

Facing global challenges

Christina Schlichting from Volkswagen about the group-wide information security program




Health check for an IT network

Performance check-up in the network of the German Federal Institute for Drugs and Medical Devices

From zero to hero

How to make "Zero Trust" not only a buzzword



24  Learning from critical infrastructures: Secure IT (not only) for CRITIS

National

- 4 Performance check-up in the network of the German Federal Institute for Drugs and Medical Devices: Health check for an IT network

International

- 7 New secunet easygates in Poland: Witamy w Polsce: Polish border police further expand automated border control
- 8 EU regulation on Schengen visas: Digital help for the paper visa

Title

- 9 Empirical values at Volkswagen: IT security strategies facing global challenges – how to counteract them?

Science

- 12 Industry 4.0: “Real innovation can happen at the E4TC”

Technologies & Solutions


- 16 Study by secunet and techconsult – IoT projects in companies: External expertise often required
- 18 How to make “Zero Trust” not only a buzzword: From zero to Hero
- 21 IT and cyber security in the automotive environment: “Complex automotive architectures require uncompromising hardware and software security”
- 24 Secure IT (not only) for CRITIS: Learning from critical infrastructures
- 27 Secure cloud computing: secunet acquires SysEleven and expands its cloud portfolio

News in Brief

- 28 Tap-proof voice communication: SINA Communicator H wins iF Design Award
- 29 Secure and trustworthy patient care: secunet participates in the SEMECO project
- 30 VIT supports projects between science and industry
- 30 Strategies against skills shortage: secunet is training again

Service

- 31 Dates – October to December 2022
- 31 Imprint

Klaus Hardy Mühleck in interview: “Complex automotive architectures require uncompromising hardware and software security” 



Dear reader,

Just as the pandemic has eased, we have had to live with another crisis of global proportions since February of this year. The Russia-Ukraine war is primarily causing much human suffering and is also leading to political and economic uncertainty worldwide.

As a cybersecurity company, we are often asked what impact the situation has on the security of digital infrastructures in the state, economy and society. The question has two aspects. The first is the concrete threat situation, and this is rated as “elevated” by the German Federal Office for Information Security (BSI) in the current context. The second aspect is the effectiveness of the protective measures. Here, it is worth taking an unagitated look – because in this respect, not much has changed at all. The protective mechanisms that work against cyber threats and ensure digital sovereignty are still the same. The changed world situation does not force a change of strategy in cyber security; instead, the previous path should be pursued even more consistently. This is what we do together with our customers.

However, this does not mean that we have nothing new to tell. In May 2022, we made the largest acquisition in our company’s history to date and took over the cloud and Kubernetes specialist SysEleven. With this acquisition, we have added another cornerstone to our cloud portfolio and now offer a comprehensive, customised, secure cloud offering for public authorities, administrations and security-sensitive companies. For us, this is a forward-looking development, because the future of IT lies in the cloud, and the same applies to IT security.



This secuvie shows some of what else is on our minds in the world of cyber security. As always, our customers and partners as well as external experts have their say. The last category includes our cover article, which I am particularly pleased about. In it, Christina Schlichting describes how she manages a Group-wide information security program at Volkswagen AG.

I hope you enjoy reading this issue. Stay healthy!

A handwritten signature in black ink that reads "Axel Deininger". The signature is fluid and cursive, written on a light-colored background.

Axel Deininger

Performance check-up in the network of the German Federal Institute for Drugs and Medical Devices

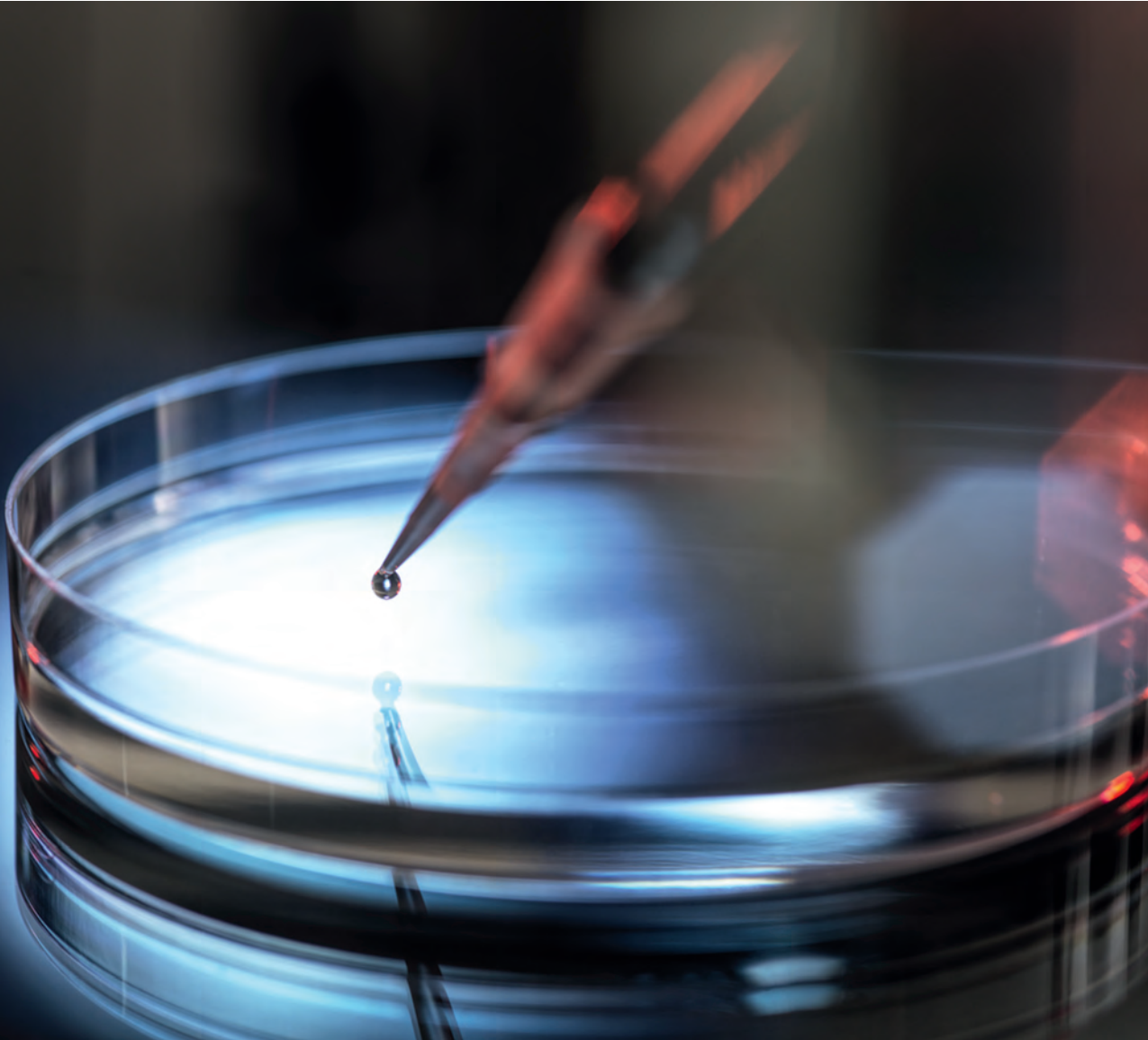
Health check for an IT network

The German Federal Institute for Drugs and Medical Devices (BfArM) employs around 1,350 staff – including doctors, pharmacists, chemists, biologists, computer scientists, lawyers, engineers, technical assistants and administrative staff. They work on the approval and the improvement of the safety of medicinal products, the risk identification and assessment of medical devices as well as the monitoring of the traffic in narcotics and basic substances. In addition, the authority provides high-quality information for all areas of the health care system. The primary goal of all measures is to increase the safety of medicinal products and thus of patients.

