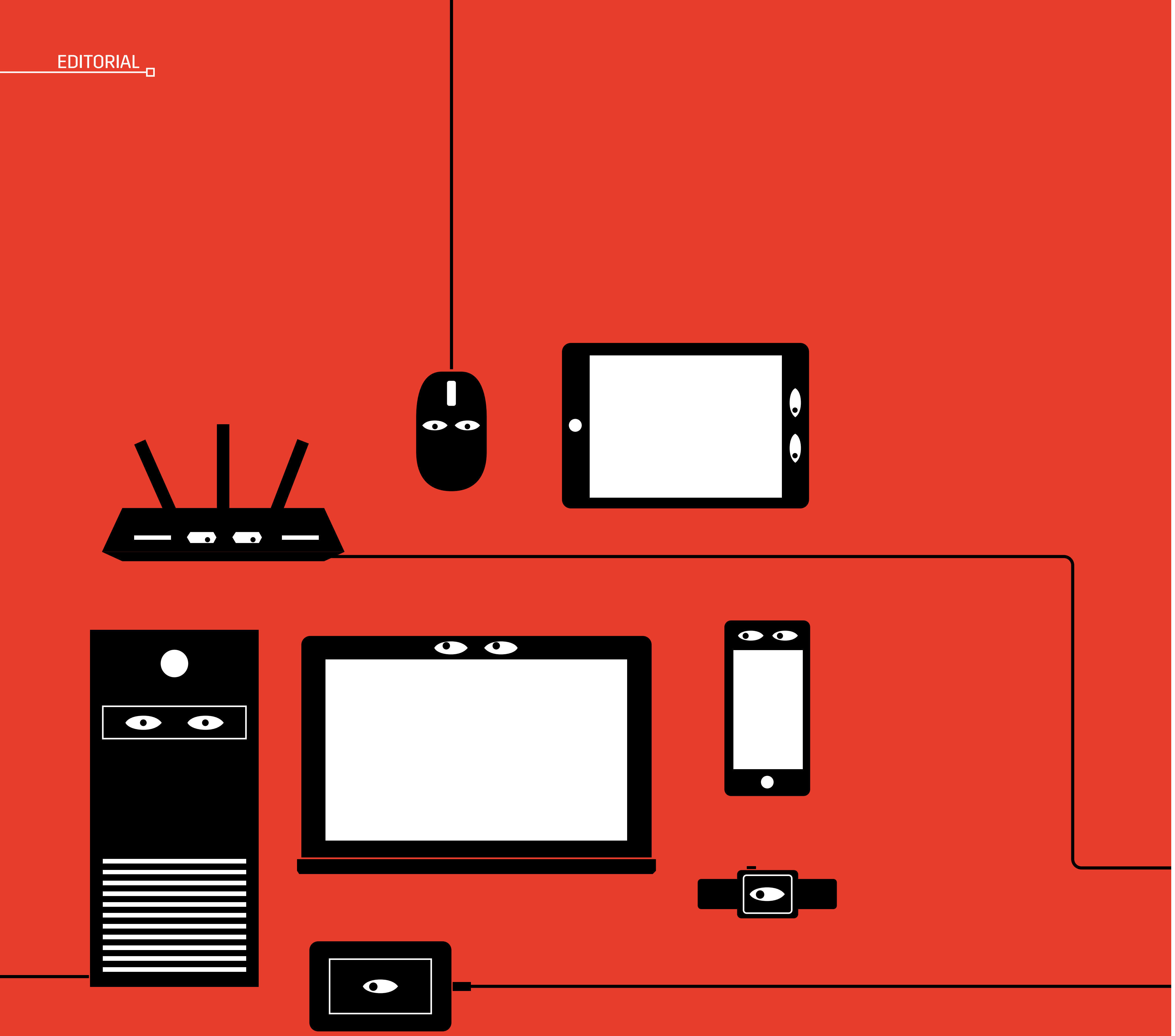
powered by RADAR SERVICES

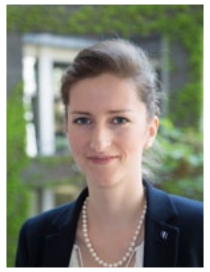
EDITION 2

©Stanislav Jenis

It's a matter of trust.

We live in a connected world in which trust in the security of IT is essential. In an in-depth interview about their own IT security measures, the management of RadarServices, Europe's market leader in IT security monitoring tells us about the cornerstones of their trust in IT security.





Dear Readers,

Do you trust in your IT's security? In the eyes of many, this fundamental question is more relevant than ever following numerous headlines about espionage, data theft and ransomware attacks.

In conversations with experts, we tackle the question of what enterprises in all types of industries can do to strengthen their own as well as their clients' trust in their IT. In detail, we ask about the foundations on which trust can be built, both objectively and subjectively.

We lend a particularly attentive ear to those that ought to know especially well: the managing directors of Europe's largest cyber defence centre. They protect enterprises from cyber attacks and know when IT security measures actually provide protection of corporate values and when they don't. Europe-wide initiatives are growing steadily, promoting common approaches to the protection of our values. More than any other, the European Cyber Security Organisation (ECSO), represented by Luigi Rebuffi, is pulling essential strings. On the other hand, Maximilian Schrems has created a fait accompli when he filed a motion against Facebook before the European Court of Justice – and won. We asked these opinion leaders to share their current estimations.

An important basis of trust is also one's own knowledge of state-of-the-art technology and security options for IT. In this regard, Eric Maiwald, Vice President of IT research specialist Gartner, shared his overview of technology at an international level with us.

Finally, "evidence of trust" may also be provided in the form of certifications that build trust because many experts in different fields go to great lengths to (further) develop them. DDr. Stampfl-Blaha and Dr. Karl Grün of Austrian Standards allow us to peek behind the curtains.

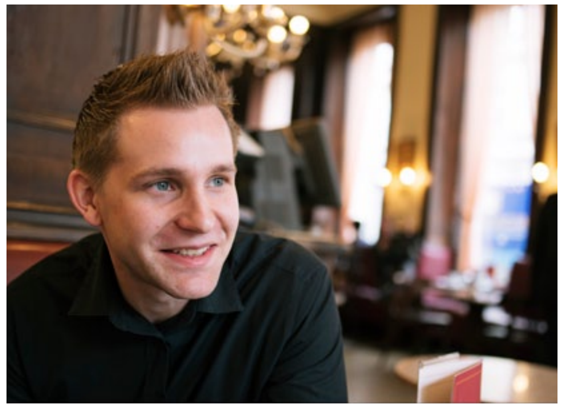
With the publication titled "IT Security – Know-how for the Corporate Management", we aspire to win back trust in IT security and present measures for everyone to take in order to increase the general feeling of security. Because in the end, trust forms the basis for accepting technological progress in our society.

