secuview

The secunet Customer Magazine 1|2019

AXEL DEININGER NEW SECUNET CEO

A Wealth of Future Topics

Security for industry 4.0

Connecting, safeguarding and monitoring machines in IoT environments

Transformation at Europe's external borders

European countries are preparing for the Entry / Exit System

National

International

Corporate Update

Trust between machines:
The ifm group of companies provides its Industry 4.0 components with digital identities.

Technologies & Solutions

News in Brief

Service

Interview with Bernd Kowalski, German Federal Office for Information Security, on the biometric requirements of the new European Entry/Exit System

Editorial

Dear Readers,

As of today you will notice a new face in this role. On 1 June 2019 I took over from Dr. Rainer Baumgart as Chair of the secunet Security Networks AG Executive Board, following Dr. Baumgart’s retirement after 18 years in this role. I am now looking forward to the tasks that lie ahead of me, both big and small. Writing the secuview editorial is one of the smaller tasks; however I will gladly seize the opportunity to regularly address a few words to you!

In recent months I have had the opportunity to deal in depth with some fundamental issues in respect of secunet. What is the status quo; where do we want to go; how will we get there? My predecessor and I answer these questions in a joint interview inside this edition of secuview.

Only so much in advance: when it comes to IT security we’re talking about an exceptionally dynamic market that is constantly generating new customer demands. At secunet we will prepare for these by orienting ourselves towards a more international focus, and also – more so than before – focussing on the industry sector.

Two more articles in this edition highlight how exciting the change processes in industry, which were initiated by digitalisation, are: ifm manufactures components for industrial automation. These devices are equipped with reliable digital identities to allow them to be identified unequivocally within industrial infrastructures. Furthermore, we show how machines in the Industry 4.0 environment can be securely networked and maximise their potential using edge computing features.

There is also a lot going on in our core markets. In 2022 the European Union will introduce the EES Entry/Exit System, which will secure the external borders of the Schengen Area more effectively. In addition, however, the system will also cause considerable extra workload at border controls. Many states are therefore introducing automatic border control solutions that will lessen the strain of this extra workload. In a twelve-page special report we highlight the current state of affairs and possible solutions, as well as the existing challenges.

I now wish you an enjoyable read and a pleasant autumn!

Axel Deininger

RheinEnergie's gas and steam turbine heat and power plant Niehl 3 boasts an electric capacity of 450 megawatts and a district heating performance of 265 megawatts.
(c) RheinEnergie AG

PROTECTING CRITICAL INFRASTRUCTURES

Delivering over and above the IT Security Act

RheinEnergie AG supplies around 2.5 million people, as well as industry, trade and commerce, with energy, drinking water, natural gas and heat. This puts the company in the ranks of critical infrastructures, which, since 2015, have had to meet specific IT security requirements in Germany. To satisfy these requirements RheinEnergie decided to introduce an Information Security Management System (ISMS). The system is deployed throughout the company and therefore goes further than legally stipulated. We spoke to Patrick Porsch at RheinEnergie who was in charge of setting up the ISMS.

Herr Porsch, energy and water providers such as RheinEnergie have to get to grips with a constantly growing number of rules and regulations. These include the German IT Security Act (IT-Sicherheitsgesetz), industry-specific security standards like B3S for virtual power plants, or the security catalogue of the German Federal Network Agency (Bundesnetzagentur). The latest example is the IT security catalogue for energy plants, which was published in December 2018. How does your organisation manage to cope with this deluge?

It's true: for a company like RheinEnergie where many divisions are affected dealing with the many different requirements is not easy. When you count operating the electricity and gas network, supplying water, the virtual power plant for secondary control power and the power plants, we are affected by four different B3S or security catalogues. In addition to this, these catalogues contain requirements that are partly contradictory. It is therefore especially important for us that the framework for the Information Security Management System (ISMS), which we introduced in recent years, is incorporated consistently throughout the company, and only very few area-specific regulations exist. A prerequisite for this was and is good collaboration between the various major departments, which were all able to agree on the central framework.

Moreover, I must also mention the valuable input from secunet in the context of the ISMS project. secunet brought in its legislator contacts. This made it possible to interpret and implement the legal requirements correctly.

Communication within the relevant sectors is also crucial: we regularly communicate with the other energy and water suppliers about the ramifications of the legal changes and how to deal with them, e. g. in the German Association of local utilities of municipally determined infrastructure undertakings and economic enterprises (VKU), the German Association of Energy and Water Industries (BDEW), or the German Gas and Water Association (DVGW).

What provided the impetus for the development of the ISMS at that point? And how did you go about building it?

The German IT Security Act, which entered into force in 2015, provided the basis for the decision to draw up an ISMS. We went further than the legal requirements stipulated, however: although only individual major departments at RheinEnergie came under the remit of what was legally required we decided to roll out the ISMS throughout the company.

Security incidents are occurring with increasing frequency. This leads to information security becoming ever more critical for companies. We therefore not only wanted to improve the information security for the critical infrastructures in our company, but to continue to raise the level of security across the whole of RheinEnergie AG.

In the short term this does of course have a cost impact. In the medium and long term I believe we will reduce the costs through IT security measures, for instance because fewer information security incidents will arise; and where incidents do arise we shall have the ability to identify them earlier and deal with them more rapidly.

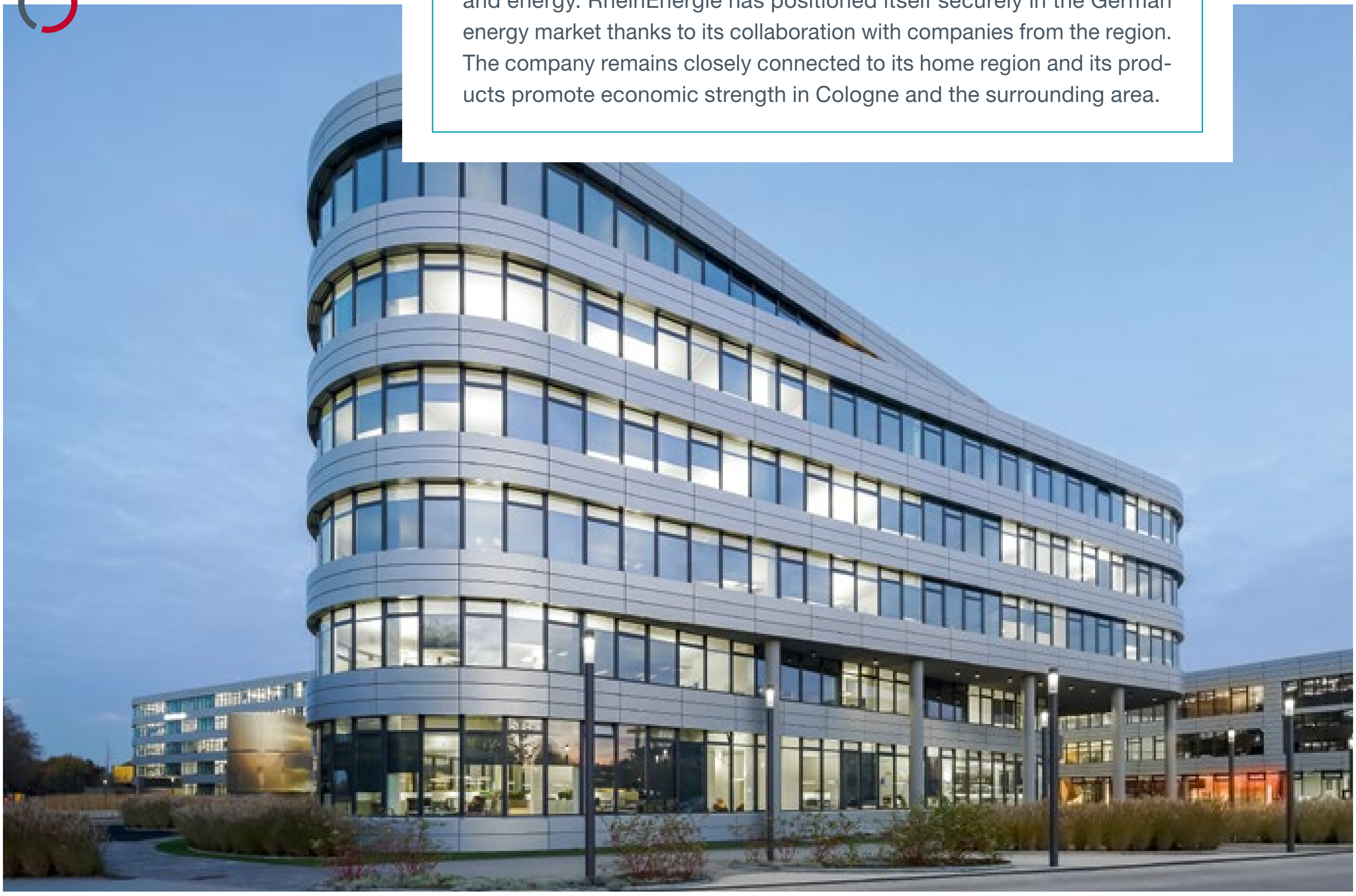
We should emphasise here that the construction of an ISMS needs to follow a top-down approach: the key thing is firstly to convince the executive team and bring them on board as supporters; the next step should then involve engaging the departments. This is how we, too, proceeded when we were setting up the ISMS. Firstly we defined a company-wide framework and set of rules, which we then used to establish the processes in the major individual departments.

Which challenges arose during implementation?

Due to the many different sectors we had to take a variety of requirements into account, which all needed to be brought under one roof. We were already using several management systems, e. g. a quality management system and an energy management system. Information security was a new aspect in this context, however. A number of organisational units had to be collated and combined. To achieve this, it was especially important to raise awareness of information security among employees and managers.

Overall the implementation ran very smoothly, which among other factors can be attributed to the secunet employees' specialist expertise and the manner in which they brought their knowledge to the ISMS project.

RheinEnergie AG's head office at Parkgürtel, Cologne, Germany
(c) RheinEnergie AG



ABOUT THE COMPANY

RheinEnergie AG is an energy provider rooted in Cologne and the Rhine region and active across Germany. The company offers numerous energy services in addition to drinking water and energy. RheinEnergie has positioned itself securely in the German energy market thanks to its collaboration with companies from the region. The company remains closely connected to its home region and its products promote economic strength in Cologne and the surrounding area.

Patrick Porsch

Information Security Officer at RheinEnergie AG (until May 2019)

IN THE INTERVIEW

Patrick Porsch held the role of Information Security Officer at RheinEnergie AG from June 2016 to May 2019. In this capacity he was responsible for information security at RheinEnergie. He guaranteed that the legal requirements regarding information security were complied with and that the level of information security was continually improved and reviewed. In particular he looked after the construction, management and founding of the Information Security Management System (ISMS). Furthermore, he worked on the design of IT emergency management in order to be able to ensure that IT services could continue in the event of interruptions to IT operation.

Prior to his role as Information Security Officer Patrick Porsch worked as a Software Developer and Scrum Master at RheinEnergie and was involved in several agile projects in this capacity. At this time he was already working on the information security of self-developed applications.

What advantages does implementing an ISMS bring for RheinEnergie?

In the first instance, the ISMS helps us to identify and minimise security risks early on. This creates a defined, transparent level of security. Information within the scope of the ISMS is always appropriately protected against threats in daily operation.

Another important aspect is that the ISMS enabled us to establish a security culture that all employees can buy into, especially against a background of supply security for our clients.

Furthermore, the ISMS guarantees compliance with all relevant legal provisions. Last but not least, the ISMS supports our corporate strategy: for us it is important that shareholders, clients, partners and employees perceive RheinEnergie as a conscientious and trustworthy energy supplier. Information security makes a valuable contribution to achieving this.

How did risk management – in the form of the ISMS – influence the everyday IT security operations? Which changes took place? Can positive effects be seen? Have new challenges arisen in some instances?

We optimised many existing processes regarding information security, e. g. authorisation assignment and change management. Information security ultimately affects every process and every IT system in the critical infrastructures. Employees increasingly see this as an integral part of their job remit.

At the beginning, risk analyses and the consequent measures that followed meant extra workload. This did not go unnoticed among employees since it was generally in addition to their previous responsibilities. We therefore communicated the benefits clearly and highlighted the advantages for individual employees. An example: when employees document their processes in greater detail there is a clear benefit if colleagues are absent for a longer period of time. This avoids the answers residing exclusively in one person's head, and processes can continue to be carried out. This then also led to increased acceptance among employees.

There were also positive effects from the fact that information security is increasingly under the microscope when purchasing services and products; and the requirements on service providers and suppliers have changed in this respect. This is another reason why we have observed an improvement in information security at RheinEnergie.

What impact does the ISMS have on the IT infrastructure?

Of course, the ISMS has also brought about technical changes: we have carried out both preventive and detective security measures. IT security is a never-ending process; we are therefore keen to continue to improve in this respect and to work on the security of the IT infrastructure on an ongoing basis.

BAVARIAN TAX ADMINISTRATION

Analysing Sensitive Data – in a Mobile Office

Maximum security is non-negotiable when processing financial and tax information while away from office premises. How to do this successfully without major loss of efficiency and user convenience was the question facing the Bavarian tax administration in 2018. The starting point was the formation of an analysis unit tasked with evaluating sensitive data for statistical purposes, as well as for auditing and controlling. It was clear that, since many employees from the new unit would be working while out of the office, the new IT infrastructure needed to enable this – and, at the same time, satisfy extremely rigorous security requirements.