The employees of the BfArM are increasingly carrying out these tasks on the move or from their home offices. For this purpose, the authority uses an IT network secured with SINA. In autumn 2021, this network had to be put through its paces, as inexplicable performance fluctuations were making it difficult to work from outside the institute. For this purpose, secunet carried out a so-called SINA check-up together with its partner consistec.

Many federal authorities that work with sensitive or classified information, such as the BfArM, use the Secure Inter-Network Architecture SINA. With its numerous interlocking security components, it ensures, for example, that third parties cannot read data when users have dialled into the authorities' network via a mobile Virtual Private Network (VPN). With the specially secured SINA Workstation in laptop format, it makes no difference whether employees are in the office, at home or on the road. In addition, SINA networks and components are designed in such a way that, despite their high level of security, they are easy to operate, scale to tens of thousands of users and demonstrate high performance.

However, at irregular intervals, the BfArM observed unexplained drops in performance when employees were on the move or working from their home offices. For the users, this manifested itself, among other



With the Secure Inter-Network Architecture **SINA**, employees of public authorities or companies can securely handle sensitive or even classified information – inside or outside the office. SINA solutions combine security and user-friendliness. A regular SINA check-up can help to maintain the performance of the secured network at all times. In this process, secunet consultants check the SINA environment with regard to the functioning of all relevant components. Misconfigurations and incompatibilities are proactively detected and can be remedied. A final report not only documents the current status, but also contains the appropriate recommendations for action. In this way, a need for optimisation can be identified at an early stage, for example with regard to hardware utilisation and performance.

things, in Outlook disconnections or difficulties with video conferencing. This can have many causes. At the network level, the users' internet connection, the federal government's networks and the actual public authority network of the BfArM are particularly relevant. In addition, there are other elements such as hardware resources, performance losses due to virtualisation or docking stations. Due to the complexity of the overall setup, it was also likely that one or more of the potential causes interacted for each incident.

The reasons for the performance fluctuations could therefore be hidden deep in the entire setup. It was thus important to narrow down the search. Analysis data was required so that the various potential causes could be separated from each other and hence also investigated. And this is where the SINA check-up came into play, which secunet carried out together with consistec.

The German Federal Institute for Drugs and
Medical Devices in Bonn 



Flight recorder for the network

For this purpose, the experts used the caplon Network & Service Monitoring tool in addition to the usual conceptual-heuristic analysis by the SINA consultant. In close cooperation between the project manager on the BfArM side and the SINA consultants as well as consistec, a measurement technology was installed in the network with the caplon appliance, which makes it possible to record the network traffic completely and without loss, even at high data rates. The raw data obtained is kept for permanent circumstantial evidence and also offers the possibility to look into the past. In this way, sporadically occurring problems can be analysed or the data can be used for forensic analyses. Thus, the tool is a kind of flight recorder for the network.

All connections between the various systems are analysed and visualised so that technical problems and performance slumps can be detected at an early stage. This enabled the secunet and consistec team to scrutinise the entire infrastructure secured with SINA. In total, caplon analysed 57 terabytes of data in 85.5 billion packets. In order to comprehensively fulfil data protection guidelines, the caplon privacy protection module was used in addition to non-disclosure agreements (NDAs). This allows data to be pseudonymised online so that no conclusions can be drawn about personal data or critical infrastructure data.

After the investigation period of six weeks, the BfArM received a final report of several pages at the end of November 2021, which is similar to the test report of an independent institute such as the TÜV. In addition to the analysis results, this document also contained practical recommendations for action to further optimise the network setup.

“The project with secunet and consistec helped us a lot with the performance analysis,” says Jan Franzen, Head of Information Technology at BfArM. “We were able to narrow down the problem and also gained certainty that our SINA installation was working properly.”

Marcel Göhler, Team Leader Key Account Management at secunet, sums up: “The SINA check-up is a great way to help customers maintain their SINA solution. The customer receives proof of the security and performance of the system, and errors can be detected at an early stage. The caplon appliance can be a useful addition to this in order to analyse the system in more depth. The cooperation with consistec was very collaborative and successful – we look forward to further joint projects.”



Marcel Göhler
marcel.goehler@secunet.com

consistec Engineering & Consulting GmbH is an owner-managed, medium-sized company with over 20 years of experience in the field of network monitoring. With the caplon product line – made in Germany – consistec monitors the quality, availability and performance of IT/OT infrastructures and business-critical applications.

This gives companies a comprehensive overview of all processes taking place in the network as well as full control over the network from an operational, planning and security point of view.

New secunet easygates in Poland

Witamy w Polsce: Polish border police further expand automated border control


Less waiting time, easy handling and relaxed travellers: secunet easygates have been in use in Poland since 2018 and facilitate border controls there. Now the partnership with Enigma, the responsible security company, is being expanded, and secunet easygates are also in use at Gdansk Airport.

In total, secunet is already securing six airports in Poland: Wroclaw, Gdansk, Krakow, Poznan, Warsaw-Modlin and Warsaw-Chopin. Several easygate generations are now in use – and thanks to the modularity of the systems, components of the new generation function without any problems with the previous generations. A special feature of the easygate installations in Poland is the central control of all Automated Border Control (ABC) systems via server systems at the Warsaw location.

“Since 2018, we have been working together with secunet to support the Polish border police and relieve the officers at the country’s most important airports. Automated processes at border control simplify and accelerate the processes for passengers as well and ensure an uncomplicated travel experience. We look forward to expanding our partnership with secunet”, says Radosław Frydrych, Vice President of the Management Board at Enigma.

But how does secunet easygate actually work? In simple terms, it visually and electronically checks the authenticity of electronic identity documents such as passports and ID cards. To do this, the system reads the facial image from the chip in the electronic identity document and compares the biometric data with the actual appearance of the traveller, which is captured by a facial image camera.

Globally, more than 450 secunet easygates are already in use at international airports today – in addition to Poland, for example, in Germany, Austria, the Czech Republic, Hungary, Lithuania and Bulgaria. By the way, “Witamy w Polsce” means “Welcome to Poland”.

 secunet easygates (here at Sofia Airport, Bulgaria) will soon also provide automated border control at Gdansk airport.



Michael Schwaiger
michael.schwaiger@secunet.com



EU regulation on Schengen visas

Digital help for the paper visa

As of 1 May 2022, new rules apply to Schengen visas. The analogue documents must now be supplemented by a digital seal and are only valid in such a “combination package”. The secunet Digital Seal Signer was developed for this purpose. It offers secure travel management and provides authorities such as embassies with the necessary protection against fraud. There is still a transition period until November 2022, when the digital seal will become mandatory for all visas.

Until now, visas have only existed on printed paper or in passports. But that is about to change. The reason is that the analogue version alone is too insecure and too susceptible to fraud. Blank papers, on which authorities and embassies print the individual travel data, were coveted by fraudsters and therefore had to be elaborately stored in safes. That is why the EU Commission decided on 30 April 2020: We need a digital seal to supplement the analogue version. This applies to all visas as of May 2022.

Protection against fraudulent scams

The solution for this is the secunet Digital Seal Signer. Information such as the date, the authorised length of stay and the passport number are digitised by a 2D barcode and signed by the respective authority. This barcode is generated by a secure web service and then the visa can be printed. This creates an additional technical safeguard to the print version. Estonia and Iceland are the first partners to use the Digital Seal Signer.



Andreas Hellrung
andreas.hellrung@secunet.com

Empirical values at Volkswagen

IT security strategies facing global challenges – how to counteract them?

By Christina Schlichting, Head of Group Information Security Programs & Projects (GISP), Volkswagen AG

The entire business world is undergoing a digital transformation. No industry is exempt from this. The Volkswagen Group is pushing ahead with modernisation and digitalisation at full speed, in its products and the entire ecosystem. As Group Information Security, our tasks and responsibilities are essentially focused on corporate IT with many interfaces, including to software that is installed in the vehicle, or on the customer interface, which plays an important role in retail, for example.