With this in mind, I hope you will enjoy reading this issue.
Isabell Claus, publisher

Evidence of trust: The importance of ISO standards for IT security **P. 24**

"Responsibility creates trust!" **P. 8**

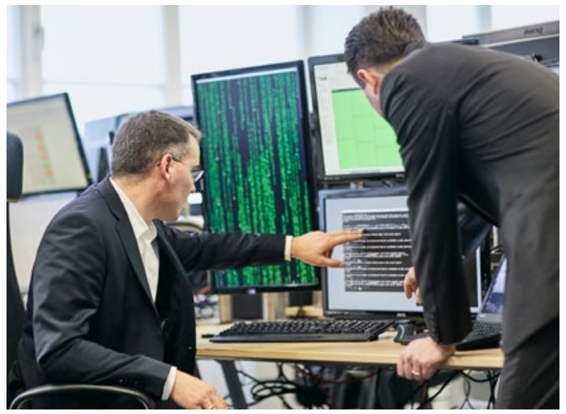
DON'T PANIC! PLAN! – The EU General Data Protection Regulation is shaping our future **P. 26**



"Trust is really being put to the test at the moment" – Interview with Max Schrems **P. 16**

"We need to overcome the challenges ahead together" – Interview with Luigi Rebuffi, Secretary General of ECSO **P. 12**

2017 – where do we stay in IT security and what do we need to focus on? **P. 18**



Behind the curtains of security technologies research: "New models are tested like vaccines" **P. 20**

CONTENTS

©Stanislav Jenis

"Responsibility creates trust!"

The management of Europe's leading managed security services provider explains the factors on which trust in a company's own security is based.

TO USE TODAY'S and, especially, tomorrow's IT applications and services, we must be able to trust IT security. However, the virtual world lacks those physical security mechanisms we know from the "real" world. Security measures that lead us to trust that the brakes in our cars work or that the plane that carries us to our destination won't crash cannot simply be copied.

Users themselves are hardly able to review important functions such as system integrity, protection against abuse, protection of personal data and protection against digital attacks. Thus, trust plays an important role in the perception of IT security, how people handle IT, which companies they entrust with their data and of which they become customers. Media reports of cyber attacks against large enterprises, authorities, entire industries or countries affect our trust. This is how the public learned that foreign governments collect and analyse massive amounts of data without the consent of the individuals, enterprises and public institutions concerned. In doing so, these governments collaborate with large technology companies or – as is the case with the USA – even force them to cooperate by taking legal action.

Ever since this information was made public, people's trust in the safety of their personal data and IT security has palpably – and understandably – diminished.

This lost trust in IT security needs to be won back. It forms the basis for economic growth and further development of the global digitalisation trend in all spheres of life. It decreases transaction and control costs, promotes trade and growth, the development of the financial markets as well as acceptance of and demand for new technologies. Hence, it is a prerequisite for long-term business success in all industries.

How to win back trust

Considering solutions in terms of economic efficiency only usually ignores the trust factor and reduces the contribution of technology to a superficial cost-benefit calculation. Whether this approach can actually be effective in the event of a sudden attack is highly doubtful.

Hence, we asked IT security experts Harald Reisinger, Thomas Hoffmann and Christian Polster of RadarServices, Europe’s market leader in IT security monitoring, about their trust in RadarServices’ own security, and about the factors justifying that trust.

Harald Reisinger: First of all: yes, I trust in the security of our IT! My reasons are, among others, a number of measurable elements, such as the daily reports of our own continuous IT security monitoring process, the best practices and processes established by us that would be effective in an emergency situation, our rigorously evaluated security components, the compliance we live by and our organisational security measures and awareness trainings. Of course, my trust is also built on our many years of experience and our expert knowledge. We know what happens on the attacker’s side, which naturally gives us an edge in knowledge compared to enterprises whose core business is not purely focused on making their own and their clients’ IT safer every day on an international level.

Christian Polster: Trust in our IT security is also based on our constant desire to research and develop IT security detection and evaluation modules. We employ a large team of developers for the security software used by our clients and, of course, also by ourselves. We use this IT security monitoring technology to control the different gateways for cyber attackers in large and medium-sized enterprises 24/7. By developing this technology inhouse we make sure that, first, there are no back doors in the software, and, second, it is governed by an appropriate quality assurance system. This is what sets us apart from providers that only deploy third-party technologies, lack in-depth insight in the coding and are unable to determine whether quality assurance and testing were sufficient or not.

We are convinced that quality assurance begins with the research with regard to new trends and processes required in the future to provide a basis for the functioning of a software. Carefully chosen methods that lead to the desired results, a theoretical and objectively justifiable basis and extensive practical testing are the pillars of development provided by our Research Department.

The following development processes rely on well-defined best practices and standards for secure coding our employees must strictly comply with. A multi-layered approach, i.e. the control of the entire development process, is a significant quality feature. During the coding process, we believe in the principle of dual or even triple control. Then, our well-staffed Quality Assurance Team conducts both automated and manual tests on several levels using live data to check for potential negative effects of code changes. Another must-have during the development process is a continuously updated documentation. Finally, our Research, Development and Testing Teams regularly attend further training.

Thomas Hoffmann: Security is based on trust and I fully trust the security of our IT! The awareness that we not only use the right tools for IT security but also use them correctly is deeply rooted in our company. For any tool is just as good as the person who uses is. This is why we regularly review the overall concepts of all our security measures in the big picture. There is no such thing as an uncoordinated “instant solution”. Moreover, we make sure that enough and, above all, highly qualified experts have an eye on our security every day.

They configure the tools, master every little detail of them and always adapt them to the current circumstances. Another factor that increases my trust is the ongoing further training that is part of the job of the security intelligence experts. This way, we are all set for potential attackers.

What do you recommend enterprises from all industries that wish to increase trust in their IT security?

Harald Reisinger: Review all technologies and the companies that provide them and consider them in the overall context. For many enterprises from non-IT industries, this issue is some kind of black box, an unratable risk that some of them are willing to take to a certain degree, while other enterprises grow more and more reluctant to do so. What counts here are hard facts and extensive assessments that each organisation should perform for themselves.

Thomas Hoffmann: Providers have different standards for their own responsibility, clarity and transparency. Management priorities, the importance of compliance, the awareness among employees and their commitment to “living” IT security are essential.

You should strongly consider these elements when choosing new security technologies. An objective set of criteria is as important as the subjective amount of trust put in the people in charge at the provider. Personal rather than virtual contact. Speaking the same language rather than putting up language barriers. A continuous flow of information rather than stagnating processes. All these elements create a high level of trust, and they are decisive factors where time is of the essence.

Christian Polster: Further reference points are the manufacturers’ locations and jurisdictions, corporate business ratios and goals, recommendations and quality marks such as “made in Europe”. Certifications and a certain product’s status in a manufacturer’s product range as well as expectations with regard to a manufacturer’s competence in the relevant business sector matter as well. Reviewing a provider’s “fitness” in the area of data security is also a great indicator for the value they attribute to actual IT security and data protection. The EU’s new General Data Protection Regulation ensures that Europe sets the highest standards in terms of international requirements. Moreover, comprehensive national legislations as well as certification possibilities and requirements make Europe’s IT comparatively safe. Security providers should know these requirements like the backs of their hands, and observe them. This is what forms the foundation of trust in their solutions.