When searching for a solution the focus quickly moved to the client systems. “Client systems are the eyes, ears and fingers of an administration; and thus their extended brain” – this was one of the premises for the project. The central position of the clients makes them especially important for security. In other words: as soon as a client is compromised, many safeguarding mechanisms are rendered futile.

This ultimately directed the IT operations at the Bavarian tax administration towards a SINA infrastructure: the SINA Secure Inter-Network Architecture can guarantee maximum protection right the way through to the end device. Within this architecture, the SINA Workstation acts as the client. It is able to handle various security domains that are sealed off from each other on a single machine.

So what does the solution look like today in practical terms? Data are transmitted from the computer centre to the secure area using a data diode. Two zones exist: one featuring a normal level of security and one an extremely high security level. In the first, employees have access to their usual office environment via LTE, WLAN or LAN. In the highly secure zone they can access the sensitive data stored in databases and other file systems. The highly secure zone thereby represents an additional VPN in the VPN.

Consequently, the solution satisfies both the mobility and security requirements and, in addition, is easy to use: SINA Workstation users do not require any specific IT knowledge.

Christian Eisenried
christian.eisenried@secunet.com

Main entrance of the Bavarian State Office for Taxes’ premises in Munich, Germany
(c) Bayerisches Landesamt für Steuern

HIGHLIGHT TOPIC: EU ENTRY / EXIT SYSTEM

Transformation at Europe's External Borders

From 2022, the European Union's Entry/Exit System (EES) will secure the external borders of the Schengen area – and significantly change the border control processes there. With the introduction of the EES, all third country nationals (TCN) who wish to travel to a country within the Schengen area will be required to register at the border by providing four fingerprints and a facial image. This process supersedes the former manual stamping of passports. The biometric data are stored together with other information about the traveller's identity in a central database, which is run by the EU agency eu-LISA. In the future, this will make it simpler to check who is residing within the Schengen area and who has exceeded the time limits for their stay. This serves to protect against people entering illegally, against document and identity fraud, and against organised crime and terrorism.

The introduction of the EES brings some challenges for the border control authorities of the Schengen states. Registering third country nationals at all external land, sea and air borders in the Schengen area will entail considerable additional efforts, meaning that slower processing times and, consequently, long queues at the borders can be anticipated. One solution to this problem lies in automating individual elements of the border control process. While many countries already take this approach at their international airports, there are still outstanding questions at land borders. The following pages cast light on the situation from a number of different perspectives.

KONG
NATIONAL
ORT
Your Eyes in the Factory!

FACTS AND FIGURES ON THE SCHENGEN AREA'S EXTERNAL BORDERS

By land, sea and air

The external borders of Schengen in numbers

644 air border crossing points

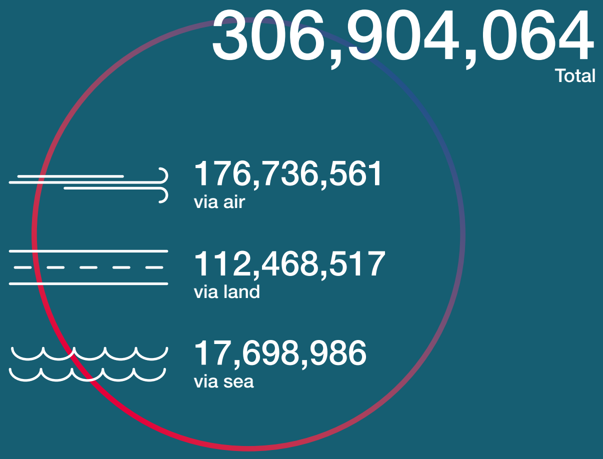
7,721 km land borders

maritime borders 42,673 km

26 countries

Source: EU Commission

Scope of regular, legal border traffic per year



306,904,064 Total

176,736,561 via air

112,468,517 via land

17,698,986 via sea

Source: Projekt SMILE - SMart mobILity at the European land borders, figures from 2017

Risks and challenges

54,780 Refusal of entry at air borders e.g. due to fraudulent documents

6,667 TCN with fraudulent travel documents at BCPs on entry to the EU/Schengen

361,636 Number of detected cases of illegal stay

504,590 TCN refused entry or stay (Source: SIS statistics)

4,481 Refusal of entry at sea borders

150,114 Detections of illegal bordercrossing at the EU's external borders

2,258 Detections of clandestine entry e.g. people hiding in trains, lorries and other vehicles

131,641 Refusal of entry at land borders

Source: Frontex Risk Analysis (unless stated otherwise) Figures from 2018

EES PREPARATIONS AT AIR BORDERS

Now Mainstream: Automated Border Control

Today, over 300 secunet easygates are already in use at major international airports, including in Germany, Austria, the Czech Republic and Iceland. The latest installations were completed in Lithuania, Poland and Hungary. Automated border control systems can help to compensate increased workloads and waiting times resulting from the introduction of the European Entry / Exit System (EES).

In combination with electronic identity documents, automated border control systems such as the secunet easygate accelerate border control through largely automated processes. The majority of passengers who previously had to stand in queues at the border control counter can now undertake the border crossing by themselves instead.

The automated process is quite simple and has already been widely used throughout the world. Passengers are therefore increasingly familiar with it. The secunet easygate checks the authenticity of the presented electronic identity document both optically and electronically. In addition, the system reads the facial image of the traveller from the chip in the electronic identity document and compares the biometric data with the live image of the individual. This all takes place within a few seconds. Travellers have already used secunet easygates around 75 million times. The most recently installed systems are those at the international airports in Vilnius (VNO), Liszt Ferenc in Budapest (BUD), Debrecen (DEB), Chopin in Warsaw (WAW) and Warsaw Modlin (WMI).

All parties involved benefit from the automation: border police officials are relieved as they primarily monitor the process from adjacent monitoring workstations, allowing them to concentrate on those passengers where further investigations are necessary. Airports benefit from higher passenger throughput. Last but not least, those travelling can enjoy shorter waiting times and the option of taking charge of the process themselves.

secunet easygates at Vilnius Airport, Lithuania

> › We are very happy to work with a flexible and experienced supplier who can provide us knowledge on how to implement a solution that best suits our expectations from best practices in other airports. ‹
>
> Lina Laurynaitytė, Technology Project Manager, Lithuanian Airports (LTOU)

The European states are currently under increasing pressure to enhance their border control processes: with passenger numbers continuing to rise and unchanged infrastructure, the introduction of the EES from 2022 onwards would mean largely increased workloads at the border. This is because the new system will require far more comprehensive checks and the collection of biometric characteristics for passengers from outside the Schengen area, also known as third country nationals (TCN). Unfortunately, longer queues at borders can therefore be expected. However, this increased workload can be minimised by using automation and process optimisation at critical points: all passengers who do not require thorough checks at the border control counter can directly proceed to the automated systems.

Automated border control systems are not only available as single components, but also as elements within more extensive solutions. secunet border gears is a complete product portfolio with a range of interoperable components that already cover the requirements of the EES. They can either be integrated individually as part of existing infrastructures or as a whole new system – completing a modular and future-proof border control infrastructure.

In many European automated border control projects using secunet easygates, the secunet easyserver is also installed. This central server infrastructure ensures e. g. reliable, fast and secure access to police background systems, public key infrastructures (PKI) and master lists.

The border control products from the secunet border gears portfolio have been used successfully for many years, while taking into account the respective customer-specific as well as country-specific requirements. Each new implementation implicitly incorporates know-how from the collaboration with other airports and security authorities.

Georg Hasse
georg.hasse@secunet.com

10 YEARS OF THE SECUNET EASYGATE: SECURITY AND USER CONVENIENCE AT BORDER CONTROL

The cornerstone for the secunet easygate was laid in 2009 with the launch of the EasyPASS pilot project at Frankfurt am Main airport. As a general contractor for the Federal Office for Information Security (BSI), secunet was responsible for the planning, implementation and evaluation of the project, together with the integration of the whole system. secunet delivered the secunet biomiddle software platform, which makes the EasyPASS system uniquely flexible, and supported the testing and development of this new border control technology.

Since 2010, EasyPASS is an integral part of the border control strategy of the German Federal Police. Developed in close collaboration with the Federal Police, the current generation of eGates features exceptional protection against circumvention as well as optimised intuitive user experience, which enables fast passenger processing times. In the summer months of 2019, EasyPASS reached a user record with more than 2 million passengers per month, who chose to pass the border via automated border control systems at German airports.

“Automation is One of the Key Elements”

In Interview: Petr Malovec, Head of the National Border Situation Centre, Czech Border Police

COL. Mgr. Petr Malovec Ph. D. has been working in the area of border control since 2001. In 2008 he started extensive activities in terms of deployment of the biometrics and related PKI infrastructure at the border control procedures that ended with the successful implementation of the Automated Border Control (ABC) system at Vaclav Havel Airport Prague.

As the head of the National Border Situation Centre he is in charge of the successful deployment of all ICT technologies and systems related with the border control protection including wide range of use cases from the stationary, mobile up to the ABC control.

Petr Malovec

Czech Border Police

What are the implications for border control due to the implementation of the EU Entry/Exit System?

It is more than obvious that we have to enhance the functionality of the recently operated stationary border control solution to be fully compliant with EES regulations. However, aside from the functionalities the overall throughput of the border control is one of the main challenges that we have to focus on. There is a completely different setup for Vaclav Havel Airport in Prague compared to other small airports with significantly less throughput of travellers, especially TCN travellers.

Which measures is the Czech Border Police taking towards the implementation of EES?

Currently we conducted a comprehensive project study that also comprises a detailed design phase which will help us to determine appropriate measures. All study findings are continuously discussed among all stakeholders at Prague Airport and other airports to address, for example, redesign measures of already existing border control locations. We do believe that automation is one of the key elements to support the whole process. With regards to biometric enrolment as required by the EES, our study determined the need for an efficient solution that ensures an automated enrolment of facial images that are compliant to all relevant standards and implementation acts. While this is high on our wish list – it is not easy to find.

Could you please share your experience regarding the use of eGates (Automated Border Control gates) by third country nationals (TCN)?

Just recently we opened the ABC system in Prague – better known as EasyGO – for nationals from South Korea. We are evaluating it as a temporary measure during the arrival of a daily flight from Seoul carrying an average 90% of TCN travellers. The brief evaluation so far has shown that opening ABC gates for TCN is beneficial and we do plan their usage for the EES use-case scenario ”exit” – when leaving the country.

Which challenges poses a potential Brexit for the border control process at Vaclav Havel airport in Prague?

In a favourable scenario, UK travellers would be considered as Freedom Of Movement (FOM) travellers and would therefore be eligible to use border control procedures assigned to EU, EEA and CH travellers. Otherwise we could face an approx. 25% increase of TCN travellers. However, we would like to take into account all feasible and supportive measures. Therefore we plan to extend the number of border control counters and eGates in both border control areas at Prague airport. We expect that maximum automation of the border control process could help us.

Aside from the importance of automated systems at airports, are mobile systems playing an important role from your perspective?

The situation in the Czech Republic is much easier since we do not have land borders. However, small green field or temporary airports need a mobile solution. The Czech Border Police is already using a comprehensive mobile solution that is capable to check all kinds of travel documents including visas stickers. It is expected that it will be enhanced with all EES features especially for verification use cases.

IMPLEMENTING THE EES AT LAND BORDERS

Diverse Scenarios

At the air borders of this world – i.e. at the terminals of international airports – it is a similar picture everywhere, irrespective of whether the airport is in Asia, Europe or North America. The measures that border control authorities are taking to prepare for the introduction of the European Entry/Exit System (EES) at air borders are also comparable. This is not the case however at land borders as each is considerably different; and there still appear to be more questions than answers with regards to the introduction of the EES.

Anyone who has ever travelled to the US will know that long waiting times must be reckoned with because biometric data are collected at the border. With the introduction of the EES in Europe this will be the case here, too – affecting travellers from third countries (third country nationals, TCN) who travel to or leave the Schengen area.

At airports, both self-service terminals for pre-registering third country nationals and eGates for the automated processing of Freedom of Movement (FOM) travellers will play a crucial role in guaranteeing an efficient border control process. These types of technologies are comparatively easy to roll out at airports, since the use case scenario is almost always the same: passengers cross the border within the airport on foot, after undergoing document and identity checks at stationary counters or automated border control systems.

Individual land borders

Land borders come with a number of challenges, however, starting with the fact that no land border looks like another. Major border crossings have sometimes various buildings, surrounded by car parks, roads and rail routes. Small border crossings, on the other hand often have almost no infrastructure at all. Further, land borders not only have pedestrians crossing – like the passengers in an airport – but also cars, trucks, buses, trains and even bicycles. There are not only people who need to be checked, but vehicles as well.

As in other border control scenarios, longer waiting times can be anticipated at land borders in the future due to the required acquisition of the biometric characteristics of travellers. The amount of work required to enrol and check the data of a person at border control counters will increase. As a result, border control officials may no longer be able to fulfil their own sovereign and security-related tasks.