We have twelve brands, 120 production sites, more than 670,000 employees in the Group, 153 countries in which our vehicles are offered, as well as vehicle production. Also part of this are other business areas such as large diesel engines, steam and gas turbines, compressors, battery production, finance, green electricity and much more. This shows the high level of complexity in which we operate with information security.

History

Major projects and programs in IT are the order of the day for us. For example, the Volkswagen Group launched a Group-wide information security program back in 2011.

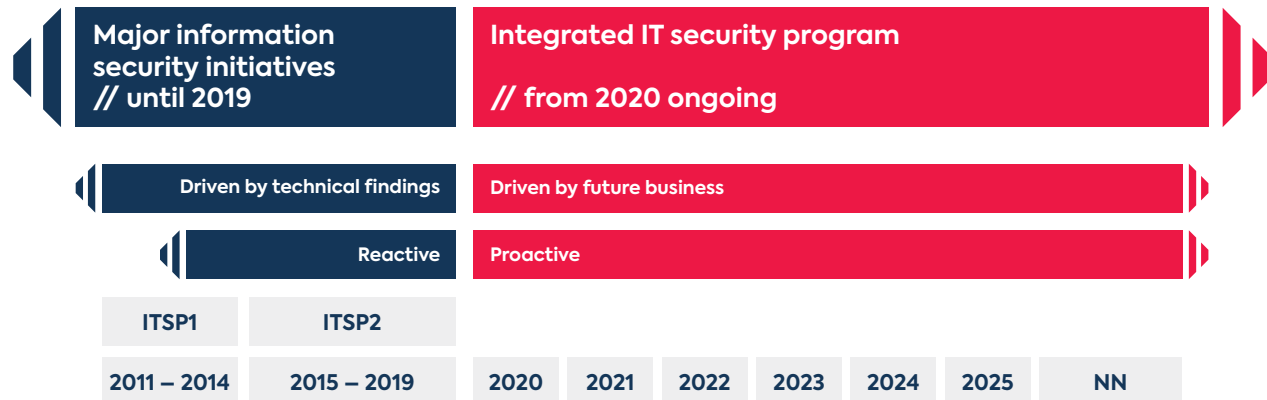
The program included twelve very complex projects and topics, which essentially dealt with increasing the level of information security across the Group, uniform processes, standards and technical solutions. When this program was completed in 2019, PwC attested:

“The major IT security initiatives form the basis for raising the level of information security throughout the Group, the harmonisation of standards and tools, and the deployment of centralised solutions across the brands and companies.” (PwC audit ITSP2)

And this was to continue, albeit under slightly adjusted parameters and framework conditions:

- Shorter, faster intervals – based on annually redefined focal points
- Continued cross-brand and cross-regional cooperation
- Even more synergies between the brands
- Easy adaptability to enable a well-orchestrated rollout

IT security initiatives and projects in the Volkswagen Group

**Procedure**

The Group-wide information security committee consisting of the CISOs (Chief Information Security Officers) of the brands jointly analyses the threat radar of the Information Security Forum (ISF) every year and derives corresponding risks. These risks are used to define measures that are then prioritised and incorporated into the Group Information Security Program (GISP).

The program includes different focal points each year. The projects are staffed by different brand representatives and a promoter who, as a member of the CISO panel for the program, represents the entire panel and does not only have the interests of his brand in mind.

The projects are controlled by a cross-sectionally organised Global Program Management (GPM) with reporting, finance, communication, quality assurance and risk management.

Since the beginning of 2022, another cross-cutting issue has been added: the rollout of the work results in the brands and locations. The work results developed in the first two years are now being integrated systematically and prioritised into the line functions of the brands. The brands are supported in their implementation by dedicated rollout managers, a close exchange between the project managers on best practice approaches and with bookable rollout packages.

Current projects in the GISP include the topics of Cloud Security, Identity & Access Management, PKI Enhancement, Shopfloor Security, Cross Functional Monitoring, Endpoint Security, Secure Software Development and Governance

Success factors

In retrospect, the PwC recommendations are also success factors for the implementation of the program. The recommendations mentioned above, such as faster intervals and adaptability, are an essential aspect.

But also the cross-brand staffing in the project responsibilities and the active role of the promoter contribute to the high acceptance of the program.

For programme steering, the following factors are crucial:

- Regular project manager meetings
- Regular retrospectives
- Feedback & implementation of measures
- Regular review of interdependencies between projects
- Actively manage risks
- New Work (Covid19): Try out new methods!

“The Group-wide information security committee analyses the ISF’s threat radar every year and derives corresponding risks. These risks are used to define measures that are then prioritised and incorporated into the Group Information Security Program.”

Of course, we have also learned from previous programs. These aspects are important success factors too:

- No overregulation
- Low administration
- Professional programme management
- High level of self-organisation in the teams
- Rollout not left to itself

Collaboration between Group brands at management and staff level has been strengthened, and the program’s active communication with best practices and lessons learned is helping to develop a global community around Group information security.

Christina Schlichting

Twitter @xiexingna

After studying Sinology, Political Science and German, Christina Schlichting started her working life at the end of 1990 with an international trainee program at Volkswagen AG in Wolfsburg. In 1993 she moved to Audi AG in Ingolstadt, where she held various positions, including Sales Manager for the People’s Republic of China with responsibility for setting up and managing the Audi Beijing Office.

In 2003, she moved to the Information Technology and Organisation department. After another move to Volkswagen AG in 2005, she took on various management functions in the area of IT personnel, development of service systems and IT governance tasks. Since September 2019, Christina Schlichting has been responsible, among other things, for the development and implementation of a Group-wide information security program.





Industry 4.0

“Real innovation can happen at the E4TC”

The digital transformation of industry thrives on agile development and implementation experience. This is where the European 4.0 Transformation Center (E4TC) comes in, which was founded in 2015 as a cooperation platform at the RWTH Aachen Campus. The E4TC offers its members from industry, research and IT, including secunet, the opportunity to further develop and share holistic process scenarios or solution architectures. *secuview* spoke with Prof. Dr Thomas Gartzten, Managing Director of the E4TC.

What is the state of digital transformation in industry today?

Prof. Dr Thomas Gartzten: At the latest since the challenges that the Corona pandemic brought for industry, it has become very clear to a large number of companies that they can only build up the necessary resilience for such dynamically unstable situations by digitising and networking their working environments. In this respect, the last two years in particular have seen a tremendous amount of movement in the industry and today we see digital transformation programs on the strategic agendas of companies almost everywhere – whether SMEs or major corporations. Of course, the maturity levels of individual companies and industries are very different. In this respect, it is important that the status quo in the company is transparent, because a digital transformation can only succeed with an unbiased view of one’s own processes and application landscapes and without unrealistic expectations.

What are the main obstacles that can arise in digitisation projects?

From my point of view, there are two different types of obstacles. First, there are the classic technological hurdles that arise from neglecting long-term strategic planning. All too often in the industry, people think in terms of use cases and proof of concepts that are isolated from each other. Without an overarching digitisation strategy and associated IT architecture that acts as a north star to align all digitisation activities towards a common goal, the subsequent scaling of initial solutions is often not possible. This means that the actual potential of continuous information flows, namely the closing of control loops within and across the company, cannot be exploited.

Second, there are also organisational obstacles to overcome. Digitisation projects should not only be ordered top-down, but should always involve the users in the development process and make them active players in the transformation. In this way, implicit knowledge is used sensibly on the one hand, and on the other hand, involved employees will accept the projects much better. Many people in companies have great reservations about digitisation projects, as they involve the elimination of process routines and the introduction of new procedures and standards that first have to be learned and

appropriated. The more participatory this design process is, the steeper the learning curve is when it is introduced and the less reservations there are about digitally networked work processes.