CONCLUSION

There are plenty of objective and subjective criteria to consider when reviewing the security of our IT and the efficiency of the technologies and resources deployed for it. Evaluating these criteria enables you to develop well-founded confidence and win back lost trust. Enterprises that purchase security technologies to protect the data of their clients are in great demand. They should conduct regular and comprehensive reviews of the security of their IT, both for their own and their clients’ benefit. An effort that will certainly be rewarded with valuable trust by their clients.

iStock.com/artJazz

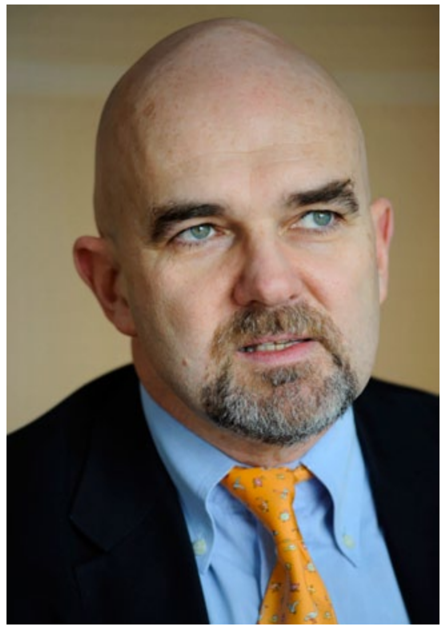


Image: ©ECSO

"We need to overcome the challenges ahead together"

The European Cyber Security Organization (ECSO) was founded in 2016 in Brussels. ECSO members include a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries. **Luigi Rebuffi, Secretary General of ECSO, explains the challenges ahead for Europe with regard to cybersecurity.**

Where do you see the biggest challenges for European businesses with regards to IT security in the upcoming years?

The booming digitisation of the European society, industry and economy has enabled a new industrial revolution setting the scene for a European Digital Single Market. Driven by emerging and fastly advancing digital technologies such as Internet of Things (IoT), 5G, cloud computing, data analytics and robotics, these changes have significantly increased the freedom and prosperity of society and businesses but they also have exposed some important vulnerabilities.

Cyber-attacks are frequently making the headlines putting entire businesses under the spotlight, damaging the trust of users in the services they provide. These ever-evolving attacks, not only in their methods but their targets too, have put legislative powers under public pressure to take decisive actions to protect the citizens / consumers and safeguard critical infrastructures to avoid potentially dramatic disruptions of essential services such as energy, transport, etc. which are more and more digitised. Based on the latest 2016 threat landscape report produced by the European Union Agency for Network and Information Security (ENISA) and other studies, hackers have concentrated on the following types of attacks:

- Distributed Denial-of-Service (DDoS) attacks by infected IoT devices;
- Extortion attacks or also called ransom cyber attacks targeting phones, laptops, company computers, and other devices that are a daily necessity. Radware's Global Application and Network Security Report 2016-2017 revealed that 49% of European businesses confirmed cyber-ransom was the number 1 attack motivation in 2016, an increase of nearly 100% from the 25% recorded in 2015;
- Attacks on critical infrastructures of key sectors such as transport, health, energy, e-government, finance and telecoms.

Moreover, the European industry continues to face obstacles specific to R&I (scattered funding due to a lack of transnational approach and global European investments strategy; innovation led by imported ICT products) and the development of the market (persistent fragmentation; market dominated by suppliers from outside of Europe contributing to a strategic supply chain dependency) that hinders its competitivity. These challenges are coupled to low investments (weak entrepreneurial culture), a lack of experts in cybersecurity and a low European political will curtailed by national sovereign prerogatives.

These challenges require industrial actions (research and innovation, vulnerability checks, investments, etc.) supported by political measures and adequate legal and operational frameworks at Member States and European level (e.g.: implementation of the NIS Directive, common industrial policy, investments, funds, regulations / directives).

Against this background, the European Commission has taken the initiative to set up a Public-Private Partnership on cybersecurity focusing mainly on addressing research and innovation in Europe and supporting key industrial measures to protect the Digital Single Market and boost the competitivity of the industry.

Which are among the most urgent issues ECSO intends to tackle in the near future?

In its industrial policy, ECSO has identified several challenges. ECSO has set up 6 working groups (standardisation, certification and labelling; market deployment and investments; sectoral application of cybersecurity solutions; support to SME and regions; education and training; R&I). Each of them is addressing one or several essential industrial measures geared to tackle the following strategic and operational objectives:

- Protection of critical infrastructures from cyber threats by increasing the use of trusted cybersecurity solutions in the different sectors (energy, health, transport, etc.)
- Regulate the use of massive data collection to increase overall security
- Increase European digital autonomy
- Improve security and trust of the whole supply chainStärkung der Wettbewerbsfähigkeit
- Boost investments in economic areas where Europe has a clear leadership
- Support SMEs and their innovations
- Increase competitiveness
- Development of innovative technologies and services to tackle evolving threats
- Support the development of education programmes and professional trainings

Since the signature of the contract of the PPP with the European Commission, ECSO has been intensively working on contributing to the European initiative on creating a framework for cybersecurity certification of ICT product and services. Also, ECSO has consolidated its Strategic Research and Innovation Agenda and will continue to support the implementation of strategic research in Europe beyond the scope of the H2020 Framework Programme and even after the end of the contract with the European Commission.

There is a need to restore trust in the security of IT since suspicion turned into certainty that foreign governments collect and analyze massive amounts of data without the knowledge of the individuals, corporations or public authorities concerned and since large-scale cyber-attacks regularly hit the news. What is done on the EU level to restore trust?