Furthermore, the space available at border crossing points is often very limited. There is a lack of both external infrastructure for additional car parking places and also space for new border clearance systems to speed up the border control process.

The EES regulation requires that the same comprehensive scope of checks are guaranteed at every border control station – at any location, any time and any situation – irrespective of whether it is an air, land or sea border; and independent of the respective infrastructure, the border control process and the traveller's method of transportation. The same quality of biometric data collection and verification must also be guaranteed under all circumstances.

States with land borders face the biggest challenge here: how can biometric data be collected effectively when checking people in cars or buses? How do land borders comply with the EES regulation without waiting times exceeding all reasonable limits? Furthermore, how can checks be carried out to the same high quality standards everywhere, given all these challenges and adversities?

Multi-stage processes

In order to fulfil the EES requirements it is necessary to also have a multi-stage process at land borders, which involves the pre-registration of third country nationals. Research carried out by secunet has shown that many security authorities consider both self-service kiosks for pre-registering third country nationals as well as mobile systems – portable solutions and hand-held devices. The focus lies on the kiosk systems: pedestrians, car drivers, bus passengers, lorry drivers can enter their data on their own before proceeding to a stationary counter or – depending on the respective scenario – directly to the border post.

This relieves the pressure at stationary control, and border police officials can focus on their actual tasks. Further, capturing the biometric data at self-service kiosks as part of the preregistration process, guarantees a continuously high data quality. Furthermore, the kiosk systems are monitored – a key requirement of the EES regulation.

Strict guidelines

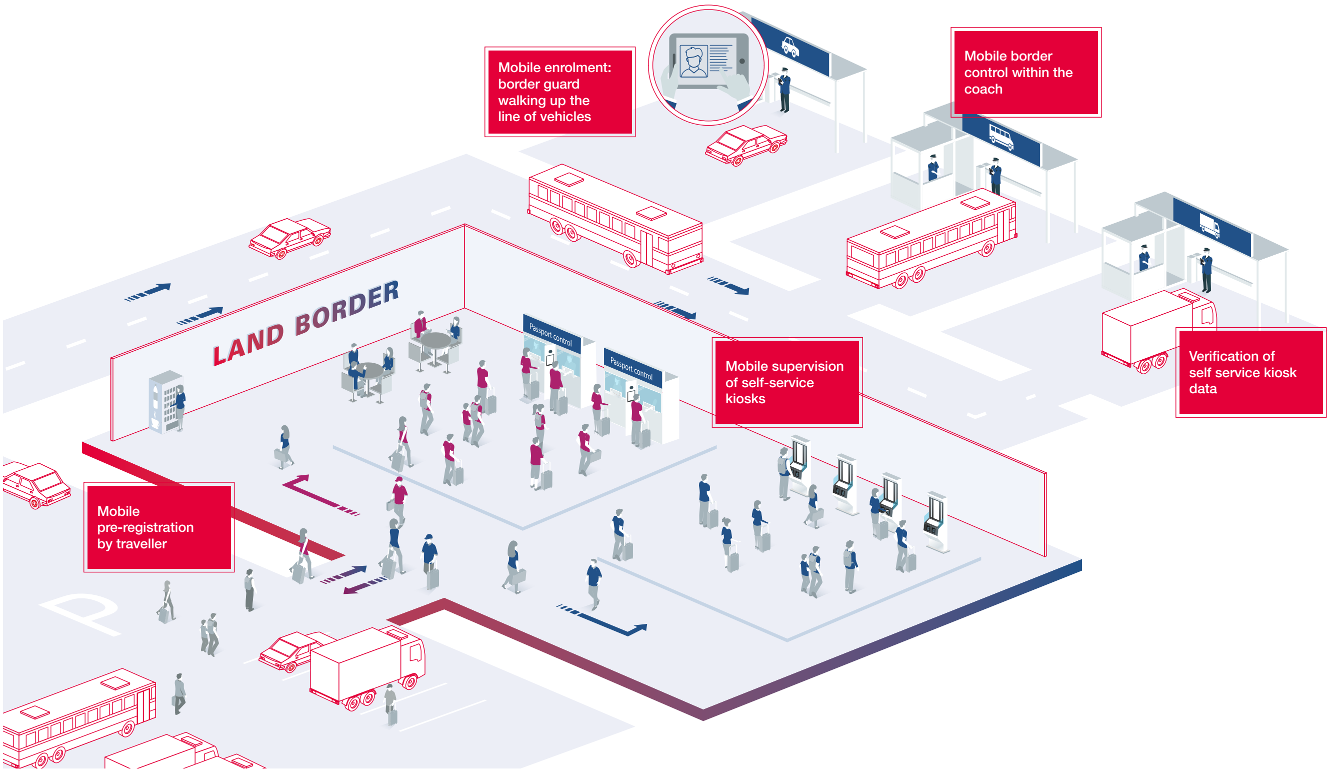
The kiosk systems themselves need to fulfil the strict requirements of the EES regulation. These extend for example to specifications regarding biometric data, e.g. facial images must be captured as high-quality, front-facing photographs in accordance with ISO/IEC 19794-5:2011.

In addition, there are high requirements for the protection against circumvention: so-called 'presentation attacks. These fraud attempts using manipulated biometric characteristics, such as masks or falsified fingerprints, need to be identified which includes that liveness detection for face and fingerprints must be ensured.

Mobile systems play an important role when checking passengers travelling on trains and in buses and carrying out pre-checks on those travelling in cars. Here it is conceivable that several border control officials will check multiple vehicles at the same time ("cluster"). With respect to these scenarios, it is important that the same stringent requirements apply everywhere to capturing and checking the biometric data as well as to verifying identity documents – irrespective of whether the data is collected and verified by means of stationary, mobile or self-service kiosk methods. No loopholes must be allowed to arise.

The use of self-service and mobile systems at land borders enables to compensate the increased efforts resulting from the additional process steps required by the implementation of the EES. More than at airports, it is a matter of taking the individual circumstances into account.

Frank Steffens
frank.steffens@secunet.com


Mobile enrolment: border guard walking up the line of vehicles
Mobile border control within the coach
LAND BORDER
Passport control
Passport control
Mobile supervision of self-service kiosks
Verification of self service kiosk data
Mobile pre-registration by traveller

“High-Quality yet Efficient Collection of Biometric Data”

Interview with Bernd Kowalski, Head of Cyber Security for Digitisation and Electronic Identities in the German Federal Office for Information Security (BSI)

Could you briefly outline the goals and responsibilities of the Smart Borders group?

The BSI’s Smart Borders project group is part of the national Smart Borders project group under the leadership of the Federal Ministry of the Interior, Building and Community (BMI). We have been involved in the design and implementation of the European Smart Borders programme since 2014, together with the Federal Police and Federal Office of Administration. With the adoption of the regulation on the European Entry/Exit System (EES) the BMI founded a national, inter-agency project group which is responsible for implementing the EES and ETIAS (European Travel Information and Authorisation System) in Germany. The new systems provide the opportunity for comprehensive identity management based on biometric data for all third country travellers. We are dealing, for example, with the connection to the new European central systems which yet have to be implemented as well as the digitalisation of the border control process at Germany’s external Schengen borders. A further aspect is the access by other national migration and law enforcement agencies to the EES. The BSI supports the operational police authorities in this process on the basis of its legal powers.

Which standards and technical guidelines support optimal implementation of the EES?

The pivotal focus of all guidelines is the EES regulation itself. Different from other legislation, detailed provisions regarding access rights and respective procedures are defined here in the context of the EES processes. Both the delegated and the transposition acts, which have been drawn up together with the member states, are supplementary to the technical implementation. From the perspective of the member states these requirements specifications do not go far enough, however, since they ultimately only illustrate the view of the central system regarding data delivery and retrieval. The BSI has therefore been commissioned to develop other implementation-related requirements specifications for the technical components of the EES. In this context, the relevant technical guidelines are, first and foremost, BSI TR-03135 for official document verification and BSI TR-03121 for the biometric components of border control. In addition, the BSI is currently working together with the operational authorities on the process guidelines for official identity management in the context of EES. The intention is to make these specifications available for all member states as a European version in 2020.

Where do you see the biggest challenges for the implementation of processes for collecting and verifying biometric data at border control?

The EES regulation is taking an interesting new approach with respect to the requirements for biometric data. Rather than following the usual approach in criminal prosecution of taking all ten fingerprints, this approach requires only four fingerprints, as well as a facial image to be taken. The latter therefore plays a much more important role, as we also know from the use in travel documents, where the facial image has established itself as the core interoperable biometric feature worldwide. The quality of biometric data collection at the border is therefore crucial for the usability of the data obtained in the European central system. In the context of technical regulation BSI TR-03121 the BSI defines a comprehensive catalogue of requirements for high-quality

Bernd Kowalski joined the German Federal Office for Information Security (BSI) in 2002. Currently he is in charge of the divisions “Certification and Standardization” and “Cyber Security for Digitisation and Electronic Identities” where his activities cover all aspects of BSI certifications, certain ID-solutions and support of the digitalization projects of the Federal Government like BSI Certification based on Common Criteria, IT-Grundschutz certificate, and cyber security aspects of eHealth and Smart Metering/Smart Grids, Industry 4.0, intelligent transport systems und the digital administration.

Bernd Kowalski
German Federal Office for Information Security (BSI)

yet efficient collection of biometric characteristics in the border control process. The industry has been called upon to develop innovative solutions for all application scenarios in the frameworks defined.

In your estimation, will other member states also orientate themselves towards the BSI’s technical guidelines?
Due to the significant complexity of the European project we anticipate that other member states, too, will follow our guidelines with great interest. The BSI’s technical guidelines are available to view on our website http://www.bsi.bund.de/EN. The BSI consciously defines guidelines with a general focus and without specifically German features; they can be profiled accordingly to suit a particular purpose.

Quality Is Key – Especially when It Comes to Biometric Reference Data

Interview with Prof. Christoph Busch, Professor of Computer Science / Biometrics at the Norwegian Biometrics Laboratory (NBL), Norwegian University of Science and Technology (NTNU) and the Darmstadt University of Applied Sciences (HDA)

You have been focussing on data quality in the area of biometrics for a long time. Can you give us a brief abstract of your research?

The significance of image quality of biometric reference data has been acknowledged for many years now. When biometric passports were introduced in 2005 we compiled technical reports on this subject in conjunction with the standard ISO / IEC JTC1 SC37 and documented the state of the art technology at the time. Since 2010, together with the US National Institute of Standards and Technology (NIST), the German Federal Office for Information Security (BSI), the German Federal Police Office (BKA), secunet, and the Fraunhofer Institute for Computer Graphics (IGD) we have researched new algorithms that measure the quality of fingerprint images. This development, the NFIQ 2.0, became an international standard (ISO / IEC 29794-4) in 2017 and is available on an open source basis.

How is the quality of biometric data assessed?

The groundwork was established with the framework standard ISO / IEC 29794-1, which defines the procedure for all biometric modalities. The quality rating ('score') is intended to be predictive of the later successful recognition, this means that a good score predicts that recognition is reliably possible. In the NFIQ 2.0 project we investigated which characteristics from a fingerprint image are relevant for this. The NFIQ 2.0 software is a good solution for optical fingerprint sensors.

What are the specific challenges when dealing with biometric data in large databases?

When it comes to identification solutions the growing size of the database not only necessitates a longer transaction time, but also an increased risk of a false decision, since the False-Positive-Identification-Rate (FPIR) is inherently linked with the size of the database and increases in a linear fashion. This makes it all the more important, that only high-quality images are captured and stored.

Prof. Christoph Busch
https://christoph-busch.de/

Prof. Christoph Busch received his Ph.D in 1997 from the Computer Science department at the Technical University of Darmstadt. In the same year he joined the Fraunhofer Institute for Computer Graphics (Fraunhofer IGD) as Head of the department Security Technology.

On behalf of Fraunhofer IGD, Professor Busch works on standardising biometric systems and is chair of the German Standardization Body on Biometrics (DIN-NIA37). He is head of the German Delegation in the Plenary of ISO / IEC JTC1 SC37 (Biometrics) and leads Working Group 3 (Biometric Data Interchange Formats).

Since the 2005 summer semester Prof. Christoph Busch has represented the System Development department at Darmstadt University of Applied Sciences. In autumn 2007 he was moreover appointed professor at the Norwegian Information Security laboratory (NISlab). Furthermore, since 2007 he has taught at the Technical University of Denmark (DTU).

Why are standards important for assessing the quality of biometric data?

The international standards offer not only the opportunity to simply exchange data, as we have already been practising using biometric passports for 15 years. The use of standards in quality evaluation will additionally lead to all countries that contribute to a large, shared European biometrics database being able to achieve a consistent level of quality. Moreover, this will avoid problematic vendor lock-in situations in the EU member states, i. e. dependencies on certain suppliers.

What are the ramifications of poor-quality biometric data in databases?

Poor image quality holds a significant risk of high error rates, as well as both false rejection (causing inconvenience) and false acceptance (jeopardising security). These issues can be avoided for fingerprint images (thanks to ISO/IEC 29794-4) and iris images (thanks to ISO/IEC 29794-6). We will begin ISO/IEC 29794-5 standardisation for facial images this summer. I am grateful to every expert who takes part in this process.