At the same time, it is important to always consciously reflect on successes and to view digitisation as a continuous process. An agile way of working in sprints, in which changes can be introduced, tested and evaluated in short cycles, has proved successful.

In your experience, how important is data security in the digital transformation towards Industry 4.0?

In the transformation to Industry 4.0, data security is one of the central fields of action. The aim of digitising and networking our production and working environments is to automate not only the work processes at the machine and plant level, but in particular the planning and regulating processes. This means supporting employees as best as possible in their tasks and decisions through digital tools. This requires that company-specific, mostly implicit know-how is digitally mapped in order to make it usable for AI applications, for example. In this way, IT applications can help machine operators, for example, to control production plants more sustainably by predicting quality losses and excessive energy consumption in real time based on data and thus preventing them. However, the necessary knowledge

The partners of the **European 4.0 Transformation Center (E4TC)** are research institutions as well as long-standing members of the RWTH Aachen Campus who are involved as technology providers or industrial companies in the digital transformation in their respective fields. In the E4TC, they form an exclusive cooperation platform for continuous and long-term scientific collaboration.

In test environments, experts can set up and improve production facilities in test scenarios. With its demonstration factory, the E4TC provides industrial companies with advice and support for their digital transformation – for example, on the topic of the Industrial Internet of Things (IIoT).

secunet has been a member of the E4TC since spring 2022 and contributes its expertise in the area of industrial IT security in particular. A first project together with Liebherr IT and Hewlett Packard Enterprise (HPE) has already started.



In the demonstration factory of the E4TC, industrial companies can present technological solutions in a larger and application-related context. 

about the production process, which must be made explicit and digitally mapped, is relevant to a company's competitiveness and absolutely worth protecting. The corresponding IT/OT infrastructures must therefore be reliably protected against attacks, which can occur both via the internet and on site. It becomes clear that Industry 4.0 solutions can only unfold their benefits if comprehensive data security is ensured.

How was the E4TC launched and what are its objectives?

The E4TC is a collaboration platform at the RWTH Aachen Campus and has been bringing together industrial companies, technology providers and science since 2015 to jointly develop new solutions for the digital transformation of the manufacturing industry. The scope of our ecosystem is deliberately very broad. We are convinced that in Industry 4.0, digitalised networking must already be taken into account in the development processes of a company. From there, it extends through production to customer processes, where, for example, data on the use of a product is collected. Especially in current research on the realisation of a circular economy, it is quickly becoming clear that a true circular economy cannot be realised without such digital data continuity.

At the E4TC, such approaches are concretely implemented for testing and validation, for example in the demonstration factory. At the same time, this also serves to communicate these solutions in a clear and tangible way. In this way, the E4TC member community also provides advice and support to industrial companies outside of our ecosystem on questions relating to digital transformation.

How does the cooperation within the framework of the E4TC actually take place?

Our cooperation always pursues the goal of bringing together or expanding new digital technologies in the form of concrete projects in order to apply them to industrial application fields and prove their benefits.

Once a common task and goal has been defined, an agile project team is formed with experts from our member companies as well as colleagues from the centre and the university institutes. This heterogeneous team then develops a concrete solution in the form of a Minimal Viable Product (MVP) in short-cycle sprints over a period of three to six months. We deliberately go beyond purely theoretical conception and always aim to develop not a PowerPoint presentation, but a functional digital-physical solution. Of course, we benefit from the

“According to the motto ‘demonstrating is better than claiming’, competence is credibly shown at the E4TC.”

unique infrastructure of the RWTH Aachen Campus with its demonstration and start-up factory as well as various real laboratories.

How do members benefit from technologies and insights developed within the E4TC?

The networking and collaboration opportunities in the ecosystem of the RWTH Aachen Campus, which consists of top research institutes and over 400 innovative companies, are, in my view, unique in Europe.

In the E4TC, as already mentioned, the focus is on the concrete implementation and continuous further development of functional digital-physical solutions. Since this is always done in cooperation with other members, the companies come into direct contact with new technologies and approaches and can at the same time demonstrate their own expertise in a real ecosystem.

Regular tours, workshops and events organised by the individual members allow not only representatives of the member companies but also many decision-makers from the industry to see these solutions.

According to the motto “demonstrating is better than claiming”, competence is credibly shown in this way. The presentation of one’s own technological solution component in a larger and application-related context, such as in the demonstration factory, helps immensely to convey the technology benefits in a tangible way. Real innovation can happen at the E4TC on the basis of clearly defined, practice-relevant tasks that are often even derived from the direct industrial practice of our members. We always work with our members to implement what is technologically possible. We cover all phases, from the generation of ideas to iterative testing and further development to the initiation of re-industrialisation. We provide support with many years of expertise and a strong network from practice and science.

Prof. Dr Thomas Gartzzen



Prof. Dr Thomas Gartzzen has more than ten years of practical experience in digital transformation and the realisation of Industry 4.0 projects along the entire value chain of manufacturing companies. Thomas Gartzzen studied mechanical engineering at RWTH Aachen University and, after completing his doctorate in 2012, worked as managing director of DFA Demonstrationsfabrik Aachen GmbH, a reference factory for Industry 4.0 on the RWTH Aachen Campus. Since 2016, he has been responsible for the European 4.0 Transformation Center GmbH in a managing capacity. Thomas Gartzzen has also held the professorship for manufacturing systems at Cologne University of Technology since 2021.

Study by secunet and techconsult

IoT projects in companies: External expertise often required

How important is the Internet of Things (IoT) for German companies? What obstacles affect implementation and what types of security incidents have there been in connection with IoT systems? To answer these and other questions, the research and analyst firm techconsult, on behalf of secunet Security Networks AG, surveyed more than 150 companies as part of the study “IoT – but secure. Secure infrastructures in a networked world”.

The results show that awareness of the opportunities offered by IoT is growing in German companies, but at the same time there is still a need to catch up in practice. Although the technology has a high or very high relevance for just under half of the companies, only 13% of the respondents say they have already implemented IoT on a broad scale. This is also due to the fact that only around a quarter consider themselves to be in a position to implement IoT projects completely on their own. More than 60% of the companies therefore rely on external partners in order to be able to take appropriate account of specialist, technical and legal levels from the outset.

At the same time, the study points to a significant lack of security precautions. According to the study, 44% of companies have not taken any specific measures to secure IoT. “Many companies believe that only large corporations are targeted by cyber-criminals,” says Jan Ludwig Tiedemann, Senior Solution Architect at secunet. This is a persistent misconception: around 30% of companies with fewer than 1,000 employees have already been affected by attacks, according to our survey. Cyber security is everyone’s business”.

Opportunities of IoT systems

Networked devices, machines or systems in the IoT hold numerous opportunities for companies from different industries. However, the companies surveyed primarily expect increased product quality (45%), process optimization (44%), improvements to existing products and services (42%), lower (production) costs (38%) and increased customer satisfaction (36%).



Jan Ludwig Tiedemann

jan.tiedemann@secunet.com

How do you implement or plan to implement your IoT projects?

Based on 151 companies

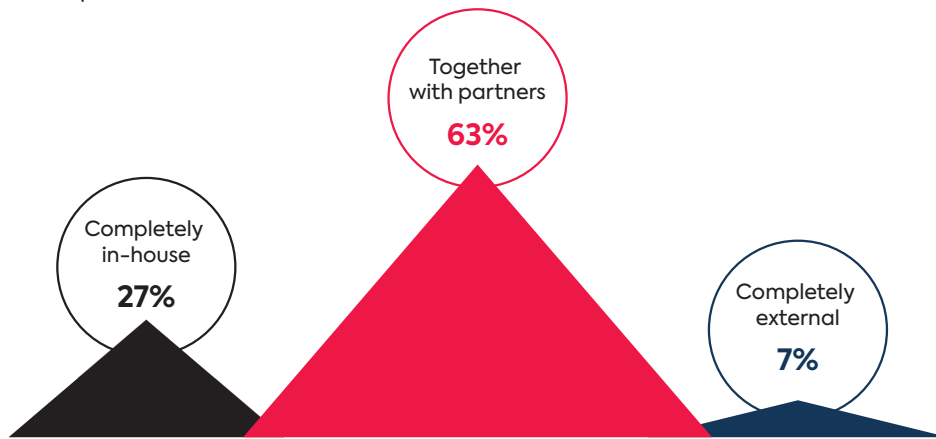


Fig. 1: secunet/techconsult study “IoT – but secure. Secure infrastructures in a networked world”.