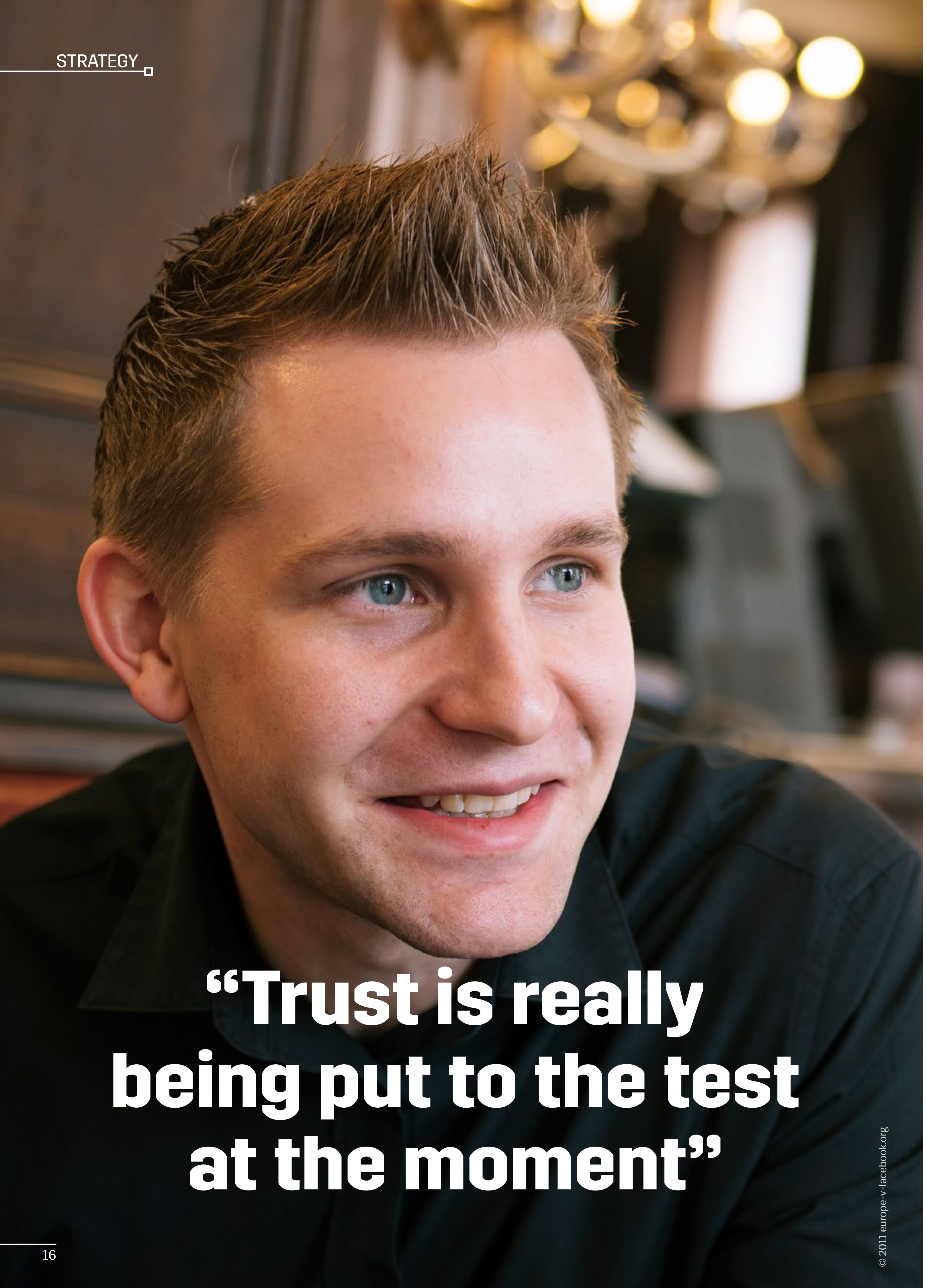
Trust between the user and the provider of a service and between the citizens and their government is paramount. As previously mentioned, this trust has been increasingly hampered by cyber-attacks targeting business and strongly re-considered by citizens following infamous revelations from whistle-blowers. The protection and management of data are at the heart of the issue. To repair and reinforce this trust, we need to achieve the following goals:

- **Rebuild and strengthen collaborations** between users, public administration and industry addressing the most urgent issues identified previously. This is the reason why ECSO is an umbrella organisation gathering various stakeholders both from the private sector (industry, research centres, universities, operators) and public sector (national and regional public authorities), structured around a unique governance model that encourages and facilitates such a cooperation. This mix of stakeholders gives ECSO members the chance to tackle together, and for the first time, the majority of issues linked to cybersecurity.

- **Increase public awareness** campaigns on the potential harmful consequences of digitalisation and how to protect their personal data. ECSO has set several actions to improve digital skills early on in education systems and provide necessary programmes to train experts.

- **Invest in the development, manufacturing and deployment of trusted cybersecurity solutions** and systems to be used at strategic levels of the supply chain and reach a certain degree of digital autonomy when it comes to safeguard critical infrastructures.

- **Improve interoperability** supported by common standards and certification mechanism. When setting up the Public-Private Partnership, the European Commission has announced its commitment to exploring the possibility of creating a framework for cybersecurity certification of ICT products and services which could be complemented by a European labelling scheme for the security of ICT products.



“Trust is really being put to the test at the moment”

Maximilian Schrems, lawyer, author and privacy activist from Salzburg, filed a motion against Facebook in front of the European Court of Justice. The judgement ended the transnational Safe Harbour agreement between the EU and the USA. In our interview, he talks about the current international situation.

How important is the users’ trust for further development of innovative technologies?

Currently, we see many people who don’t feel comfortable using the new technologies. Those are hard to grasp for the individual and complex to an extent that they can hardly be judged by the person concerned. In my opinion, trust is really being put to the test in the digital world at the moment. The topic itself is very complex and difficult to understand. Particularly in the B2B sector, I can already see that trust is playing an increasingly crucial role. Because for customers and business partners it becomes increasingly important to have a safe and reliable environment. In the past, companies were rather following the approach of “the cheaper, the better” with regard to various IT solutions, but now they pay closer attention to the associated compliance costs, which are often not taken into account. This is a development that can increasingly be observed at the moment.

Create trust, enjoy trust – what can and should companies do to establish trust?

I think that they have to create transparency and be proactive. Because trust is an important prerequisite for successful business relationships. In order to distinguish themselves from their competitors, it is necessary to disclose information and make clear statements. In my opinion, this is the only way to create trust. Comprehensible statements instead of “creative descriptions” are absolutely necessary to give the average user an understanding of the complex topic.

Can you name any companies you would praise for the data security they practise?

I think that “practised” data security is not part of the mainstream yet. There are indeed some start-ups dealing with this topic. However, this sector primarily relies on open source, which does not constitute a financial incentive. Some companies currently try to take this approach, but as far as I can see those are still niche solutions.

In your opinion, how will data security as a basis for trust in technology develop in Europe and the USA until 2025?

I don’t see lots of major developments in the USA at the moment. Currently, all cases are being brought to an end legally as effectively as possible. Market movements are primarily caused by European users, who increasingly ask for anti-cloud solutions. With effect from May 2018, a new data protection regulation will apply in Europe. If companies violate these regulations, they will have to face high fines. For companies, these can amount up to EUR 20 million or 4% of the global group turnover. The degree of punishment really differs greatly from the currently applicable regulation. Until now, the fines were just too low to justify the high compliance costs that would have been necessary for complying with the rules.
I believe that many companies will only wake up at a later point in time. But it will be difficult to find experts in this field. The persons responsible at the companies are under high pressure, because in terms of compliance they will definitely have to expect longer lead times for implementation. I have already noticed law firms with expertise in the field of data security becoming very popular. This will definitely intensify over the coming months. Considering the large number of changes and the increased threat of punishment, it will be interesting to see how the companies will prepare for the new EU data protection regulation.

2017 where do we stay in IT security and what do we need to focus on?

An interview with Eric Maiwald, Managing VP of Gartner's Security & Risk Management Team within the "Technical Professionals" research area.

Mr. Maiwald, what is the status quo of IT security in organizations today?

Security remains a top concern of business and IT leaders, and cybersecurity is increasingly visible in the mainstream media. Data breaches — including theft of personal information, intellectual property, and government and business emails and documents — are still the greatest worry. But other types of incidents and issues, including ransomware, denial of service, and general abuse of computerized systems (for example ad-click fraud) are affecting organizations of many types and sizes. Security demonstrations of IoT insecurity also add potential consequences and show a change in the nature of digital business risk — safety is now a greater cybersecurity concern.