Geysers, Glaciers and Electronic Passports

With its unspoilt landscapes set amidst active volcanoes and perpetual ice, Iceland attracts increasing numbers of tourists from all over the world. Yet it is not only Iceland's tourism that is responsible for the rising passenger numbers through Keflavik airport, which is situated close to the capital, Reykjavik: the airport also serves as a hub for intercontinental flights between Europe and North America. Because of this, Iceland began to completely renew the border control infrastructure years ago. Their most recent addition, however, mainly benefits Icelanders: thanks to its new infrastructure the island nation can issue high-secure electronic identity documents (eID) to its citizens and check them when its citizens exit or enter the country.

Registers Iceland ('Þjóðskrá Íslands' in Icelandic), the authority that operates the Icelandic civil registry, is in charge of the project. The aim was to find an eID solution that would put security at the top of the agenda and ensure the confidentiality, availability and integrity of the personal data of Iceland's citizens at all times. Registers Iceland therefore decided to implement a public key infrastructure (PKI) based on secunet's eID PKI Suite. The high security standard of this solution is proven by the certification of its CA Kernel – a core component essential for the issuance of electronic certificates – in accordance with Common Criteria EAL 4+.

secunet has provided Registers Iceland with a turnkey full-service PKI solution that includes all software components for protecting the biometric data of Iceland's citizens and regulating access rights (EAC-PKI) – as well as the components which ensure the integrity and authenticity of the travel documents (ICAO-PKI). The solution can be configured flexibly to a large extent, which keeps the operational administrative workload very low and makes the system future-proof. The high degree of standardisation also allows the implementation of future legal and technological requirements.

Recently, the new PKI has been connected to the automated border control systems (eGates), which were brought into service back in 2017 at Keflavik airport. The secunet easygates can be used by Icelandic citizens, citizens of the European Economic Area and Swiss citizens. Efficiently and securely, they check the authenticity of official documents optically as well as electronically, read the traveller's electronic facial image, and compare the biometric data with a live image.

✉ Christian Rutigliano
christian.rutigliano@secunet.com

SERVICE-ORIENTED IMPLEMENTATION

"Besides the excellent performance and usability of the PKI system during operation, secunet's service concept as well as the profound expertise of the whole team are remarkable," says Þorvarður Kári Ólafsson, Programme Manager ID and Travel Documents at Registers Iceland. "In this complex project, we always had someone at our side who immediately solved the challenges to our complete satisfaction – even on-site at short notice when it was necessary."

A Wealth of Future Topics

In June 2019 there was a change of management at the helm of secunet: Dr. Rainer Baumgart, who has spent over 18 years as CEO of secunet Security Networks AG, retired from the company and the top job passed to Axel Deininger. secuview spoke with both the former and new CEOs about secunet's past and future as well as the development of the IT security industry.

secunet is going through its first change of management for 18 years. How significant will be the upheaval that this brings?

Deininger: secunet currently has an outstanding market position. We are the leading provider of high-quality IT security for public authorities and companies in Germany. In addition, we operate in a positive market environment. Business has continued to thrive during this current year, too. All this shows that, in many areas, it makes sense to capitalise on continuity. Naturally, we will also be making some alterations to our course that will drive us forward both in organisational and substantive terms, since the market is evolving and this provides us with new business opportunities.

Which are the areas where you plan to make changes?

Deininger: For example, we will be addressing the industrial segment with greater intent in the context of Industry 4.0. To date we have been particularly well-positioned in regulated markets. Strict security requirements apply to the IT infrastructures of public authorities where sensitive or classified information is concerned. Solving these types of tasks, which involve demanding challenges in terms of security technology, has been at the core of secunet's business for over two decades. This also includes our biometric solutions, which are used in automated border control for example. We can now assume that further regulated areas will be added in the future. We have had the IT Security Act in Germany since 2015, which obliges operators of critical infrastructures to do more for their cyber security. Further regulations will follow.

A rethink is taking place in non-regulated markets too, however; ultimately, IT security incidents can lead to major financial losses. Plus, as the digital transformation takes hold IT systems are becoming increasingly connected – with the internet, too – which they were not originally designed to do. The best example of this is industry. Some machines in industrial environments are in use for 30 years or more. To fully exploit the advantages of digitalisation there, too, in future each machine and control device will be connected – which can only work with IT solutions that establish the appropriate level of security.

Another example is international markets. secunet has already been active for many years outside Germany, primarily in other European countries and in a NATO setting. There is certainly room for our involvement in these markets to increase, though. The need for cyber security is growing all over the world and we have enough references to obtain international recommendations as well, even in areas that are not state-regulated.

Where can we expect continuity?

Deininger: On one hand we will continue with our strong IT security business in the public sector, offering tried-and-tested solutions. On the other, secunet has also always defined itself through its proximity to universities and research institutions. For instance, we maintain a good relationship with the Horst Görtz Institute in Bochum, with if(is), the Institute for Internet Security in Gelsenkirchen, with TU Dresden and with TU Ilmenau, to name but a few. We definitely want to maintain this proximity to science, since this is one of the keys to our innovative strength. The other key is our ability to attract and retain the right employees.

Were these ingredients also part of the recipe that turned secunet from a start-up into the market leader?

Baumgart: Absolutely, they were definitely part of the mix. Even at the moment of flotation on the stock market in 1999, secunet, originally a TÜV spin-off, was involved in protecting IT networks by means of cryptographic mechanisms, along with many other providers. Our ability to bring the right experts on board put us in the position to

Axel Deininger (left) and Dr. Rainer Baumgart

Axel Deininger was appointed to the secunet Security Networks AG Board in January 2018 and took over as Chair in June 2019. Prior to joining secunet he spent over ten years working for the Munich-based corporate group Giesecke+Devrient, most recently as Group Senior VP and Head of the Connectivity & Devices Division at G+D Mobile Security GmbH. In the course of his career the industrial engineer has worked for companies such as Siemens AG, Infineon Technologies AG and Samsung Semiconductor Europe GmbH.

Dr. Rainer Baumgart has worked at secunet since the company was founded in 1997 and has sat on the Board since the company converted to a stock company in 1999. He took over as Chair of the Board in 2001. Holder of a PhD in Physics, prior to joining secunet he worked for RWTÜV and, from 1995, headed up the Information Security department at TÜV IT GmbH in Essen.

expand our portfolio – with public key infrastructures (PKI) for example, which were utilised in government-certified trust centres for issuing certificates. Our broader positioning helped us among other things to survive the bursting of the dot-com bubble – and to free ourselves from the niche.

At the start of the Noughties we developed the SINA security architecture at the behest of the German Federal Office for Information Security (BSI) – this was a milestone. Today, a large number of public authorities use SINA to guarantee high levels of security. 2004 then brought two momentous changes for secunet: firstly, we became IT security partner of the Federal Republic of Germany. Secondly, the arrival of the new majority shareholder, Giesecke+Devrient, brought us further stability. This remains the situation today. We were given the opportunity to prove our skills through involvement in major infrastructure projects for public institutions like ELSTER, the 'Netze des Bundes' (Networks of the Federal Government], or the German Federal Armed Forces' Management Information System.

What was and remains important for secunet is collaboration with institutional partners: we have had an excellent and close working relationship with the BSI for many years. We also have a good rapport with the European cyber security agency ENISA. Furthermore, we have been helped by technology partners such as atmedia, S.I.E and Siemens: they enabled us to offer our clients complete solutions comprising hardware and software.

THE NEW SECUNET MANAGEMENT TEAM

As of 1 June 2019 the Board at secunet Security Networks AG has comprised the CEO Axel Deininger, along with Torsten Henn, Dr. Kai Martius and Thomas Pleines. Chief Operating Officer (COO) Torsten Henn and Chief Technical Officer (CTO) Dr. Kai Martius, who have been with the company for many years, were newly appointed to the Board. Chief Financial Officer (CFO) Thomas Pleines has been a member of the Board since 1999, when the company converted to a stock company.

Has the development that secunet has experienced also been reflected in IT security as a whole?

Baumgart: You can certainly say that. 30 years ago IT security was still something for nerds. But time has proved the nerds right. Little by little, many people realised that the issue of IT security is a crucial aspect in Germany and Europe in order to guarantee national and European sovereignty. The IT security sector, which was still in its early days then, has grown and become increasingly professional.

I am also convinced, though, that this is still just the start and it's going to get extremely exciting in future. There are new challenges and pressing questions that need to be resolved. I am following the developments around post-quantum cryptography with particular interest. If powerful quantum computers become available in future cryptographic methods must be able to withstand them. Therefore, encryption technology is in the process of reinventing itself once more. In years to come, perhaps the last few decades will be known as the prehistoric phase of IT security. It's been fun to be part of it.

Herr Deininger, which specific topics for the future can be found on your to-do list alongside post-quantum cryptography?

Deininger: One topic that is just around the corner is 5G. For the first time, the new mobile communications standard is offering the opportunity for end-to-end implementation of cryptographic security mechanisms from the traditional world of IT within mobile communications. Biometrics, too, will become even more important in the future. Ultimately, nobody can remember 50 passwords! Mobile applications are another topic: with the German Federal Police's app for mobile identity checks we have demonstrated that apps can be implemented in areas where high levels of security are paramount. We are keen to build on this. We are already successfully represented in the health market thanks to the secunet konnektor; and the next developments are imminent. The topic of automotive security, an area that secunet has been active in for a long time, will grow in importance in future due to the gradual implementation of autonomous driving and vehicles becoming increasingly connected.

Of course, the list wouldn't be complete without mentioning artificial intelligence. AI is guaranteed to lead to some revolutions in IT and beyond. Hackers will try to exploit it for themselves, but we will also do that. Another topic: cloud security will play a bigger and bigger role, both for companies and public authorities. We recently therefore founded the joint venture SecuStack together with Cloud & Heat Technologies GmbH. SecuStack offers cloud-based solutions for applications deemed critical for security and enables many customer groups to enter the cloud for the first time.

A wealth of promising topics abounds in the field of IT security. Industry 4.0, which I alluded to at the start, is another pivotal topic. I am looking forward to addressing all these topics together with my colleagues here at secunet, and my view of the future is an optimistic one.

Herr Baumgart, what advice would you give your successor for the future?

Baumgart: In my view, it has always paid off to keep the idea of partnership in view and to capitalise on collaboration between the private sector, public authorities, science and research. The German IT security industry and the public authorities in their environment are shaped by mutual respect and desire to cooperate, which I have always found positive. This makes it easier, therefore, to solve the often complex challenges facing us; and which IT security will always face.

How will you keep yourself busy in the coming months?

Baumgart: First and foremost I shall be spending more time with my family, which I am very much looking forward to. My grandchildren may have missed out a little up to now. I also own an old Porsche tractor that is in urgent need of repair and restoration. I certainly won't be sitting around twiddling my thumbs.

Many thanks to you both for talking to us.

DIGITAL REVOLUTION IN AGRICULTURE

Farming and IT Security

Agricultural machines have reached a level of development that cannot be significantly boosted further using traditional approaches. In order to continue to position itself as a leader in the market, agricultural machinery manufacturer CLAAS is therefore focussing on new and forward-looking business segments. These are connected with the wide-ranging digital transformation that the agricultural sector has seized in the meantime – albeit later than other sectors – but all the more thoroughly since it promises further major revenue and efficiency benefits. To fully exploit the potential of this development CLAAS is investing in IT security and has, among other things, established a public key infrastructure (PKI) as the core cryptographic authority for all services.

The high, constantly growing proportion of electronics and software in agricultural machinery is a clear indicator: the digital revolution on farms is in full swing. Today, agricultural machines are connected to each other, to the IT backend, or even to cloud-based IT systems. In the meantime, important framework conditions are also in place: mobile network coverage in the agricultural sector has been significantly expanded, for example.

One application scenario that is currently resulting in major changes to farming is Smart Farming, or Precision Farming. This enables disparities in soil condition to be assessed, even within a single field, and to be exploited through optimal cultivation. Alongside this, digital processes can structure the everyday routines of agricultural enterprises in various ways, making them more efficient: using Parallel Driving, agricultural machines can be automated and driven across the field in parallel lines, controlled by GPS. Predictive Maintenance analyses the condition of agricultural devices so that maintenance tasks can be carried out at the precise moment they are actually required. Software updates and the activation of other services and functions can be carried out over the air, which saves time and effort.

Wireless data transmission

CLAAS offers its customers digital services for these and other application scenarios and is always developing them further. The technical realisation of the services makes it necessary to transfer data inter alia via wireless interfaces, e. g. via mobile communications or wireless networks. It is important to protect this data flow: to preclude manipulation, there must be measures in place at all times to ensure that the data come from trustworthy CLAAS authorities. Moreover, protecting personal data and CLAAS's intellectual property can make it necessary to encrypt data. A further crucial aspect is safeguarding the CLAAS agricultural machines from hacker attacks.

IT security is well-known from the world of the internet and corporate IT; for agricultural machines, however, it is a relatively new field. CLAAS therefore launched its Security@CLAAS project at the start of 2016, to satisfy the requirements of IT security for connected CLAAS machines and services. The cyber security programme, which was rolled out throughout the company, aimed at end-to-end safeguarding of the various digital use cases against unauthorised manipulation, together with protection of confidential data.