Obstacles to secure implementation

Data protection (43%) and security concerns (36%), lack of expertise (38%) and integration into the existing IT infrastructure (36%) are seen by companies as the biggest hurdles in implementing IoT projects. In turn, compatibility with existing infrastructure is the biggest challenge for half of the companies surveyed when implementing IoT security. 46% also stated that they do not have sufficient expertise in this area, and 38% simply lack the necessary specialist personnel.

Most common security incidents

Almost 70% of the companies that were affected by cyber attacks were infected once or even several times via existing (legacy) devices. 44% of the companies surveyed had been affected by such an attack once in the last two years, and the number of unreported cases is likely to be even higher. In one quarter of the companies, these vulnerabilities were even exploited multiple times. Almost 70% also report targeted sabotage or industrial espionage. Around half said they had been affected by the compromise of IoT devices or their misuse for criminal purposes.

Demands on IoT security service providers

For companies to be able to adequately protect their IoT systems from cybercriminals, they regularly rely on the expertise of a security partner. What they want from this partner above all is a high level of technological know-how (50%), an understanding of processes (45%), industry expertise (41%), innovative strength (40%) and security certificates (36%).

All results of the study can be found at the following link:

<https://www.secunet.com/en/iot-but-secure>



Where do you see the biggest challenges in implementing IoT security?

Based on 151 companies

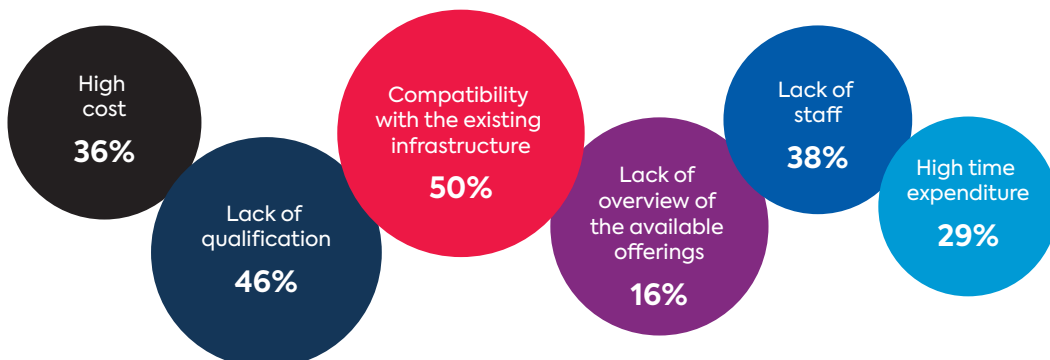


Fig. 2: secunet/techconsult study “IoT – but secure. Secure infrastructures in a networked world”.



How to make “Zero Trust” not only a buzzword

From zero to hero

A commentary by Dr Kai Martius, Chief Technology Officer, secunet Security Networks AG

Zero Trust and Zero Trust Architectures (ZTA) seem to be the new silver bullet for IT security. Are they? Or is Zero Trust another pixie dust? First, the term is somehow misleading to me. I don't want to live in a skyscraper built from a zero trust architect(ure). But as an engineer, I don't want to bash my, honestly, really creative marketing folks too much who often promote terms like this. So let's see what Zero Trust can, what it should mean.

For a start, when it means to reduce the inflationary use of the T-word to zero, I'm totally in. When it further means to shift the focus to trustworthiness, instead: yes, please! We really need to look for ways how to provide reasons to trust our IT systems.

Looking at some ZTA related concepts like “data centric security”, it feels like sitting in a super-secure war room on the roof top of my ZTA skyscraper and hope, that everything underneath will be safe enough to not let the skyscraper collapse. Because I don't trust, sometimes I look into a random floor downstairs, and see a lot of people running around repairing crumbling plaster and stuffing holes in the wall.

Seems, I hit another “Patch Day”. Don’t get me wrong: Of course we need to patch vulnerabilities, and we are very good in bringing the patch to the hole in the wall quickly today. But do you feel comfortable when every day someone rings the bell and fixes a hole in your structure you even weren’t aware of?

Ok, let’s be a bit more positive: Good ZT architects make me feel much better in my war room on the rooftop, when they build strong supporting pillars into all floors. If something breaks, some second line of defense is there. It is common knowledge of security engineering to build systems based on the concept of “defense-in-depth”. Whenever possible, you should make use of this principle, as it’s really hard to gain enough trustworthiness (here it is again) in one single pillar. Whether the whole architecture is called ZTA today or something else tomorrow – the concept is good. Two-factor-authentication (2FA) is a very good concept too. Using virtual machines as a second separation layer around container workload is also very helpful in case someone attacks your service.

Another take of ZT is a distributed or layered fashion of check points. Because there are so many different housemates with so many different notions of “trust” in my skyscraper, the single guard at the ground floor would simply had to admit access to too many people. Of course, it would not be wise to just check access at my war room on the rooftop, which is pointless when someone blows away the second floor.

So, a very first “entry check” could be to validate a base identity. However, a bag or parcel check at the ground floor is impossible, as there is encryption everywhere today. Now trustworthiness comes into play again: If the parcel comes from a trustworthy delivery service, it can be sent to the second floor. Ultimately you should only open the parcel when you know who sent it. You see: a good layered approach could be rights management on the application data layer, transport encryption and client certificate validation with TLS and a rather coarse-grained access control on network layer with VPNs.

It would not be wise to just check access at my war room on the rooftop, which is pointless when someone blows away the second floor.

Sometimes you have to accept parcels from somewhere you don’t know. Then it would be a good idea to have a bunker room, that is strong enough to not make our skyscraper collapse if something explodes. We have such building blocks with virtual machines for isolated environments today.

So, if we don’t have the super-trusted single guard at the ground floor anymore, how do I tell all the check points (also called “policy enforcement points”) all over, what is allowed to let in and what not. I admit, this layered approach is more complicated to manage than a single perimeter firewall. If ZTA products help you to easily manage these different layers: that’s really an improvement!

Btw., the multitude of trust relationships we are faced with in today's architectures and operator models was well researched in the concepts of multilateral security back in the 1990s. The idea behind was to start at zero trust – and to build trust relationships between all involved parties until a participant was willing to share data with others, certainly only under negotiated protection mechanisms.

Building trust until a relationship is trustworthy to share data is something we do all the time as humans. It starts with ZT, but ends up with trustworthiness.

Here we are again: trustworthiness. But the question is, how to get there. We have to consider a huge technology stack, but finally it ends up in people, companies, countries that are building and operating this technology stack in a (hopefully) secure manner. So when you make yourself aware of this huge networked tech stack, you can imagine what size of a skyscraper we talk about.

There is a lot of work underway to improve the situation in my skyscraper systematically. For instance, there are new rock-solid bricks like "Rust" (a more secure programming language) or magic doors (well-researched cryptography). A lot of opaque walls are replaced by glass bricks (Open Source) giving much more transparency how good a wall could hold. And we start to learn the laws of physics and how to calculate the statics of the building (mathematical proofs of correctness, automated test methods for software). Nothing about this is really new, but the multitude of interlocking approaches and technologies is making IT security more and more practical. Also, the issue is becoming more and more pressing. Just as new machines and knowledge have enabled us to build skyscrapers only in the 20th century, we are now in a position to implement truly secure IT infrastructures.