At the same time security and risk teams remain under pressure to "say more 'yes' with less." Security teams are under ever more pressure to be better business enablers but are still often not included at the start of a project. Faced with project time constraints, security teams — especially those with few resources — find it easier to follow a compliance and audit checklist than to spend time on extensive risk analysis and control selection. Third-party security assessments and risk management are proving particularly time-consuming, and strong security personnel are hard to find and retain (with industry estimates of up to 1.5 million cybersecurity job openings by 2019).

Increased regulation and oversight are almost unavoidable given the prominence of security breaches and the general public's views on privacy and security. However, the specificity and breadth of those regulations are hard to predict, and unfortunately, many organizations struggle to interpret what "taking a risk-based approach" means versus using stricter compliance checklists.

As in previous years, 2017 will remain challenging in terms of balancing these calls for better risk-based approaches with the capacity to execute security and risk practices.

Which areas of IT security do IT leaders need to address particularly?

There are four areas I would say.

Number one: Privacy and data confidentiality remain the top security challenge for most organizations. But ransomware attacks and IoT hacking demonstrations show increased needs in the areas of integrity and availability to maintain safety and reliability.

Number two: Because persistent attackers will inevitably circumvent preventive controls, detection and response capabilities are critical. Newer approaches, such as machine learning and deception, promise to lessen the amount of human effort required to execute these capabilities.

Number three: The "traditional" ways in which some security controls are implemented become less effective in modern IT environments. But underlying concepts such as limiting administrative privileges, configuration hardening, malware controls and vulnerability management are still vital.

And number four: Infrastructure-level security changes in mobile and cloud environments, and is often implemented with a lack of granularity to address modern attacks. Adding more host, application and data security is a necessity — especially for cloud, mobile and IoT use cases.

What do you recommend organizations in the view of the above?

Three things are vital in my view.

First, take an increasingly evidence-based approach to cybersecurity technology and practices. Unless required by compliance mandates, avoid "best practice" controls if they have questionable effectiveness or are too expensive for the amount of risk reduction they deliver.

Second, strengthen basic security, such as malware controls and vulnerability management practices, and take advantage of built-in security on mobile, cloud and other technologies. Combine these with add-on security products for greater visibility and control.

And third, invest in detection and response practices and technologies, with an increased focus on monitoring entity and user behavior. Leverage machine-learning approaches to reduce manual effort, and strongly consider deception technologies to improve the accuracy of detection.

Behind the curtains of security technologies research:

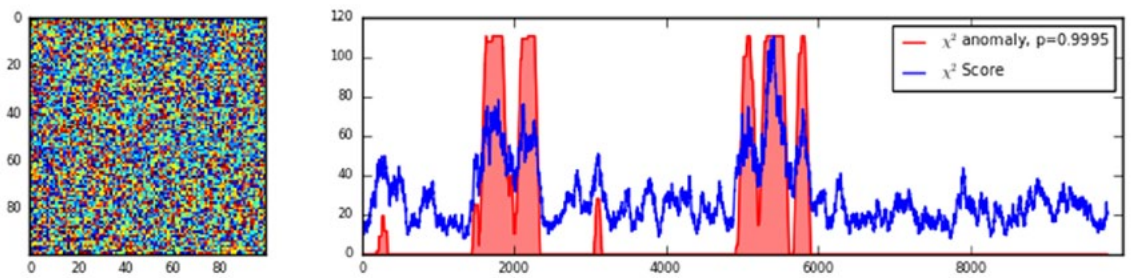
New models are tested like vaccines

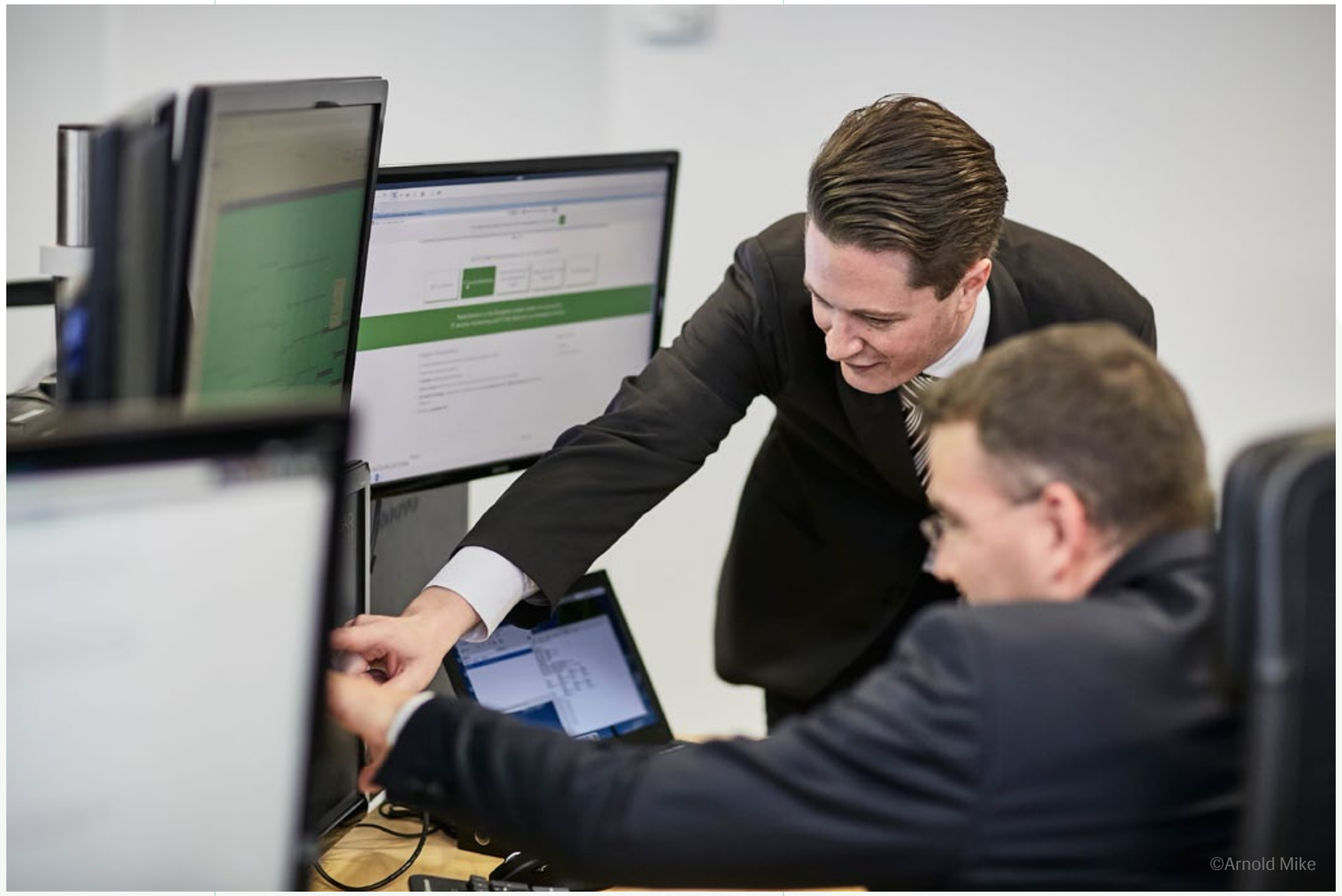
IT security technologies have their origins in the investigation of statistical models. They detect anomalies in huge data volumes. A glance into the research department of RadarServices, Europe's leading provider of continuous IT security monitoring, shows how models are tested before they are put into practice.