Precision farming enables farmers to cultivate sections within a field for optimum success according to the soil conditions in situ by, for instance, spreading varying quantities of mineral fertiliser as required.

In secuview 2/2016, Thomas Böck, Member of the CLAAS Group Executive Board and Head of the Technology and Systems department, introduced the Security@CLAAS project in an interview. Readers who would like to know more can download the edition in PDF format via the following URL: www.secunet.com/en/service/customer-magazine/

CLAAS successfully concluded the project in September 2018. “Through Security@CLAAS we have initiated a palpable process of change throughout the company,” says Thomas Ehl, Project Director at CLAAS. “Following the specification of requirements in the form of a workshop, as well as risk analysis and creation of a security concept for the usage scenarios, we have developed and established a security manifesto that acts as a company-wide standard for safeguarding functions and services.”

PKI as core technology

The last milestone was the introduction of a CLAAS product PKI (public key infrastructure). This core service for cryptographic functions generates electronic certificates that verify that specific data come from a trustworthy source, and regulates access to these data. For many years PKI solutions have been a tried-and-tested mechanism in other areas where confidentiality and data integrity are critical: for example, at border controls they ensure that the authenticity of electronic identity documents can be checked reliably and quickly. PKI-supported processes are also utilised with HTTPS-based web servers, which are used in online banking, for instance. PKI solutions usually run automatically in the background, largely unnoticed by end users. This is the case with the CLAAS solution too.

In establishing the IT security measures the CLAAS project team received considerable support from secunet. “secunet delivered both conceptional input and the technology for the CLAAS product PKI,” Ehl adds. “Specifically, what tipped the balance was the flexibility and the ease with which this

Parallel driving involves directing agricultural machinery, here combine harvesters, across the field using GPS.

Digital technologies help to map yields.

technology was integrated within the CLAAS IT systems. This flexibility was particularly apparent during the start of production phase for the connected electronic components: secunet was able to make adjustments even at the very last minute. I must also highlight the speed with which the CLAAS product PKI was set up: it took a mere six weeks from the start of implementation to the point of commissioning."

An important precondition for the success of a project of this type was fulfilled from the beginning: "We received consistent backing from the CLAAS management team," says Harry Knechtel, secunet's Project Director on the project. "The collaboration with the dedicated project team and the goal-oriented, inter-departmental cooperation were also excellent."

Only the start

As so often is the case in IT: the successful conclusion of the project cannot mean the end of implementing IT security at CLAAS. Cyber attackers do not sleep; the bar therefore constantly needs to be raised. The Security@CLAAS project created a forward-looking architecture that can also cover the security of future applications. Ultimately, though, it must be understood purely as a starting point in a process of continual improvement, which CLAAS will now flesh out in full.

Alexander Kruse
alexander.kruse@secunet.com

AUTOMOTIVE SECURITY

Testing Security Efficiently – Through Greater Standardisation

Penetration tests now form part of traditional IT domains such as websites and services or IT infrastructure, not only as the done thing, but because they represent a mandatory measure for the respective operator. With the modern vehicle having increasingly developed into a mobile, connected infrastructure in recent years, the demand for carrying out regular, development-linked vehicle penetration tests has increased in this segment, too. This is essential, since attacks on vehicles are facing a boom in popularity.

Some of these attacks have received prominent coverage in the media: these include, for example, the relay attacks that enable criminals to steal vehicles that have Keyless Go systems; or the notorious Jeep hack, where security researchers took over control of a whole vehicle. In addition, there are many less high-profile instances: for a wide variety of reasons – tuning, vehicle theft, academic curiosity or recognition in the hacker community – there are groups that have specialised in hacking real vehicles. Since the reputation damage caused by a successful, publicised attack primarily affects the vehicle's brand, it is OEMs (original equipment manufacturers) in particular who are increasingly investing in cyber security. Furthermore, OEMs bear liability towards the end consumer.

Since the strategies for protecting vehicles differ greatly from one manufacturer to another, especially when it comes to verification – including penetration tests inter alia – this raises Herculean challenges for

The connected car is an attractive target for hackers.

CONTINENTAL AND ARGUS

Protect, Detect and React to Prevent, Understand and Respond: Observing those paradigms Continental not only offers pen tests to their customers but also comprehensive bumper-to-bumper cyber security solutions. In order to accomplish this by the end of 2017 Continental acquired the cutting edge automotive cyber security startup ‚Argus‘.

the supplier industry in particular. They need to fulfil the manufacturers' various specifications. This is especially tricky if the product in question represents a platform where the similarities in development only generate a competitive advantage in the strongly price-driven automotive market.

The Chassis & Safety division at Continental AG has already been affected by this development for some time. Control units, which are similarly designed for various manufacturers, must therefore nonetheless be individually tested for most manufacturers (OEMs). Each manufacturer thereby qualifies its own tools (e. g. for robustness tests) and not only demands that Continental acquire them, but also keep them operational on an ongoing basis. The training for employees on the different tools also presents a challenge for the supplier industry. There are, moreover, varying demands regarding the implementation of penetration tests. While a generally accepted tool landscape has now become established in the area of network pen tests, in the automotive domain the differing views of OEMs and the strongly heterogeneous technology environment have so far precluded almost all automation. But in times of shorter release cycles and over-the-air updates automation is becoming more necessary than ever.

At the start of 2018, Michael Gerhard Schneider, Head of Cyber Security of the VED (Vehicle Dynamics) Business Unit in the Chassis & Safety Division at Continental AG, qualified suitable tools that, based on experiences of the Corporate Cyber Security Competence Center (SCC), could be used to meet the diverse spectrum of requirements of different manufacturers. One important criterion is that these tools must always be able to cover new test cases and interfaces by means of enhancements; and also replicate new trends and technologies without going through a migration process.

To this end the VED Cyber Security business unit also works closely with its supplier secunet. The collaboration began mid-way through 2018. Initially, the known manufacturer requirements were consolidated. These flowed into the functional scope of a product that was currently still in development at this stage: the secunet redbox, a tool for automated security tests within heterogeneous project landscapes.

The secunet redbox builds on the experience and technology that secunet has used for several years to support OEMs with penetration tests and release processes for control units. The tool thereby unites automotive pen test expertise and the toolchain that secunet has developed specifically for this market.

In a workshop with Daniel Hrisca, a pen test expert at the Vehicle Dynamics business unit at Continental AG, Continental was able to gain an understanding of how the secunet redbox could be enhanced with application scenarios specific to Continental: to achieve this, a number of experts from secunet and Continental took part in a three-day hackathon in Frankfurt am Main to successfully implement a new interface specific to Continental within an earlier development version of the secunet redbox. This therefore provided the proof that it could be enhanced specifically for a particular customer.

The project reached a further milestone in spring 2019. Over the space of two weeks secunet demonstrated the powerful capabilities of the secunet redbox on a recently completed brake control unit. What made this special was that the control unit had to be tested using a test method specified by an OEM; and thus it allowed a direct comparability with other test tools. Once the control unit had been put into operation, with the assistance of Roopashree Dheenadayalan, Security Tester at Continental, the secunet redbox was able to display more findings through its automated check for possible vulnerabilities than the tool used previously.

This result convinced Continental. It also demonstrates that it is worth authorising stronger standardisation in the areas of security and robustness testing. This is the only way to create a strong automotive security community that, in future, can advocate industry-wide for protecting the roads from cyber attacks.

Alexander Siegel
alexander.siegel@secunet.com

SECURE NETWORKING IN INDUSTRY 4.0

At the Edge of the Network

Digitalising production environments is a double-edged sword: operators benefit from new opportunities, but are also confronted with a relentless onslaught of new challenges. The secunet edge solution enables connected machines to be secured – and, over and above this, answers further questions arising from Industry 4.0.

One consequence of digitalisation within the industry is that information technology (IT) and operative technology (OT), which were originally separate spheres, have become increasingly intermeshed. It is now the case that machines are controlled and monitored centrally from process IT; they work in partnership with ICT systems from business IT; and are reliant on IT services provided by external suppliers. This high degree of connectivity inevitably leads to new challenges, however. Today, operators need to get to grips with IT threats that were absent from the former working world of engineers and technicians.

In addition, the legislator has underlined the necessity of preventing against these types of threats and has set out provisions, regulations and recommendations. Examples from Germany include the IT Security Act (IT-Sicherheitsgesetz), the Ordinance on the Identification of Critical Infrastructures from the German Federal Office for Information Security (BSI-KritisV), and the BSI recommendations regarding IT in production (BSI-CS 005). These measures ultimately show the high protection requirements of the components in sensitive network areas of the production environment. Systems and machines consequently require comprehensive protection from IT impacts; at the same time,

Today, operators must deal with IT threats that were absent from the former working world of engineers and technicians.

however, they also need networking to implement data-driven operational processes. How can such a seemingly paradoxical aspiration be fulfilled?

Long life cycles, high risk

For machines that operate in process IT (PIT) life cycles of over 30 years are typical. On the contrary, modifications to components to arm machines and systems against current IT threats are not typical. The reason for this is that operators consider the failure risk entailed by these types of modifications to be too high. As the adage goes: 'never change a running system'. The risk posed by networking unprotected, outdated technology is underestimated, though. It is not simply the smooth running of the machine itself that is jeopardised; other participants in the network are also endangered – moreover, it can open up gateways for potential cyber attacks. Action is therefore required to provide machines with the necessary level of IT security.

A number of security incidents that have recently come to light illustrate how acute this need for action is: e. g. the security flaws that occurred in remote maintenance functions of up-to-date operating systems as well as ones that are no longer being updated. Another example is the successful manipulation of machine-generated data from medical devices, which was made possible by the lack of protection of the information transmitted.

Yet it would fall short of the mark to place the focus solely on the required safeguarding of machines. There are other questions to be answered as well: today, for instance, there are far-reaching demands on networking that are by no means fulfilled. Is it sufficient to connect machines to the infrastructure using cables and LAN, or should the focus be more on maintaining the machines' mobility, which requires a wireless connection via WLAN or mobile communications? How can new interfaces and standards like 5G be utilised in future? And how can connecting machines to any internal and external services or platforms be implemented in individual application scenarios?

An all-encompassing concept should – alongside the critically necessary safeguarding of networked machines – also answer these and similar questions. What is needed is an approach that combines the following aspects:

- 'Protect':
  Secure networking and regulated communication behaviour of machines
- 'Connect':
  Use of software from third party suppliers for the flexible integration of machines in Internet of Things (IoT) and Industry 4.0 application scenarios
- 'Detect':
  Security monitoring of the machines and communications to strengthen the defences against cyber attacks

Protect: safeguarding and secure networking of machines

The PIT operating principle with its machines and systems differs greatly from traditional IT. It is important to take this into account when adapting the security strategy. This is the only way to achieve successful protection from external influences and, at the same time, to ensure controlled, secure networking. A high level of security can be achieved for systems in this area of the infrastructure as well by decoupling the life cycle of machines and systems from that of the IT environment.

The secunet edge security system, which was specially designed and developed for the industrial setting, is therefore positioned at the critical interface between the machine and the network. The machine connected with the security system operates in its own network segment isolated from external influences thanks to micro-segmentation of the network. In other words: secunet edge acts like a protective cover around the machine. The incoming and outgoing communications always take the path via the security system, allowing the data flow between the network segments to be fully managed and controlled. The connected machine can therefore be afforded a high level of security, which can also be maintained at all times. In addition, only the hardened and minimised operating system of the security system is affected by fast-paced update cycles. This enables updates to take place seamlessly and the whole system to remain continuously up-to-date, without having to factor in any side effects or impacts on the machine's availability.

The long runtimes of machines mean that their data transmission is often based on protocols that are no longer considered secure. Therefore, neither the confidentiality nor the authenticity of the information exchanged can be proven. This is problematic, since falsified information that is sent from the machine to a control centre elicits false assumptions about the machine's operation. Manipulated commands sent to the machine can even lead to immediate danger for operating personnel. Consequently, protecting the information transmitted in the PIT is important. Retrofitting the appropriate measures is difficult, however, especially when the data are still transmitted using outdated interface standards. A protocol converter integrated within secunet edge solves this problem. Unsecured transmission of data in the network only takes place along the marginal path between the machine and the security system (secunet edge). From there, the conversion takes place 'on the fly', for example from unsecured file transfer protocol (FTP) to the SFTP or FTPS secure protocol methods.

Connect: flexible integration of machines within IoT and Industry 4.0 scenarios

Where networking is secure and a robust foundation is in place, the operators face new challenges. The different technologies, protocols or transmission technologies used in a production environment lead to increased complexity. Also, various interested parties want to access machines or their information for different reasons. Machine-generated data potentially need to be transmitted to IoT platforms and analysed to optimise processes as well as to minimise downtime. Or technicians need to maintain the machines remotely over the internet due to cost reasons. With these types of demands, connecting the machines to internal and external services must be done in a secure and controlled way.