When we started to build our today's "world computer" many years ago, did we do it as we would have built a skyscraper in the middle ages? Sometimes it looks like that. But surely we can renovate it with these great technology bricks and knowledge we have had for some time now. We should constantly check and measure, and challenge our level of trust. If Zero Trust is considered to make us work like this: great!

PS: Anyway, maybe my super-secure war room will be for rent soon – I'm sure there will be someone who enjoys the view, and still feels good there. But we have started to build a new bunker on a solid foundation, rock-solid glass bricks from bottom up. Anyone who wants to rent a room there? Not so great view as on top of the skyscraper, but feels much safer!



Dr Kai Martius



IT and cyber security in the automotive environment

“Complex automotive architectures require uncompromising hardware and software security”

Mr Mühleck, in your career you have been CIO of Volkswagen AG and DaimlerChrysler AG as well as CIO of the German Federal Ministry of Defence and have thus taken on the perspective of both private companies and the state. What developments in the field of IT security have you noticed during this time and have you also helped to initiate some of them?

Klaus Hardy Mühleck: With the entry of the internet into all areas of life, IT security has taken a huge development. In the automotive industry, for example, we started implementing security mechanisms in communication relationships as early as the nineties, for example in video conferencing systems and IT access in factories. I can still remember the digital design of the first secure immobiliser for our vehicles and the transition from disc-based maintenance software to network-based dialogue maintenance. That was more than 15 years ago. After that, it was one blow after the other: intelligent firewalls,

intrusion detection, trust centres and PKI to the present day SOC with semantic AI support in a Security Information and Event Management (SIEM) world.

Government institutions were also required early on to secure their digital worlds with systems for VS-NFD (RESTRICTED) or GEHEIM (SECRET) and NATO SECRET or, for example, to use dynamic PKI keys for the deployment of large-scale military equipment. Police authorities, embassies, services and ministries such as the German Ministry of Finance with the ELSTER electronic tax return use modern technologies for security and even for police manhunts. Only recently, a six-figure number of high-security communication routers were rolled out in Germany (such as the secunet konnektor, editor's note), which network all doctors' practices with the telematics infrastructure of the healthcare system. High security is unavoidable in all these areas. And companies like secunet have made these highly secure IT structures possible.

Klaus Hardy Mühleck

After studying electrical engineering, process automation and data processing, Klaus Hardy Mühleck began his professional career at Siemens AG. He then worked for 14 years in the Daimler Group, most recently as CIO Automotive and member of the Daimler Management Committee. When he moved to the Volkswagen Group, he assumed responsibility as CIO for the AUDI brand group and then as CIO for the entire VW Group. In mid-2016, Mühleck was asked to move to Berlin as CIO to build up the cyber and IT organisations of the German Federal Ministry of Defence.



To what extent do you see a change in the automotive sector from monolithically thinking automotive groups to an exchange within the industry involving actors from other sectors such as politics or infrastructure?

Traditionally, the automotive industry in Germany has been concerned with the development and production of high-quality and innovative vehicles. The exchange of different competences as well as at vehicle trade fairs has always taken place, especially in the classic disciplines, but also partially in IT. Supplier partners and engineering service providers have played a very large part in this. They have made technology transfer possible.

But the big transformation comes with the digital ecosystems in and around the vehicle: the connection of cloud-based online services, services in the electric vehicle for charging management with charging stops along the route, parking guidance systems up to (partially) autonomous driving and emergency assistance are almost standard today.

The change to see a vehicle as part of various ecosystems of the automotive environment is in full progress. Tesla is certainly a pioneer or even a disruptor here. The German automotive industry is still struggling with this digital influence of the surrounding cloud world. But it is catching up and arming itself for the future.

But our politics are also in demand. We need the necessary infrastructure for 6G in order to bring about this change in Germany quickly and innovatively. I still see a great need for action here. Finland and the Asian countries, for example, are on their way much faster. This is also due to data protection regulations in Germany. The political and legal

hurdles in Germany should be adapted to the times and data storage should be intelligently structured so that it does not remain an obstacle and at the same time protects personal data.

Let's talk about networking – from telematics in the vehicle to vehicles that communicate with other devices to autonomous driving: Where do you see the biggest challenge for the automotive industry to realise communication between so many players?

Today, it is impossible to imagine vehicles without networking. Back in the late nineties, we connected our US trucks at Freightliner to logistics networks to enable "route planning" and optimise driving routes over thousands of kilometres. The trucks already had laptops that could communicate securely. This was still very cumbersome back then, but today the technology is much more advanced.

Telematics services have been around for a long time, but it was Tesla that boldly took them to a level that everyone has to measure up to. The reading out of vehicle data and flashing used to be done via the car repair shops, controlled by the maintenance technician. Today, flashing is also possible via the online telematics interface and without a visit to the repair shop. All these accesses must be secure and there should be no uncontrolled interventions. This will be a key factor especially if Car2Car communication and connection to 5G networks are to enable autonomous driving.

The major challenge for the automotive industry is the storage and evaluation as well as networking of sensor data from the vehicle and the sensed environment. These data volumes must be evaluated with high computer performance via AI and made

“Holistic security architectures across all layers of the vehicle and environment components will be a decisive factor in the success of future vehicle generations.”

available to the automobile for vehicle control. The actuators then use this data to control the vehicle.

All of this requires a high level of software expertise and semantic AI of the next generation, so-called 6G. This new dimension of virtual system integration in the Digital Twin of the automobile has yet to be fully developed by the automotive industry and coordinated with many partners.

What role does IT security play in this?

Networking and data storage in such complex automotive architectures require uncompromising hardware and software security. This begins in the vehicle at the binary unit system (BUS) level with all common protocols and networked electronic control units, includes the ad-hoc networks in Car2Car communication and extends to the multitude of services in the cloud. Already today, for example, the immobiliser and available remote access functions with keyless go play a central role in vehicle security.

All interfaces and the communication between the systems require security technology. This starts in the vehicle with BUS systems and “embedded safety components” in the networks already available today such as CAN, LIN, FLEXRAY, continues with Car2X communication in mobile ad-hoc networks (MANets) with safety procedures such as Secure Dynamic Source Routing (SDSR) and ends with data storage and AI in the cloud.

The automotive engineering of the future will necessarily include holistic security architectures across all layers of the vehicle and environment components. This will be a decisive factor in the success of future vehicle generations.

The high-frequency automotive production processes are highly susceptible to supplier disruptions. How will supply chains change in the future and how can the OEM ensure that it can trust the complete supply chain?

That is an interesting question! Today, the OEMs' value chains are extremely synchronised and globally oriented. The optimisations stem from the “LEAN production era”, with all the associated procedures of “Just in Time”, KABAN and “Just in Sequence”. In

addition, many production steps and components were outsourced to countries with favourable cost structures.

The interaction of the entire supply chain from the first-tier supplier to the fifth-tier supplier is immensely heterogeneous and difficult to control. OEMs try to overlook these chains and control them via planning networks. Complex predictive planning models are already in use today.

Nevertheless, events such as corona lockdowns or a war cannot be foreseen and planned in advance. However, these events have a serious impact on the networks' ability to deliver. About 70 to 75 per cent of all parts in the vehicle are vendor parts. This high number always brings dependencies with it. Constant cost pressure in vehicle manufacturing has led to such structures via outsourcing.

One way to correct this is for OEMs and their first-tier suppliers to once again do more of their own manufacturing in stable countries, such as Central Europe, the USA, Canada, Japan or South Korea. But this immediately leads to cost increases and consumers are not willing to pay double.