©Arnold Mike

1. Determining the research area
Quick detection of anomalies in the IT landscape is the prerequisite for identifying current cyber attacks in time. However, with large enterprises, big data is an issue. To find the needle in the haystack, we must first have an idea of what that needle looks like. "Our Security Intelligence Team provides us with this information. They are the experts that keep an eye on everything that happens in our clients' IT landscape every day. Let's say you want to determine a certain pattern in large data volumes and ask us to create a model for that purpose," says Andreas Esders-Kopetzky, RadarServices Research. "IT security officers of companies who are our customers may come up with similar ideas. Such concerns from all kinds of industries are brought to our attention. When we know what to look for in large data volumes, we test all eligible models from our experience, but also from completely different areas like econometrics or bioinformatics. Different customers have different

Pattern detection in large data volumes – how visualisation helps render statistical models accountable





demands, so we create different solution processes, accordingly,” Esders-Kopetzky continues. “Our Research Team picks up outside stimuli and develops them further. Additional patterns are evaluated, and everything is aggregated to form a superordinate strategy, in order to improve the entire IT risk detection and analysis process,” explains Christian Polster, responsible for research in the management of RadarServices.

2. The validation process

The Research Team’s efforts are aimed at finding a valid model to produce correct results in many different cases. “For example, our colleagues from the Security Intelligence Team might first provide us with an extract of data. We know that these data have interesting patterns. However, the systems in use did not detect those patterns automatically. So we consider a model and first evaluate what is unusual about these data. During the subsequent validation process, we try to identify where exactly anomaly and non-anomaly correlate,” Esders-Kopetzky explains. An analysis is carried out to determine whether the error rate (false positives and false negatives) of the chosen model is acceptable. Once this comprehensive analysis and evaluation process has been successfully completed, the new model is accountable and, thus, reliable. To assure highest quality levels, this process might take months and the efforts of an entire research team with a wealth of experience in many fields.

3. Risk assessment before practical application

The model has been chosen and its adequacy tested with numerous data sets. To assess the risk of non-detection of anomalies despite detailed tests, a risk analysis is conducted in a separate step. Once again, it is evaluated whether the model in use detects enough anomalies without generating too much “unnecessary data” (false positives and false negatives). “Risk assessment is carried out in similar ways in each statistical scenario: for example, when a new vaccine is developed, its efficiency is weighed against any risks it harbours. We use the very same approach for risk assessment before we deploy a model,” Polster states.

4. Visualisation of model decisions

Understanding every detail of models and their limitations is important to win even the statistics experts’ trust in correct functionality. A key method here is a visualisation of model decisions. This is a valid option for models as long as they are not too complex. Models with high complexity, however, require comprehensive testing. These tests are used to demonstrate the inflow of data and visualise the anomalies actually shown by a model in a large number of scenarios at the end of the day. “These extensive validation, testing, risk analysis and visualisation processes are necessary to convince our security intelligence experts, our management and ourselves on a permanent basis that the model we use has been put to the acid test, and that we can rely on it to raise an alarm when it is meant to. Only then do we put it to practice and consider our work successfully completed.”

EVIDENCE OF TRUST

The importance of ISO standards for IT security

Images: ©Austrian Standards

Left: Dr. Karl Grün, Austrian Standards

Right: DDr. Elisabeth Stampfl-Blaha, Austrian Standards and International Organization for Standardization (ISO)

Certifications are an important means to convince clients of the quality of a company's own products and processes. The ISO/IEC 27000 series published by the International Organization for Standardization is particularly significant for the IT security sector. DDr. Elisabeth Stampfl-Blaha, Vice President Technical Management of the International Organization for Standardization (ISO) from 2012 to 2016 and Managing Director of Austrian Standards and Dr. Karl Grün, Director Standards Development at Austrian Standards allow us to gain an interesting glimpse in the development and importance of standards.

Standards create trust. What are key components during the development process of standards that ensure their wide acceptance and the level of trust they build?

Stampfl-Blaha: Decisive factors to build trust in standards – and I mean standards in all fields – are the high level of recognised quality of their contents on the one hand, and the way these standards come into existence on the other. We are talking about an open and completely transparent process, which is a non-negotiable prerequisite for standards to be accepted. By openness and transparency, I mean that everybody can file a request for a project to develop a standard, and you can contribute to this process for as long as you are interested in, affected by or familiar with the issue at hand. Important is that the committee that works on the project is well-balanced (i.e. no interest group should dominate another), because this is not about overruling, but about convincing, about reaching an agreement. Two other factors are important as well: First, you can make a contribution even if you are not in the committee, for example by giving your opinion on project proposals and drafts – something everybody is welcome to do. And second, you can always share your real life experience and suggest improvements. What is more: Austrian Standards, a recognised organisation with decades of experience and a worldwide network guides and manages the process and ensures fair play. This is quite essential. Because standards are continuously gaining importance in the area of R&D as well, paving the way to the market for innovations and preventing the development of incompatible isolated applications.

How important will it be for enterprises in all industries to obtain certifications for IT security in the years to come?

Grün: Nowadays, IT security is rated very highly, and looking at the rapid increase in electronic data exchange, also beyond company borders, it will gain even more significance. The growing, almost exhaustive digitalisation of all spheres of life and the entire working environment renders IT security indispensable. Accordingly, enterprises must be able to proof that they do everything they can to make their IT applications and IT infrastructure safe. Here, a certification is essential – it is a confirmation by an independent authority that a security management system that complies with internationally recognised standards has been implemented and is being continuously improved. This facilitates collaboration with clients and business partners and creates mutual trust.

What do you recommend to enterprises that want to effectively establish an ISMS (information security management system)? What is decisive when working with such a system on a daily basis?

Grün: First of all, the top management needs to become aware that IT security is a key priority – this should happen before anything else. Next, information must be obtained as to which legal and contractual requirements exist in terms of data protection and IT security and which standards currently apply, i.e. the ISO/IEC 27000 series must be taken into account. These standards universally apply to enterprises and organisations of all kinds and sizes. Then, the ISMS needs to be developed following these guidelines. As soon as everything is in order, certification must be applied for. It goes without saying that this is not a closed process, but – quite literally – a daily challenge. Because the threats change and grow, too.

DON'T PANIC! PLAN!

The EU General Data Protection Regulation is shaping our future

In May 2018 requirements with regard to data protection measures will increase massively for organizations. The EU General Data Protection Regulation determines that they have to protect the human behind the data record. If this does not work out, organizations are facing high penalties.

The EU-GDPR protects a wide range of persons. Organizations that process data of EU citizens in their systems are governed by this regulation. Solely anonymous data, which is data whose personal origin is no more identifiable, shall not be fall under the scope of this regulation. At the same time, the EU-GDPR protects a wide range of persons. All organizations that process data of EU citizens in their systems are governed by this regulation. They do not need to be located in the EU or use a server of the EU.

Companies have to face the challenges now. Five To Dos are in focus.