The secunet edge security system contains a modular platform concept in the form of an execution environment for applications. Applications that run in it, e. g. agents of IoT platforms, applications for preprocessing data or communicating with internal services, receive controlled access to information on connected machines and can send and/or receive this information to/from the respective service securely and in a targeted way. The crucial advantage of this type of open and modular platform concept: the overall complexity is lessened by grouping the required applications on one edge computing platform. Individual IoT application scenarios do not therefore require individual solutions, and can be implemented step by step at the desired pace. Both developers and suppliers of data services, for instance in the areas of artificial intelligence or Big Data, benefit from this type of concept. They can offer their platform-independent applications securely via the secunet edge platform without the need for in-depth security expertise, and without experiencing limitations in hardware issues.

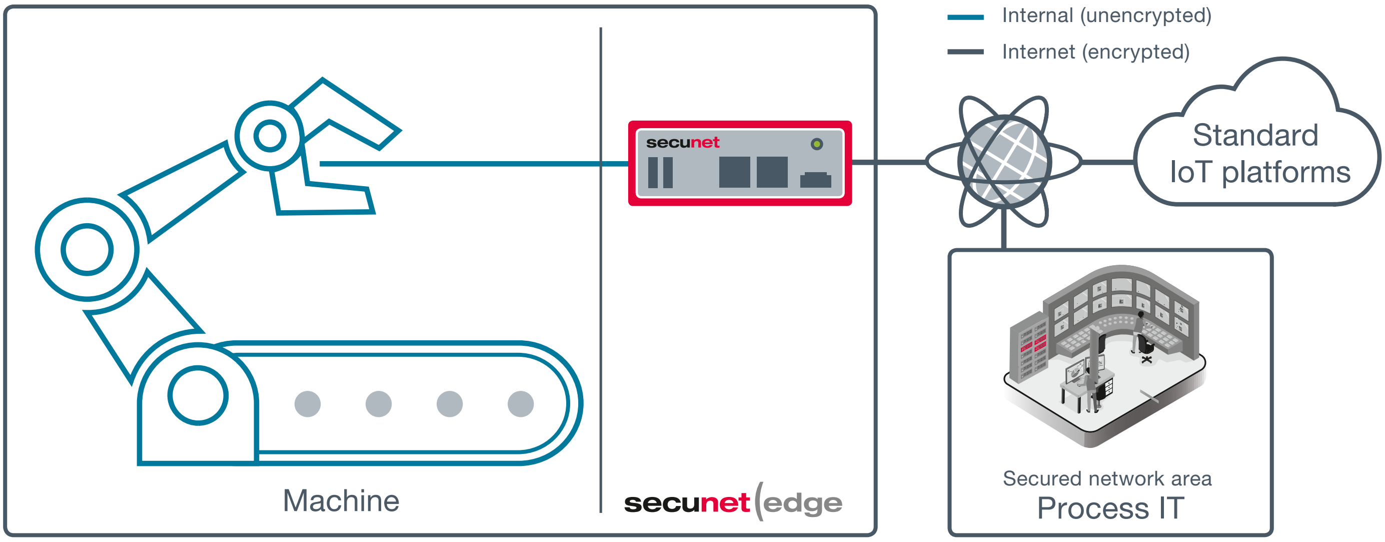
Detect: security monitoring to strengthen defences against cyber attacks

In addition to fundamental security, continual monitoring of communications to and from the machine is critical for maintaining the highest level of IT security. Security monitoring makes the information flow transparent and enables the machine's communication behaviour to be analysed. secunet edge offers an integrated sensor system in this respect that continuously captures the incoming and outgoing data traffic to the interface between the machine and the external network and evaluates it via a central analysis system.

The analysis system records the normal behaviour of a machine's communications with the help of auto-adaptive algorithms. Any abnormal communication behaviour that suddenly occurs, which can happen due to the machine being infected with malware or an attacker establishing an unauthorised connection to the machine, is then identified. The benefit of this type of behaviour analysis: it even reveals previously unknown types of attacks. This enables an immediate response as soon as a security incident occurs, and the unauthorised communication between the machine and the network can be blocked.

Hardware-based information security

Cryptographic functions, which the system implements based on hardware, are necessary for the different tasks that secunet edge performs. The fixed-installation,



certified Secure Element (SE) – comparable to a technology with a Smartcard – acts as a trust anchor and enables, for example, encryption mechanisms to be carried out, or cryptographic keys to be kept safe within a tamper-proof chip. These security functions can also be used for external applications that are executed on the platform. It is likewise conceivable to equip the machine connected to secunet edge with a digital identity and integrate it into a public key infrastructure (PKI), which creates a host of other application options (you can find examples of PKI use cases in the articles on CLAAS and ifm in this edition of secuview).

Versatile sphere of application

secunet edge not only services various requirement remits in industrial security; but also provides basic functions for implementing Industry 4.0 concepts. Here it is clear what IT security providers have been postulating for some time: cyber security technology can become an enabler when used correctly.

Furthermore, secunet edge covers not only present-day requirements but future ones too. The protective cover that the system, as it were, places around the machine is variable and can easily be adapted to meet future demands. Therefore it is not just operators retrofitting their machinery and wanting to underpin the process of digitalisation with a solid basis of IT security who benefit from secunet edge. The target audience also includes machinery manufacturers looking to equip their new machine designs with a future-proof protective cover – and, at the same time, fulfil their clients' requirements vis-à-vis securing existing machines. Last but not least, system integrators can take advantage of the edge computing platform and bring their IT services to the operator's machines.

Although in structural terms machines find themselves 'at the edge' of an Industry 4.0 network, nonetheless they play a key role. This is why it is so important to protect them adequately and to exploit their potential through new technologies.

Torsten Redlich
torsten.redlich@secunet.com

SECURITY FOR INDUSTRY 4.0

Trust Between Machines

One of the requirements for an intact communications chain is that the communication partners trust that the other party actually is the person or authority they claim to be. In everyday human communication this trust is created or denied by means of empirical experience; in contexts where security is deemed critical people utilise identity documents. What happens though if the communicators are machines, as in the highly automated Industry 4.0? In this instance the machines are allocated verified digital identities. The ifm group of companies uses a public key infrastructure (PKI) to 'personalise' its gateway components.

When it comes to automated operations using the Internet of Things the reliability of data is of paramount importance. This is because, in contrast to non-automated or partly automated processes in which existing data and the resultant actions can be evaluated by technicians, automated processes have to manage without these authorities: the data transferred are utilised according to specified schemata and activities are carried out autonomously. There are neither any additional cross-checks nor any scope for interpretation.

How can we create trust in the data under these circumstances? The decisive factor is authenticity, i. e. the guaranteed identity of the data source. Where this is provided beyond any doubt the second stage is to check whether a disruption-free, tamper-proof connection can be established between the data source and the recipient using the resources available. If this is the case, full trust can be placed in the data that have been transferred.

The ifm group of companies manufactures and sells sensors, controls, software and systems for industrial automation and digitalisation – in other words, for Industry 4.0. In order for a digitalised industry to function, it is first important that components such as gateways, for example, are able to connect with the relevant IT infrastructure. In addition, they require an identity that allows them to be clearly allocated within the infrastructure and addressed accordingly. We are speaking figuratively of the 'personalisation' of machinery components. Only in this way can an intact communications chain composed of numerous components be created, for example from the sensor at the beginning of the chain to the processing IT system at the end, whereby it is guaranteed that all elements are reliable.

PKI as an approach

In 2018 ifm was developing a new Industry 4.0 product line and was searching for a solution to personalise these components. A public key infrastructure (PKI) is generally used for this. PKI solutions guarantee the reliability, authenticity and integrity of data by generating, utilising and managing digital certificates on an automated basis. They usually run in the background and are now firmly established in many everyday areas of application: from checking identity documents at border controls, to safeguarding sensor and control data in the digitalised agricultural sector (cf. the article on CLAAS also in this issue, see page 23), through to protecting data flows in automotive IT.

The TLS hybrid encryption protocol (transport layer security), too, which is utilised in HTTPS-based web servers inter alia, where it safeguards everyday applications like online shopping, also uses a PKI-based process. In the context of Industry 4.0 TLS is suitable for creating reliable connections for exchanging data. TLS allows data to be transmitted over the internet or other networks in an encrypted format. On one hand this guarantees the communication partner's authenticity through the use of certificates. On the other, this form of encryption protects the data to be transferred from unauthorised access by third parties, as well as from manipulation or forgery. A TLS-based solution can therefore satisfy both of the aforementioned requirements for personalising the components produced by ifm.

It was clear at this point which approach ought to be taken. Yet the implementation presented a challenge for ifm since, although the company specialised in production, it needed to break new ground in terms of implementing IT security standards. Here, the close collaboration between the

The automation and digitalisation of the industry has already made significant progress.

BEST PRACTICE: WHAT SHOULD A PKI FOR THE PRODUCTION OF INDUSTRY 4.0 COMPONENTS LOOK LIKE?

PKI solutions fulfil a host of diverse purposes, which each have typical requirements. The following requirements are essential for use in producing industry components and are primarily aimed at avoiding delays in production:

- The PKI must show a high certificate throughput to avoid losses in production volume at the planning phase.
- There must be a focus on fail-safe operation during planning and installation so that the production of the industrial components is fully guaranteed, even if an error occurs in one of the system components, or if maintenance tasks become necessary.
- Since, where applicable, certificate requests need to be executed in formats that differ from standard IT systems, the PKI must be designed flexibly in relation to the interfaces between the PKI and the industrial components' personalisation system.
- To ensure continuous automation the PKI must offer automated workflows for smooth operation without user interaction.
- The solution needs to be open to expansion in order to accommodate growing production volumes, or to provide individual certificates that are customised to specific components.
- The PKI should also optionally be available as a Managed Security Service. This enables the production company to concentrate on its core competencies.

The secunet eID PKI Suite is a well-engineered product for implementing a flexible, efficient PKI for production in an Industry 4.0 setting.

in-house integrator ifm services gmbh and secunet proved useful. In this manner, all those involved were able to contribute their respective core competencies and realise the project successfully.

Integration into the production process

The partners developed bespoke procedures for the specified requirements, together with an integration plan to embed the PKI seamlessly into the production process. The coordination and implementation of the requisite interfaces were completed on time, enabling ifm to offer gateways that had already been personalised with certificates right on schedule for the planned market launch. Furthermore, secunet took over the continued operation of the PKI components as a Managed Security Service. This meant that ifm was freed up from having to establish its own team for this and was able to continue focussing on its core competencies.

The rapid pace of implementing the ifm solution was successfully maintained on account of it being based on a tried-and-tested standard solution: the secunet eID PKI Suite. This modular infrastructure was originally developed in the context of checking identity documents; today, however, it has a panoply of uses that extend far beyond this. It provides suitable building blocks for a wide range of application scenarios – in industry in particular.

The project proved so successful that there are currently plans to extend it: in future, the device personalisation, which to date has been tailored to a product line, will be extended to enable individual certificates to be generated for various other components. ifm plans to collaborate with secunet again when implementing this element of its Industry 4.0 strategy.

Björn Jansen
bjoern.jansen@secunet.com

ifm gateway components for industrial automation, seen here in the picture, are given digital identities so they can be allocated with confidence within the infrastructure.
Source: ifm group of companies

THE COMPANY

Measuring, controlling and evaluating – When it comes to groundbreaking automation and digitalisation technology, the ifm group is a pioneer and partner. Since its foundation in 1969 ifm has developed, produced and sold sensors, controllers, software and systems for industrial automation and digitalisation worldwide. Today, the family-run ifm group is in the second generation. It has more than 7,000 employees in 85 countries and is one of the worldwide market leaders. ifm combines the internationality and innovative strength of a growing group of companies with the flexibility and close customer contact of a medium-sized company.

PEN TESTS FOR INDUSTRY 4.0

First the Scare, Then the Solution

Pen tests reveal potential gateways for cyber attacks. Based on the security status identified, which can be somewhat frightening for operators of IT systems initially, solutions are drawn up to provide security. This procedure has been successfully carried out in industry as well for a long time.