Somewhere in the middle, the future path of the production and supply network will settle in the OEM network. Stable supply chains require stable partners in stable countries and a rethinking of the global supply chain philosophy. More of the OEMs' own involvement in relevant areas of the body, drive, electronics and software reduces dependencies. In addition, partners must be chosen who produce in a stable environment.

All this needs to be rethought, and the climate crisis will additionally force us to bring the supply chains closer to the OEMs again, with all the advantages and disadvantages of manageable globalisation and localisation.



Secure IT (not only) for CRITIS

Learning from critical infrastructures

Uncertain times make it clear how strongly dependent we are and how much we rely on these foundations in our everyday lives. Especially in the case of critical infrastructures (CRITIS) such as energy suppliers or hospitals, restrictions or failures hit us hard. That is why their IT security is subject to legal regulations. Other companies that handle sensitive data can also learn from the security technologies designed for CRITIS. And also a cloud solution can be a building block of a security strategy.

With regard to IT security, CRITIS operators are confronted with a threat situation that is changing rapidly. In its latest status report on IT security in Germany, the German Federal Office for Information Security (BSI) identified around 144 million new malware variants – an increase of 22 percent compared to the previous year. Attacks with ransomware in particular – malware that encrypts data or threatens to leak it in order to extort money – have increased sharply. The consequences of such an attack can be devastating: in 2021, for example, a university hospital was unable to admit emergency patients for 13 days after a successful attack.

In order to succeed under these circumstances, companies and operators should not see cyber security as a one-off investment, explains Dr Marius Feldmann, COO of Cloud&Heat Technologies GmbH

THE SECURE CLOUD

For public institutions and highly regulated private sector companies such as energy suppliers or health-care providers, cloud computing has hardly been an option up to now. To change this, secunet has built up a cloud portfolio that brings digital sovereignty to the cloud. One of the cornerstones is the cloud operating system **SecuStack**, which secunet and Cloud&Heat have developed on the basis of open source software. With SecuStack, data is consistently encrypted with the same security modules that secunet has been using for many years in the high-security sector. The cryptographic mechanisms are integrated transparently and can therefore be tested. Users retain control over data and applications at all times. With the acquisition of the cloud and Kubernetes specialist **SysEleven** (see next double page), secunet has added another cornerstone to its cloud portfolio this year. Now secunet offers a comprehensive, customised cloud offering for public authorities, administrations and security-savvy companies.

and CEO of secustack GmbH: “After all, IT security is not simply a state that you achieve. It’s a permanent process that involves a permanent build-up of competence – and the corresponding protagonists who want to do exactly the same thing on-site.” This is not only advantageous in the event of damage, it also contributes to the prevention of future cyberattacks.

The IT Security Act 2.0 as an opportunity

In Germany, the new IT Security Act 2.0 (IT-SiG 2.0) will come into force in May 2023, with stricter requirements for CRITIS companies. The group of affected companies will also be significantly expanded, primarily to include the so-called “companies in the special public interest” (UBI). The catalogue of minimum requirements will also be more extensive. But what do truly secure IT infrastructures look like?

The German IT Security Act 2.0 makes a number of concrete specifications in this regard. For example, all security-relevant network and system components may only come from trustworthy manufacturers. Companies must also have systems in place for attack detection, which ideally prevent attacks from reaching the company in the first place because they are detected and stopped at an early stage.

When designing security measures, however, the concrete requirements of the respective organisation are always in the foreground. First of all, committed protagonists and competences on site or the right partners are needed in order to determine which requirements the systems have to fulfil. A comprehensive analysis should not only document possible risks, but also how the system is used and which long-term interests need to be taken into account. Especially when making structural decisions, it pays to think long-term. Even if individual vulnerabilities can always be closed, the last decades show that IT security should not be seen as an acute problem, but as a constant challenge.

Among the most important pillars for secure IT infrastructures are the design and standards of the system itself. The question here is whether manufacturers have already thought about security and protection against external influences during development. Systems that have been developed “secure by design” or “secure by default” are characterised, among other things, by a secure configuration from the time of installation. This provides systems with a fundamental resilience to external access and helps to prevent human error and the resulting security vulnerabilities in advance.



 In Germany, many hospitals belong to the critical infrastructures.

In general, resilience to human error is a crucial feature of secure IT. Therefore, it is also important to find solutions that take this factor into account, as it poses a risk for phishing or social engineering attacks during ongoing operations that should be minimised. A high degree of automation, standardisation where possible and a secure cloud infrastructure can help to reduce the potential for human error, explains Dr Kai Martius, CTO of secunet and CEO of secustack GmbH: “It is very important to prevent possible wrong decisions in advance and to design systems as securely as possible in this respect as well. I think the critical industry has a lot of experience in this in its traditional field. But this has not yet been consistently taken into account in the design of IT systems. This is where cloud technologies can help by providing a high degree of automation.”

Partner selection is crucial

Rarely are all the competences available to set up or manage the required IT infrastructures themselves. It is therefore important to choose the right partners – and to avoid unnecessary dependencies: The introduction of a new cloud infrastructure, for example, requires time-consuming and cost-intensive integration work with the existing systems. This sometimes makes it difficult to switch to another provider at a later date, even if this other solution is better suited to one’s own requirements. It is precisely these vendor lock-in scenarios that need to be avoided. The focus here should therefore be on medium- and long-term interests rather than short-term cost advantages.

Finally, security is always about trust. Will the security partner prioritise any challenges that may arise? Understanding IT security as a process also means learning from attacks and thus further minimising potential risks. This understanding should be shared by the partner.



Dr Kai Martius
kai.martius@secunet.com



Dr Marius Feldmann (left)
and Dr Kai Martius



SECUNET SOLUTIONS FOR CRITIS AND UBI

The transparent IT security monitoring and early attack detection solution **secunet monitor** creates a situation picture in order to quickly screen, assess, contain or directly prevent potential security incidents. In addition, the solution facilitates the assessment by management and the responsible authorities. This enables companies to develop and implement much more targeted short-, medium- and long-term strategies and measures.

With the Secure Inter-Network Architecture **SINA**, companies can cover all security requirements stipulated by the BSI for working with sensitive data and documents. Employees can use SINA to access sensitive data on their end devices regardless of where they are, and the solution itself meets the requirements for classified information in public authorities. Due to the large variety of available components, SINA can be tailored to very different security requirements – including those of CRITIS and UBI.

In addition, secunet offers comprehensive **consulting, pentest and forensics** services.

More information: <https://www.secunet.com/en/utilities>

Secure cloud computing

secunet acquires SysEleven and expands its cloud portfolio

In May 2022, secunet acquired 100 percent of the shares in SysEleven GmbH. With the acquisition, secunet is significantly expanding its range of solutions in the areas of cloud and cloud security.

SysEleven is an independent German provider of Cloud Infrastructure, Cloud Services, Managed Services and Managed Kubernetes. The company has its own open source based cloud infrastructure with ISO27001 certified data centre locations in Germany (Infrastructure-as-a-Service) and provides MetaKube, a platform for the efficient management and optimization of computing, storage and network resources based on Kubernetes (Managed Kubernetes).

“With the acquisition of SysEleven, we accelerate our activities within the fast-growing market for secure cloud infrastructure. We strengthen our technological position and gain a team of highly qualified experts with proven capabilities in project implementation and managed services, as well as great expertise in Open-Stack and Kubernetes”, commented Axel Deininger, CEO of secunet Security Networks AG. “Having already developed SecuStack, an open source based cloud operating system for customers running their cloud ‘on premise’, we can now also offer a solution ‘as a service’ and further develop it together. Our customers, who generally work with security-critical applications and confidential information, benefit in two ways: on the one hand from the flexibility in terms of availability, costs and performance, and

on the other hand from the high quality and security expertise for which secunet has stood for over 25 years.”