1. PRIORITIZE YOUR TASKS.

Develop a basic concept for fulfilling the requirements based on the status quo of your company. Prioritize your To Dos. Consult legal and IT security experts in the course of planning in order to interpret the individual requirements of the EU-GDPR correctly.

On the one hand your company shall be protected from cyber attacks, on the other hand, the people whose data you are processing, shall be provided with rights and established processes. A third strategically important step is the establishment of security measures in product and process design.
Focus all your measures on improving the trust in you and your IT of clients, employees and stakeholders.

2. SECURE YOUR IT.

The central article 32 EU-GDPR states: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."

So it is clear that the legislator has no specific security measures defined but rather recommends appropriate risk-based technical and organizational measures.

Compare your potential risks with actual IT security measures and analyse possible gaps. Develop the ability to detect and react to cyber attacks quickly in order to minimize potential damages. Evaluate the tool Security Information & Event Management (SIEM) for a proactive monitoring of your IT security.

3. FOCUS ON DETECTION.

The EU-GDPR stipulates reporting obligations to supervisory authorities in case of security incidents within a maximum of 72 hours after becoming known. Also persons concerned have to be informed in case the incident is expected to have a high risk for personal rights and freedoms. In case an organization is not fulfilling its duties, high penalties (up to 20 million Euros respectively 4% of the group sales) have to be paid. Considerable reputational damages are associated with it.

These scenarios have to be prevented on the one hand and on the other hand documentation measures as well as functioning emergency processes (Best Practices) need to be followed.

The Security Information & Event Management (SIEM) therefore fulfills various tasks. Moreover, the usage of tools such as Network-based Intrusion Detection Systems, a continuous vulnerability management and Advanced Threat Detection for Email & Web shall be verified.

The goal of this risk management modules is to establish a comprehensive protection mechanism for the organizational IT, including the parts that process personal data.

4. MAP YOUR DATA.

In future persons have to explicitly agree to the use of data. It must be disclosed to them how and where the data is used. The agreement is always earmarked, meaning for specific processing purposes. Declarations of consent can also be withdrawn. Organizations have to keep up with this sustainably.

Moreover, each person has the right to receive clear and easily comprehensible information with regards to the processing of data. Also the transfer of this data into systems of other service providers has to be possible upon request without a problem.

A complete overview is required of all the IT assets in use and the personal data that is made available by them. Thereupon processes are established that allow persons their rights of insight, data portability and cancellation.

5. PRIVACY BY DESIGN & DEFAULT.

The EU-GDPR requires companies to address data protection proactively. It also requires that technology which it uses in the data processing shall be “designed” in order to be data protection friendly by nature and does not allow for specific data processing or at least does so securely. Data Protection by Default means that automatically the strictest data protection settings are applied if a client purchases a new product or service.

Besides that Data Protection by Design means that services and business processes and personal data shall be treated in the sense of the EU-GDPR. IT departments have to integrate data protection and privacy in the entire system respectively process life cycle in order to have proof in case of doubt.

In the future also your product and process design shall be aligned based on data protection issues. Evaluate the possibilities and requirements for such changes in time and across departments.

News, events and information from RadarServices

About us

RadarServices is Europe‘s leading technology company in the field of Detection & Response. In focus: The early detection of IT security risks for corporations and public authorities offered as a Solution or a Managed Service. The cutting-edge, inhouse-developed technology platform is the basis used for building up a client’s Security Operations Center (SOC) or it is used in combination with our expert analysts, documented processes and best practices as SOC as a Service. The result: Highly effective and efficient improvement of IT security and IT risk management, continuous IT security monitoring and an overview of security-related information throughout the entire IT landscape of an organization.

RadarServices is headquartered in Vienna, Austria. Customers are medium-sized and large corporations with up to 350,000 employees as well as authorities. Worldwide SOCs allow proximity to our customers.

RadarServices awarded with the “Deloitte EMEA Technology Fast 500 Award” 2016 and the “Cybersecurity Excellence Award” 2017

With a sales growth of 1,270% in the period between 2012 and 2015 RadarServices is one of the Top 100 of the fastest growing technology companies in Europe, the Middle East and Africa (EMEA). For this reason the company was awarded with the “Deloitte EMEA Technology Fast 500” Award and achieved position #69 in this competition. Another award followed in early 2017: RadarServices was elected as finalist for the international Cybersecurity Excellence Awards 2017. The jury, which consisted of renowned industry experts, evaluated the candidates with regards to their future and market potential as well as their track record and in the course of their evaluation praised RadarServices for their particularly excellent innovative strength concerning the fight against cybersecurity risks.

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

500 Technology Fast 500 2016 EMEA WINNER Deloitte.

iStock.com/shulz

CYBERSECURITY WORLD

©Arnold Mike

THE GRAND OPENING

The Cybersecurity World was recently opened in Vienna. The press conference was followed by an exciting evening for 200 invited guests: the in-house IT security experts provided them with first-hand information about how cyber attackers act, how they choose their targets and how real-life attacks on multinational enterprises are carried out. Guided tours of the building offered an overview of the measures enterprises should take nowadays to protect themselves and what they can do to avoid becoming victims. The guests had many questions and received detailed feedback. A glance into Europe's largest security operations centre (SOC) topped off the experience of the visitors to Vienna's newest "IT security centre".

The guests included representatives from politics, economy and science. Among them: Luigi Rebuffi, Secretary General of the European Cyber Security Organisation (ECSO), Prof. Dipl.-Ing. Johann Haag, Academic Director IT Security of St. Pölten University of Applied Sciences, and Reinhard Schwendtbauer, member of the management board of Raiffeisen Landesbank Oberösterreich (photo left to right).


©Arnold Mike

ABOUT THE CYBERSECURITY WORLD

The Cybersecurity World is a worldwide unique place. In this building in the heart of Vienna IT security is made to come alive. It is the home of Europe's largest Security Operations Center (SOC). Here today's and tomorrow's challenges for IT security responsibles in companies as well as the current state of research and innovation in this sector are illustrated on 2,000 sqm.

Specifically designed rooms highlight this subject from various perspectives: This way the visitors of the "hackquarter" can slip into the role of the hackers. What are their possibilities, the strategies and thoughts? How does the hacker choose its attack targets? In the "safe room" it is presented how companies can detect cyber attacks in real-time and thereby drastically can minimize damages.

Who is one step ahead of whom? The technologies on the one hand and the human intelligence on the other hand determine whether it is the hacker or the attacked company who is more successful. The tools and skills of both parties are the center of attention in the Cybersecurity World.

One-to-one meetings with and lectures by internationally renowned IT security experts are completing this world, in which everything revolves around IT security.

VISIT US!

Experts share their knowledge in the field of IT security. Every month, guided tours provide insights into our daily work. The one-hour tours address all IT security responsibles. Dive into the world of IT security at four stations: experience the perspective of a hacker, familiarise yourself with modern possibilities to detect and explore attacks, development and quality assurance of security software and the current state of security research. The Cybersecurity World is located at Zieglergasse 6 in 1070 Vienna.
For current tour dates, please refer to www.cybersecurityworld.org.

EUROPEAN ROOTS, WORLDWIDE APPLICATION

» 100% IT security made in Europe
» 170 countries where our customers are active
» 4 continents where we provide our services
RadarServices continues to expand.