Over the last 20 years the secunet pen test team has checked many different types of systems: from the very small (micro controllers) to the very big (power plant IT); from highly critical (machine controls) to much more run of the mill (office computers). The experts have therefore also come across a very diverse range of (faulty) behaviours in systems. Here are a few examples, specifically from the sphere of process IT:

- Systems that play dead at the point of a port scan and disappear into a non-defined state. **Fatal error**
- Systems that fall back into reset mode following a test update with a customised configuration and that can only then be reached by using standard passwords on standard ports.
  System not reachable
- Systems with unsecured quick accesses, which – sometimes only via detours – allow administrative access.
  Welcome root

It is not only machines and systems that have evident vulnerabilities, however. Employees, too, are not always immune from error and sometimes give out login tokens over the phone to alleged service technicians. **Human error**

Known problem areas

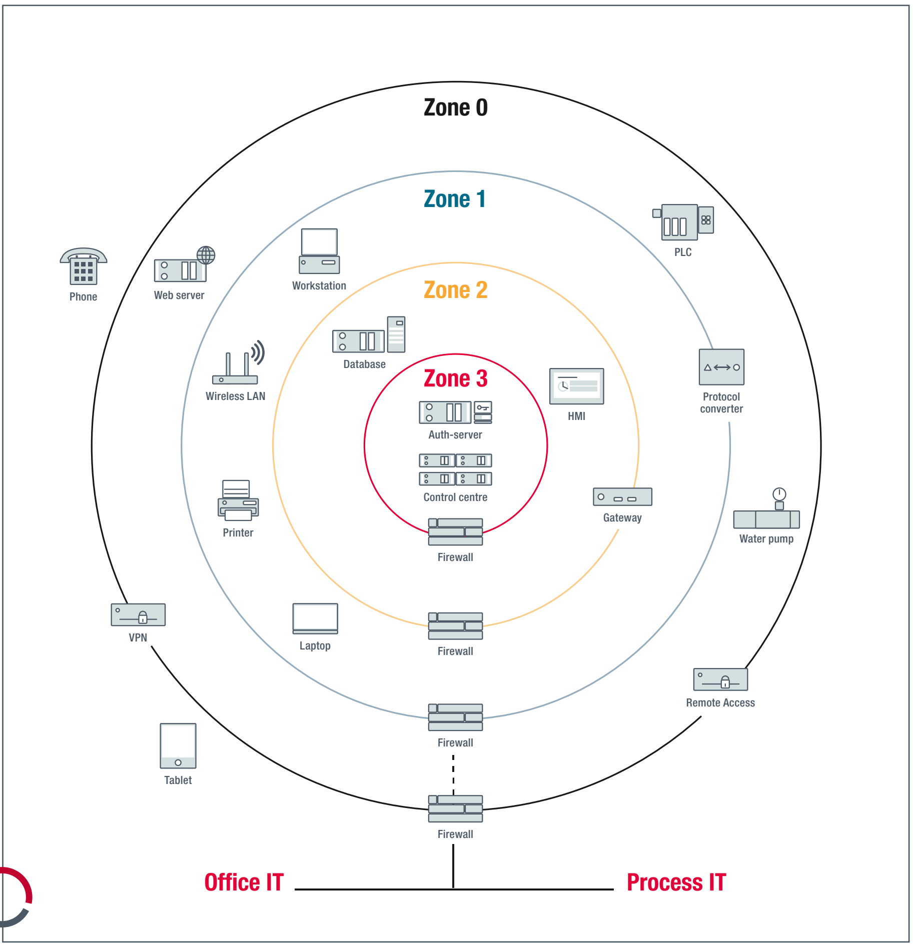
These are the top 5 problem areas in process IT systems from the viewpoint of secunet's pen testers:

1. poor access protection for systems and applications
2. use of unencrypted protocols
3. outdated hardware and software components
4. lack of system hardening
5. oversized and/or unsegmented network areas

These issues are familiar from traditional office IT. Process IT entails other, often underestimated challenges though:

- Access protection (for instance via passwords) is often implemented in a trivial way that doesn't allow modification.
- The transfer protocols used contain no appropriate security mechanisms, are often proprietary and are not upgradeable.
- Patching old systems is not possible, or leads to a loss of service guarantees.
- Systems must be operated as specified by the manufacturer; hardening is not possible retrospectively.

At this point fundamental questions arise: how can pen tests actually be carried out in process IT if the tried-and-tested security measures from office IT can only rarely be utilised? Do pen tests help in any case, if the challenges stated are not as easy to solve?



Within the framework of the secunet OT pen test model the experts analyse the infrastructure and establish various zones or layers – as per this example.

The secunet OT pen test model

The secunet OT pen test model has been developed to overcome these hurdles. It delivers the necessary risk orientation, a valid procedural structure as well as analysis applications that are proven to be effective in the process IT environment. In the first step the model splits the integrated system in question into a maximum of four shells (see figure on page 35). The external shell is often the firewall that separates the 'interior' from the 'exterior'. The inner shell is the most critical from a protection perspective, like the control room of a production facility for example. The second step is to determine the most probable attack vectors for each of these shells – these could be attacks via an internet connection, via interfaces to service providers, via data communications interfaces with external production sites, or via interfaces in the office IT. These potential gateways are then analysed in a targeted way.

The good news: poorly secured interfaces are generally easy to deal with, since they are usually controlled by standard commercial systems such as firewalls and routers – and these can be adapted without negative consequences for the actual control systems. A large proportion of known attacks can thereby be rendered ineffective.

If the external layer is secured the other layers will be checked in turn. Finally, the experts not only identify the potential for attacks on each of the individual components, but also derive actions to minimise the risks these components are exposed to. The secunet OT pen test model thus defines the key steps along the path to secure process IT.

Dirk Reimers
dirk.reimers@secunet.com

TELEMATICS INFRASTRUCTURE

E-Health: Can Germany Make a Success of Digitalisation?

Opinion piece by Markus Linnemann, Head of the Critical Infrastructures division at secunet Security Networks AG

In Germany, the process of digitalisation in healthcare began over 15 years ago. Now, in summer 2019, established doctors and dentists are the first of several groups to be connected to the telematics infrastructure (TI) – at least this is true for a majority of them. But has this created added value for doctors or insurance policyholders? Is the technology secure? Does the organisational framework fit? It's time to look at the status quo – and to beat the drum for the technology behind the TI.

On 30 June 2019 the deadline expired for connecting the first group, which included approximately 176,000 general practitioners, medical specialists, dentists and psychotherapists (also termed 'medical service providers'), to the telematics infrastructure with the connector. Those not yet connected to Germany's digital health network will be required to pay a fine – by law, 1% of the fee costs.

secunet has already delivered over 45,000 connectors for the digital health network and therefore has a very good presence in the market – not least because estimates predict that there are between 10,000 and 30,000 in the market resisting the TI or taking a 'wait and see' approach. Some may have also filed a lawsuit against the statutory provisions and are currently awaiting the result.

This is because digitalisation in healthcare has not been universally welcomed with open arms. The misgivings are considerable: Will the processes in my practice be disrupted? Is there genuinely an added benefit? Is my patients' data protected? What does this mean for me in terms of costs? Many doctors are asking these sorts of questions; and they are completely justified. There is confusion among many medical service providers as to what the introduction actually means for them – whether in positive or negative terms.

Transformation requires the right communication

Is it a case of too little information? Various authorities have given out information at numerous information events and continue to do this. The information provision is often geared towards technical facts, however, which do not align well with the actual – and often highly variable – level of knowledge among the public. If, during an event for general practitioners, the point is made that connectors contain Smart Cards with certificates that expire in five years, most participants cannot classify this information. For them, the

Markus Linnemann
Head of the Critical Infrastructures division at secunet Security Networks AG

main thing is: "In five years I have a problem; the technology is not fully developed." This is where the abstraction from the technology to the actual impact on doctors is lacking. As a matter of fact, after five years the certificate needs to be renewed, but this is an issue that can be solved technically, albeit that the process is not yet fully established.

Most doctors are not IT specialists and – rightly – have no desire to be; ultimately, IT is light years away from their own specialist area. A transformation project that is based on complex technology therefore requires communication bespoke to the target audience. This necessitates close collaboration between speakers and experts who can map out how the complex technology fits with the everyday reality that doctors face.

Awareness projects for IT security, which are designed to raise awareness of information security in companies and public authorities, work in a similar way. Communication that is oriented towards the target audience can result in affected groups of people who initially have a negative attitude moving towards rational acceptance, knowledge and integration – if the project is rational per se. These proven methods can also be used on a transformation project like digitalisation in the healthcare sector. Yet experience from awareness projects also shows that it takes time for a new mindset to take hold.

In addition, there is a significant difference between IT infrastructure and telematics infrastructure: everyone undoubtedly needs IT security. When it comes to TI, this has not been proven from the perspective of many doctors. We can only expect the added value of digitalisation for medical service providers to become clear with the arrival of future enhancements like electronic patient files. Until this point at least we can expect the project as a whole to continue to encounter scepticism.

Fear of data loss

Germany is renowned for its stringent requirements in respect of security and data protection. This is reflected in the TI architecture: its security specifications are very demanding – probably the most demanding by a long way when compared to digital health infrastructures worldwide. Nonetheless, various groups, e. g. from the medical service providers' environment, doubt the security of the TI.

Of course, security concerns are no bad thing in principle – quite the opposite. Integrating an IT system into worldwide data networks always means having to consider global potential attack vectors rather than purely local ones. What's more, there is no such thing as one hundred per cent-proof security. It is always advisable, therefore, to take concerns seriously and to investigate potential loopholes.

The most widely held concerns involve a possible loss of patient data. As mentioned above, since the majority of doctors are not IT experts and not every doctor will appoint a professional IT service with IT security capabilities, it is highly likely that some practices will be vulnerable and could be jeopardised with minimum effort because they lack the necessary security measures in their network. There is consequently a risk, although it is always limited to a single practice. The TI as a whole, with its multitude of health data, is not in danger.

SECUNET IN THE HEALTH SECTOR

From December 2018, when the secunet konnektor was approved by gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH), secunet has been present in the digital health market. The secunet konnektor serves doctors' practices, pharmacies and hospitals among others as a core element for connecting to the German telematics infrastructure (TI).

A development phase preceded the market launch. This phase was shaped by countless discussions with clients, associations, doctors, the German Federal Office for Information Security (BSI), gematik and politicians. In this way secunet's Critical Infrastructures division was able to gain a comprehensive insight into the digitalisation process in healthcare in Germany and the various associated challenges.

One particular case is currently causing a stir in the press and on social media, where an IT service provider apparently overrode the existing security arrangements of the practice network when connecting a practice to the TI, thus leaving the practice unsecured. If this did actually happen, it was evidently a mistake by the IT service provider. It poses a problem for the practice affected, but can one deduce from this that the TI is unsafe? No, firstly because the error cannot be blamed on the TI technology. Secondly, the error reduced the security of the practice's network, but the TI sustained no damage. Access to the TI is still protected by the connector.

The technology is not the security problem

At this point it seems appropriate to beat the drum for the technology behind the TI. Describing this technology as unsecure or outdated sidesteps the actual issue. This is because the encryption technologies utilised in the TI comply with the most rigorous security standards. From the perspective of a security expert the protective concepts deployed in the TI are sometimes excessive even. If devices are installed incorrectly the blame cannot be ascribed to the technology. Furthermore, organisational processes and data protection concepts (e.g. regarding the type of data retention and the access rights) can be implemented in very different ways, with entirely different levels of security. The question, though, of which groups of people should obtain access rights to which data is not a technical question but an organisational one. These aspects can and should be discussed in depth.

It is also important to consider that some of the requirements are contradictory. To let citizens benefit from the advantages of the TI it would be desirable, for instance, if in future they were able to read their patient files on their smartphone, or even on a smartwatch. From a technical perspective this challenge can be solved; gematik has already brought forward specifications to do so. Yet we shouldn't forget that, generally speaking, connecting mobile devices comes with an inherently increased level of risk than connecting specially protected, stationary devices like the connector. This example illustrates that, ultimately, it is always about weighing up risks. The bigger the potential damages, the more extensive the security measures need to be. The risk varies depending on the access point – mobile phone, doctors' practice, hospital, health insurer.

TELEMATICS INFRASTRUCTURE – WHERE HAVE WE COME FROM, WHERE ARE WE HEADING?

The goal of the telematics infrastructure is to connect healthcare stakeholders – doctors, hospitals, pharmacies, health insurers and other bodies – together with the aim of exchanging medical information about patients. gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) was set up in 2005 to build, operate and develop the TI.

The period from 2006–2011 was characterised by synchronising the health insurer associations and doctors. The project has gained momentum since 2011 with the roll-out of the electronic health card. The first practice with a connector went online at the end of 2017. Connectors (like the secunet konnektor) act as a central element for secure communication between the practice and the TI.

In the coming months the TI will be enhanced with specialist applications that will bring visible added value. These include the qualified electronic signature (QES), communication for medical service providers (Kom-LE), emergency data management (NFDM) and the electronic medications plan (eMP). In accordance with the Appointment Service and Supply Act (TSVG), on 01.01.2021 electronic patient files (ePA) should also be available.

Parallel to this, once general practitioners, medical specialists and dentists have been connected, the next few months will see clinics and pharmacies connecting to the digital data highway in healthcare. In other healthcare professions, too, the first interested parties are already lining up and examining the opportunities that digitalisation provides.

Added benefits in sight

The discussion around the TI is additionally burdened by the fact that genuine added value is not yet visible for the participants. This applies to insurance policyholders especially: they may well currently be under the impression that they are paying for a huge, long-term project that, on balance, is not giving them anything back. This is deceptive, however: the benefits will become clear as applications are introduced that provide tangible benefits to policyholders and medical service providers. These include, for example, electronic patient files, emergency data management and the electronic medication plan.

Can Germany now make a success of digitalisation? Yes, if the authorities involved communicate and organise themselves in a way commensurate with a far-reaching transformation project. To do this, all parties need to pull together. In the case of the TI the authorities involved are diverse in nature, ranging from political organisations, to health insurers, to associations and medical service providers. At the moment, it is still unclear whether the dialogue between them will end up being efficient and constructive. This would be desirable, since the TI can offer all parties, insurance policyholders included, genuine added value in future.

SINA PRODUCT NEWS

Client in Whisper Mode

The specially hardened SINA Workstation H R RW11 is now also available in a version that is emission protected as per SDIP 27 Level A. This serves to defend against attacks that are targeted at receiving and evaluating electromagnetic emissions from the client.