SysEleven was founded in 2007 and employs more than 100 people. The Berlin-based company serves more than 175 customers in the German-speaking markets (DACH) and pursues a long-term partner-



ship approach with a focus on customers who value security and independence from hyperscalers. The company, which is a member of the European initiative to build a high-performance, competitive, secure and trustworthy data infrastructure (GAIA-X), will continue to be operationally managed by the current managing directors Marc Korthaus, Jens Ihlenfeld and Andreas Hermann after the takeover by secunet. “We transform digital sovereignty into actionable products and will now approach the energetic further development of our cloud solutions at an even faster pace and add further security aspects,” says Marc Korthaus about the advantages of the new constellation.



Tap-proof voice communication

SINA Communicator H wins iF Design Award

Many technological hurdles have to be overcome to make telephone calls at the high security level of GEHEIM/SECRET. This is why the product developers at secunet initially had technology on their minds when they set about the task of developing a highly secure device for voice communication. How can the many characteristics and specifications of communication in the SECRET environment be transferred to the age of IP telephony? All-IP technology at the highest security level – of course. Modern NATO protocols – of course. Tap-proof and emission-protected – of course. But the developers at secunet like challenges. And so they soon asked themselves whether it was enough to cover only the technical aspects.

We all use smartphones in our everyday lives, which offer a variety of other functions in addition to telephony and look pretty good doing it. Are employees in ministries and the armed forces supposed to do without all this when they communicate in a tap-proof manner? “Not with us,” said the secunet developers

and created a product that not only offers state-of-the-art security – for example, it is the first national device that is capable of post-quantum cryptography – but also excellent usability and outstanding design.

With its large touch display, the SINA Communicator H has more in common with a tablet than a telephone. Its operating concept is so simple and intuitive that anyone with a smartphone can effortlessly call up its many functions and switch between different levels of secrecy.

The iF jury agreed and in May 2022 presented the SINA Communicator H with the prestigious iF Design Award. The award not only recognises the great design, but also the usability. The SINA Communicator H has thus become the world’s only award-winning device for SECRET communication.



Somewhat unexpectedly, the SINA Communicator H also caused a stir among the general public in September 2022: first, German Chancellor Olaf Scholz tweeted a photo of himself at his desk with a red version of the device. In turn, Germany’s widest-reach daily newspaper, the BILD, took an interest in this and put the photo on its front page. “When the red phone rings at the chancellor’s” was written next to it. In addition, the BILD sensed a “touch of James Bond in the Chancellery”. Who would disagree with that?





Secure and trustworthy patient care

secunet participates in the SEMECO project

More flexibility, faster approval processes and shorter innovation cycles – these are the goals of the Secure Medical Microsystems and Communications (SEMECO) project. Innovations in medical technology should thus more quickly benefit those for whom they are intended: the patients. SEMECO is funded within the “Future Cluster Initiative” (Clusters4Future) of the German Federal Ministry of Education and Research. With its expertise in the development of high-security solutions and its many years of experience in the regulatory environment, secunet is participating in two cross-sectional projects.

In order to make patient care more secure and trustworthy worldwide, SEMECO is aiming for an ecosystem and reliable partners who want to revolutionise the medical technology and microelectronics industry together. In this context, IT security and data protection are basic prerequisites for establishing a trustworthy system architecture and the desired technology platform. The protection of network-capable medical technology, medical software and patient data against digital attacks is essential for the success of modern solutions in medicine.

“As a leading German IT security company, secunet can make a decisive contribution in this regard, allowing the sustainable protection of patients, medical data and medical technology,” says Dr Tobias Urban, Business Development Manager eHealth at secunet. Specifically, the project team is involved in the development of secure and trustworthy system architectures as well as AI-assisted regulation for medicine and cybersecurity. The focus is, on the one hand, on the digital protection of medical

devices and software and on the other hand on the development of these along applicable and, if necessary, still to be defined industry standards.

The holistic approach of the cluster provides secunet and all other project partners with the opportunity to research solutions that can be easily developed into products and thus quickly and efficiently improve medical care – securely and trustworthily.

The project is still in its initial phase – stay tuned for updates and first results!



Dr Tobias Urban

VIT supports projects between science and industry


Integrating innovation and research into business and society – that is the goal of the Association for Innovation and Transfer at Ilmenau University of Technology (VIT w. V.). Since 2019, the economic association has been funding projects between scientists at the university and industry. Last week, Thuringia's Minister of the Interior Georg Maier (on the right in the picture) handed over the foundation charter to Prof. Gunther Notni (on the left in the picture) of the university. secunet supports research contracts of the VIT w. V., especially in the field of telematics/computer networks in the competence area of network and IT security.



Strategies against skills shortage

secunet is training again



 The new apprentices with trainers Irene Wolff (right) and Olaf Stottrop (2nd from left)

secunet resumed training operations at its Essen location in the summer. From 1 August 2022, the team welcomed two prospective office administrators and two IT specialist apprentices with a focus on system integration. As a company, secunet strives for medium- and long-term cooperation with professionals who share its values and vision.

The course of training is divided into a practical and theoretical, school-based part. The apprentices alternate between the secunet site and the respective vocational school. The young colleagues are each supported by a trainer who accompanies them throughout the three years of training. After consultation, this can also be shortened to two and a half years.

In addition to the training operation, the Trainee@secunet program will start on 1 October 2022. Three young talents are being sought in the area of cybersecurity: Consulting, Sales and Software Development. In two years, the trainees will pass through a total of four stations and will not only get to know the divisions and areas, but also the various secunet locations.

Dates – October to December 2022

25 – 27 October 2022
it-sa | Nuremberg, Germany

25 – 27 October 2022
NATO Edge | Mons, Belgium

3 November 2022
SPS Nuremberg |
Nuremberg, Germany

15 – 17 November
International Face Performance
Conference | Digital

15 – 17 November 2022
SpaceTechExpo |
Bremen, Germany

14 – 17 November 2022
MEDICA | Düsseldorf, Germany

30 November – 1 December 2022
Berlin Security Conference |
Berlin, Germany

Do you have any questions
or would you like to book
an appointment with us?
Please send an email to
events@secunet.com.

Imprint

Publisher

secunet Security Networks AG
Kurfürstenstraße 58, 45138 Essen, Germany
www.secunet.com

Chief Editor, Head of Design and Content (Press Law Representative)

Marc Pedack, marc.pedack@secunet.com

Design and Setting

sam waikiki GbR, www.samwaikiki.de

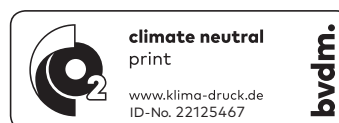
The contents do not necessarily reflect the views of
the publisher.

Copyright

© secunet Security Networks AG. All rights reserved.
All content herein is protected under copyright law.
No part of this magazine may be reproduced or
otherwise used without the prior written consent of
secunet Security Networks AG.

Photo credits

Title, p. 10, 11: Volkswagen AG
p. 2 (bottom), 5, 8, 18, 21, 29: Getty Images
p. 2, 24: kbarzycki/Adobe Stock
p. 3, 7, 14, 16, 17, 20, 26, 28 (centre and bottom),
29 (bottom), 30 (bottom): secunet
p. 6: Schoening/Alamy Stock Photo
p. 12: Scharfsinn/Alamy Stock Photo
p. 15: Rheinisch-Westfälische Technische
Hochschule Aachen
p. 22: Klaus Hardy Mühleck
p. 25: senivpetro/freepik
p. 28 (top): iF International Forum Design GmbH
p. 30 (top): Technische Universität Ilmenau





What to do when a hacker strikes?

Relax – with secunet, data and infrastructure are ultra-secure.

Wherever data and IT infrastructures need protection against cyber attack, secunet is ready to help. As IT security partner to the German federal government, we offer agencies, authorities and companies expert advice and super-secure solutions for protecting data and communications.

[secunet.com](https://www.secunet.com) protecting digital infrastructures

secunet