RadarServices expands its team in Germany

Early in 2017, Dr. Thomas Kirsten joined the RadarServices team in Germany. The new Head of Sales is domiciled in Munich and coordinates the company's activities all over Germany from this location. Among others, he is in charge of implementing the "KRITIS Secure" strategic partnership between RadarServices and Controlware, the renowned German system integrator. Using combined risk detection modules – log data analysis, vulnerability analysis, data flow analysis, among others – KRITIS Secure unites RadarServices' extensive IT security monitoring with Controlware's services for security incident processing and emergency response, especially for critical infrastructure operators.

Support is provided to German companies in all sectors by RadarServices' Security Intelligence experts both from Europe's largest Security Operations Center in Vienna and from the new Security Operations Center situated in Berlin.

Your contact:

Dr. Thomas Kirsten, RadarServices
+49 (69) 244 34 24 655
Thomas.Kirsten@radarservices.com

RadarServices continues to expand in Switzerland and Liechtenstein

The intensity and complexity of attacks on IT infrastructures of companies and public authorities increase, the battle against them becomes harder every day. With the Cyber Security Alliance, FL1 – Telecom Liechtenstein and RadarServices offer a suitable solution to medium-sized and large companies as well as to public authorities.

Based in Liechtenstein, one of the safest data locations in the world, the Cyber Security Alliance is able to provide the leading solution in terms of technology: a combination of cutting-edge software made in Europe, the latest hardware tools and comprehensive expert know-how available on site. The services are provided in such a way that security-relevant customer data will never leave the customers' premises – for security-relevant data should never be found outside the company to which they belong.

Your contacts:

Thomas Hoffmann, RadarServices
+43 1 92912710
Thomas.Hoffmann@radarservices.com

Markus Hofbauer, FL1 – Telecom Liechtenstein AG
+423 235 56 94
Markus.Hofbauer@telecom.li

Cyber security insurance: Overall solution provided by Funk Group Germany and RadarServices

Funk, Germany's largest owner-managed independent insurance broker and risk consultant, is a renowned expert with regard to insurance solutions, risk management, asset protection and preventive solutions for companies and entrepreneurs. In collaboration with RadarServices, Funk offers cyber security insurance contracts to companies in all sectors. While RadarServices provides the technical expertise for on-going cyber security risk evaluation, Funk has the matching insurance solution.

Your contacts:

Harald Reisinger, RadarServices
+43 1 92912710
Harald.Reisinger@radarservices.com

Michael Winte, Funk Group
+49 (40) 35914 582
M.Winte@funk-gruppe.de

EU General Data Protection Regulation: RadarServices cooperates with leading law firms in Germany and Austria

On 25 May 2018, the EU General Data Protection Regulation will enter into force. It requires organisations to put a stronger focus on the individual behind a data set. The individual's data must be protected and the principle of accountability is to be applied. Organisations unable to implement the EU-GDPR will have to face high fines.

RadarServices provides technical advice on this subject to customers and interested parties. In collaboration with leading German and Austrian law firms, RadarServices now offers integral expertise with regard to the EU-GDPR.

Your contacts:

Harald Reisinger, RadarServices
+43 1 92912710
Harald.Reisinger@radarservices.com

Austria/Vienna:
Dr Axel Anderl, LLM (IT-Law), Nino Tlapak, LLM (IT-Law), DORDA Rechtsanwälte
+43 1 5334795-23
Axel.Anderl@dorda.at, Nino.Tlapak@dorda.at

Germany/Düsseldorf:
Dr. Philip Kempermann, LL.M., Heuking Kühn Lüer Wojtek
+49 211 600 55-166
P.Kempermann@heuking.de

RadarServices Cybersecurity Specialist appointed as OSCE special representative

Asif Safdary, IT-Security Analyst at RadarServices, was appointed as special representative of the OSCE Chairperson-In-Office on Youth and Security at the beginning of 2017. His tasks in this position are to present the social, economic and political issues of juveniles in the OSCE area to the OSCE chairmanship. In regular conferences ideas and guidelines are developed. Asif Safdary is primarily responsible for the issues of cybersecurity and cybercrime.

This new role follows his other commitments in the political and social sector. Besides his job at RadarServices the born Afghan is also chairman of the Afghan student association and promoting networking, support and integration in this position. As ambassador of integration of the Austrian integration fund he is going to schools and presenting his own integration history and hereby acting as a role model for young people. The 23-year-old who came to Austria nine years ago is additionally holding another chairman function at the START Alumni association. START is a scholarship program which supports dedicated juveniles to graduate from school with a high school certificate.

RadarServices CFO & CSO Christian Polster personally congratulated Asif Safdary to his nomination as OSCE special representative with the following statement: "We are very impressed and proud of your dedication which is continuously and sustainably promoting essential food for thought and improvements in the 'real' as well as the virtual world."

Would you like to subscribe to or unsubscribe from the magazine "IT Security – Know-how for the Corporate Management"? The magazine is free of charge.
Simply email to publishing@radarservices.com or call 0043 1 929 12710.

Imprint

About RadarServices Publishing

RadarServices Publishing publishes articles, reports, studies and magazines on the subject of IT security. It is our aim to provide an insight into the experience of industry experts, and to pass on know-how relating to IT security acquired from intramural and extramural research to companies, public institutions and other organisations. We actively draw on co-authors from academia and business to promote knowledge about current trends in the area of IT security among the general public and, in particular, among corporate executives and politicians. RadarServices Publishing is part of RadarServices.

About this publication

The publication contains general information only. RadarServices and/or its affiliated companies are not providing any expert consultation services with this publication. Nor does this publication serve to replace any such expert consultation, and should not be used a basis for business or investment decisions or actions. Neither RadarServices nor its affiliated companies shall be liable for losses incurred by an individual as a result of relying on this publication.

About RadarServices

RadarServices is Europe's leading technology company in the field of Detection & Response. In focus: The early detection of IT security risks for corporations and public authorities offered as a Solution or a Managed Service. The cutting-edge, inhouse-developed technology platform is the basis used for building up a client's Security Operations Center (SOC) or it is used in combination with our expert analysts, documented processes and best practices as SOC as a Service. The result: Highly effective and efficient improvement of IT security and IT risk management, continuous IT security monitoring and an overview of security-related information throughout the entire IT landscape of an organization.

Address

Cybersecurity World
Zieglergasse 6, 1070 Vienna
Phone: +43 1 9291271-0
publishing@radarservices.com

Overall responsibility and editor: Dr Isabell Claus T.: 0043 1 9291271-33
Graphic design: Thomas Fadrus
Photographs/image credits: Stanislav Jenis, Arnold Mike, ECSO, Gartner, europe-v-facebook.org, Austrian Standards, istockphoto.com

RadarServices Smart IT-Security GmbH
Cybersecurity World
Zieglergasse 6
1070 Vienna, Austria

Know early what's happening.

SOC as a Service,
IT Security Monitoring,
Security Information & Event Management (SIEM),
Advanced Cyber Threat Detection and
IT Risk Detection
as Next Generation Managed Security Services

The early warning system for your IT.