The SINA Workstation H R RW11 is a universally usable crypto client for mobile and extreme operating conditions. For instance, the housing offers a high level of protection especially against shock, vibration, dust and moisture. The SINA Workstation H R RW11 was developed in cooperation with the German Federal Office for Information Security (BSI) for processing, storage and transmission of classified information up to and including German secrecy level GEHEIM. The focus is on military and governmental high-security networks with tactical mobile system components.

Being equipped to SDIP 27 Level A means the new product variant fulfils extremely stringent requirements with regard to emission protection. It complements another emission-tested version in accordance with Zone 1 that has been available since 2017. The portfolio therefore offers product variants for different use scenarios.

In addition to the hardened client, another maximally emission protected client type is nearing completion: the SINA Workstation H Client III 27A. First devices will be shipped at the end of 2019.

✉ Merlin Gräwer
merlin.graewer@secunet.com

Wunderbar together in San Francisco – secunet at the RSA Conference 2019

Each spring, the top representatives from the international IT security scene meet in California. With over 42,000 visitors, 650 exhibitors and numerous renowned experts, keynote speakers and trendsetters, the RSA Conference in San Francisco is seen as the most important IT security event globally. The extremely wide-ranging conference programme of sessions, keynote talks and seminars deals with topics like cloud-based options and cryptography through to governmental IT security solutions and cyber defence. Even for experienced conference visitors, this variety makes it a challenge each year not to miss opportune conference highlights.

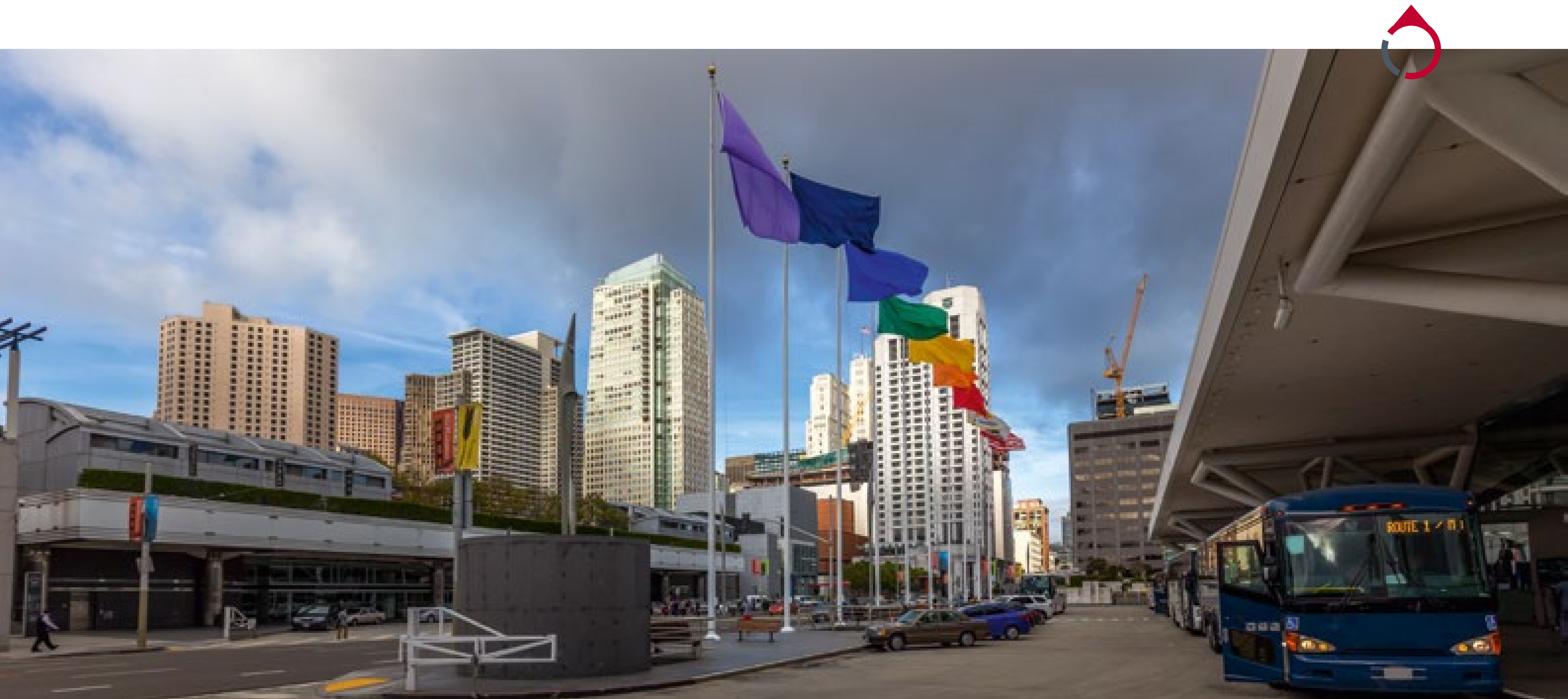
As in previous years, this time secunet was again represented at the German joint stand where, together with other suppliers, the company presented on "IT security made in Germany". The special aspect this year: the joint German presentation was included in the event calendar of the official year of German-American friendship 2019, coordinated and promoted by the German Federal Foreign Office, the Goethe Institute and the Federation of German Industries. The motto of this initiative: "Wunderbar together". Against this background, high-ranking representatives of the German Federal Office for Information Security (BSI) and the German Federal Ministry of the Interior, Building and Community (BMI) were also present at the German pavilion.

The secunet trade show stand featured thematic highlights including SINA and, first and foremost, the SINA SOLID functionality. This enables dynamic VPN networking that automatically configures the connection between the individual hubs. SINA SOLID is the result of joint development and multi-award winning research with the TU Ilmenau. The security-hardened cloud platform SecuStack also made its début. SecuStack enables companies and authorities running applications that are deemed critical for security to utilise cloud computing. Based on OpenStack, the open source standard for cloud platforms, SecuStack offers the most comprehensive cloud solution for organisations in terms of data protection and control.

In addition to the joint stand, German IT security association TeleTrusT organised an extensive framework programme together with the BSI, BMI and the German-American Chamber of Commerce, including the "German-American Security Forum" among other things. Dr. Rainer Baumgart, CEO of secunet, gave a keynote speech there titled: "Where do we come from and where are we going? A short story about Quantum Computing". The programme also featured a reception at the Consulate General of Germany in San Francisco. On this occasion Dr. Baumgart was officially presented with the German IT security certificate, issued by the BSI, for the secunet konnektor. The secunet konnektor supplies healthcare service providers such as medical practices with a central element for connecting to the German telematics infrastructure (TI), and has been ready for rollout since the approval procedure at gematik came to a successful conclusion at the end of 2018.

The secunet delegation enjoyed a further highlight outside of the trade show and conference halls that involved a minor trip to a place beyond the gates of the city: visiting the historic museum of coastal radio at Point Reyes at the Marconi RCA Wireless Station. The participants gained a vivid experience of how ships on the Pacific were still using Morse code to communicate with landbased radio stations into the 1990s.

The event took place at Moscone Center, San Francisco, USA



GERMAN FEDERAL STATES AND IT SECURITY

Exchanging Ideas about Secure Digitalisation

Hartmut Beuß, CIO of the state government of North Rhine-Westphalia (centre) with Norbert Müller (left) and Torsten Henn, secunet, at LänderDIALOG IT Sicherheit 2019

"Taking the big picture view": this was the motto of this year's LänderDIALOG IT-Sicherheit, a forum for exchanging ideas on the topic of secure digitalisation in administration at a German federal state level. secunet initiated the event series in 2018. Following the kick-off event in Frankfurt am Main, this year's event took place in February 2019 at the secunet headquarters in Essen.

The agenda included a variety of topics. Hartmut Beuß, CIO of the state government of North Rhine-Westphalia, gave a talk on the significance of IT security for the digital transformation. Fabienne Tegeler from the German Federal Office for Information Security (BSI) spoke about reinforcing cyber security through a process of collaboration. Maren Janke-Baier from the Bavarian Ministry of Economic Affairs reported on the use of artificial intelligence in continuous network monitoring. Together with secunet, Materna introduced the use of e-files for sensitive data. Other fascinating talks on registering refugees or BSI-compliant voice connection concluded the programme.

After two successful events with increasing participant numbers secunet plans to continue to hold LänderDIALOG on a yearly basis in different federal states. Topics will include content from the administrative authority of the relevant host state, as well as best practices from other federal states. LänderDIALOG will thus offer a regular opportunity for critical and direct discussion in the domain of IT security.

If you work for a German state authority or administrative authority, and you also want to take part in LänderDIALOG in future, please register on the following website (available in German only): www.secunet.com/LaenderDIALOG

KENIAL

Donations for Young People in Need All over the World

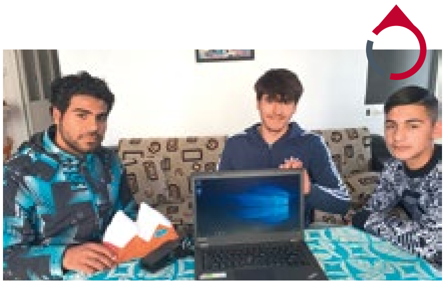
Access to information technology is especially important for schoolchildren and young people and allows them to take part in the ubiquitous process of digital transformation. Unfortunately, this access is not always available, particularly in less developed parts of the world.

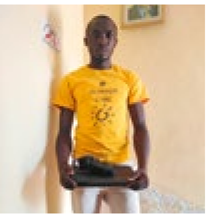
The KENIAL e. V. association has instigated projects to address this and many other issues: KENIAL works together with athletes to organise children's aid projects all over the globe. KENIAL gives the athletes involved the opportunity to give something back to the countries in which they exercise their sport.

At the end of 2018 secunet donated 25 laptops to KENIAL. The devices are currently being used in a range of different settings, including a mother and baby home in Ukraine and a monastery in Bhutan. Eight of the 25 laptops went to the Untuzi Kwa Watoto NGO in Nakuru, a city in Kenya. There are more than 120 orphans of different ages living there, from children to young adults. The devices will be used by schoolchildren and students who have grown up there. They have managed to complete their education independently, without their parents, and are now looking to the future full of expectation. Once they have finished their education they will return the laptops to the NGO so they can be used by other pupils and students.

To find out more about KENIAL go to: www.kenial.de/en/

KENIAL uses the laptops donated by secunet for aid projects in various countries.





Donation to the German Red Cross Children's Hospital in Siegen

Improving children's quality of life – this is the goal of the German Red Cross children's hospital in Siegen. The institution has made it its mission to provide the best therapeutic, nursing and medical care for children, young people and young adults. Each year the hospital looks after around 6,200 inpatients and over 62,000 outpatients – and does this in a consistently child-friendly and family-friendly atmosphere.

In support of this institution the former CEO of secunet, Dr. Rainer Baumgart, waived any kind of farewell gift when he retired from the company in June 2019. Instead, he called for donations to the children's hospital. This call resulted in a donation of around EUR 8,800 being raised, which Dr. Baumgart handed over symbolically to the institution.

Dr. Stefan Schumann (left), Doctor within the Paediatrics department, and Dr. Rainer Baumgart after making the donation.

Dates – October to December 2019

8–10 October 2019
it-sa | Nuremberg, Germany

15–17 October 2019
NIAS | Mons, Belgium

16–17 October 2019
ELIV | Bonn, Germany

22–23 October 2019
inova | Ilmenau, Germany

23–24 October 2019
AFCEA TechNet Europe | Bratislava, Slovakia

28–29 October 2019
Digital Summit | Dortmund, Germany

18–21 November 2019
Defense & Security | Bangkok, Thailand

19–22 November 2019
Milipol | Paris, France

22 November 2019
Automotive IT Security Workshop | Munich, Germany

26–27 November 2019
Berlin Security Conference | Berlin , Germany

3–4 December 2019
StrategieTage IT & IT Security DACH | Zurich, Switzerland

Would you like to book an appointment with us? Just send an e-mail to events@secunet.com

Imprint

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

Chief Editor, Head of Design, Content and Advertisement (Press Law Representative)
Marc Pedack, marc.pedack@secunet.com

Design and Setting
sam waikiki, www.samwaikiki.de

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

Photo credits
Title, pp. 3, 11, 15, 21, 37, 39, 41, 42 bottom: secunet
p. 2 top right, p. 34: ifm group of companies
p. 2 bottom left, p. 17: German Federal Office for Information Security
pp. 4, 5, 6: RheinEnergie AG
p. 7: Bavarian State Office for Taxes
pp. 8/9: iStock/baona
p. 18: Prof. Christoph Busch
pp. 23, 24, 25: CLAAS KGaA mbh
pp. 26, 28/29, 33: iStock
p. 40: Adobe Stock
p. 42 (except on the bottom): KENIAL e. V.

SUBSCRIBE TO SECUVIEW

Would you like to receive secuview on a regular basis, free of charge? Choose between the print and electronic versions and subscribe at

www.secunet.com/en/secuview

There you can also change your preference or unsubscribe.

climate neutral print
www.klima-druck.de
ID-No. 1983656
bvdm.

FSC
www.fsc.org
RECYCLED
Paper made from recycled material
FSC® C006990

Protected OT in the connected world.
secunet shields connected machines and critical networks from cyberattacks and malware.