secuview

The secunet Customer Magazine 1•2021

“The most advanced Entry / Exit System in the world”

Matthias Oel, European Commission, on the EU’s EES project

Transformation rather than revolution

Digitisation and new working practices at the German Federal Office for Migration and Refugees

A healthy level of security

Web isolation in hospitals

National

International: Highlight topic EES

International

Technologies & Solutions

secuview on secunet

News in Brief

Service

Dear reader,

At the end of last year, I expressed the hope in this editorial that the year 2021 would bring us a return to normality. This return is now slower than hoped, the pandemic is not yet over, and yet life already feels a little more normal again in many areas. On the one hand, this is because some restrictions have already been lifted. On the other hand, some permanent innovations, such as a high proportion of home working, are now perceived as normal by many.

One thing is clear: the profound change in the world of work that many observers predicted at the beginning of the pandemic is actually taking place. This is demonstrated by numerous secunet customer projects that focus on secure infrastructures for mobile working. In this secuview, we describe how the German Federal Office for Migration and Refugees has entered the new mobile working world step by step with SINA technology.

An acquisition that secunet made this year also fits in with the "new normal". The Hanover-based company stashcat ensures that organisations with high security needs, such as the police, can also use a messenger app with advanced collaboration functions. Those interested can read the story of this exciting company and product starting on page 24. I look forward to continuing our journey together with stashcat.

Our cover story also has to do with normalisation, albeit somewhat more indirectly: the EU states are currently preparing for the European Entry / Exit System (EES), which is to provide even better security for the Schengen external borders from mid-2022. This also involves how modern border control technology can prevent long queues at border crossings, which could arise as a result of the new biometric registration of Third Country Nationals. Crowded airports are a scenario that seems unreal in pandemic times – but border authorities are bracing themselves for passenger numbers to rise again as restrictions gradually fall.

Matthias Oel, Director for Schengen, Borders and Innovation in the EU Commission's Directorate-General for Migration and Home Affairs, explains his view of the EES in the interview starting on page 8. And he tells us that this project also had to overcome pandemic-related hurdles.

Now I hope you enjoy reading the new issue. Stay healthy!

Axel

Axel Deininger

Digitisation and new working practices at the Federal Office for Migration and Refugees

Transformation rather than revolution

Like most other authorities and businesses in 2020, the Federal Office for Migration and Refugees (BAMF) faced the challenge of relocating office workstations to workers' homes as a result of the coronavirus pandemic. In addition, this had to take place at a very high security level. Unlike others, however, the BAMF was prepared – as it was already using a SINA solution enabling secure mobile working. Since then, the federal authority has been driving the transition to a new way of working – taking a carefully regulated, step-by-step approach.

When plans were originally made to implement a mobile, secure IT infrastructure at the BAMF it had nothing to do with the idea of home working. It was actually in 2015 that the need arose in connection with the refugee crisis. Over the course of 2015 the BAMF registered around 890,000 protection seekers who had entered Germany. Personnel numbers were increased significantly. The BAMF employees who served in the initial reception centres at the EU's external borders needed an IT infrastructure that they could use to process and transmit sensitive information such as personal data.

The Federal Office for Migration and Refugees (BAMF) is a German federal authority within the portfolio of the Federal Ministry of the Interior (BMI). As the centre of excellence for migration and integration in Germany, the Federal Office is not only responsible for processing asylum applications and ensuring refugee protection, but is also a motor for the nationwide promotion of integration. The authority's remit also includes research into migration. With its decentralised locations, including branch offices, arrival centres and decision-making centres, it is in direct contact with all players in refugee protection and integration work.

To meet this requirement, secunet installed a SINA solution with 1,500 SINA Workstations, achieving this in just a few weeks because time was an especially valuable resource at that point given the situation. "A large meeting room at the BAMF was re-purposed as an installation office," recalls Norbert Müller, Head of the Public Authorities Division at secunet. "We had to proceed with the utmost pragmatism in order to keep to the tight timings." The SINA Workstations were integrated into cases that held the most important devices for registering the refugees, such as fingerprint scanners and document readers. This made it possible to process the data collected directly and transmit it securely.

Growth goes hand in hand with IT challenges

The increased workload caused by the refugee crisis was soon also extremely noticeable within the administrative and core areas of the BAMF. The federal authority therefore had to adopt a number of measures to fulfil the new requirements and tackle the volume of work. These measures included further growth in personnel numbers and streamlining work processes.

The legislator authorised approximately 7,800 positions at the BAMF for 2018 and around 8,100 for 2019. This means there will be a permanent workforce of over 8,000 at the BAMF. Compared to the number of employees prior to 2014 this equates to almost a fourfold increase.

Additionally, employees' expectations are changing: in today's world of work, attractive working conditions are becoming increasingly important. As a higher federal authority, the BAMF is obligated to improve the family-friendly nature of the organisation and ensure that family life and professional life are compatible. The federal office's IT plays a key role in all these developments.

This gives rise to a further challenge though, in that a very high level of security is needed. Employees' computers sometimes hold sovereign data that it is especially important to protect, for example information on politically persecuted asylum seekers.

Officials at the BAMF quickly realised that SINA would be an answer to these challenges and enable employees to work from home or other locations – which was very popular with employees.

Same solution, new objective

For this and other reasons, when the maintenance contract expired in 2019 the federal authority decided to keep SINA and install a refresh together with updates. This brought the installation fully up to date and outdated components were replaced.

Then, in spring 2020, the coronavirus crisis suddenly raised its ugly head. While many federal authorities and businesses were forced to take their first steps towards mobile working while under huge time pressure, the BAMF was among those organisations that were already one step ahead of the game. The SINA solution was already proving a success. Now, the obvious thing to do was to expand it.

According to Kausik Munsi, Chief Technology Officer (CTO) at the BAMF, there were four reasons why the authority chose to keep SINA: "Firstly, we had to find a partner who could be completely trusted to deliver, since it was also about trust. Secondly, the technology itself was important to us of course, and SINA was both highly secure – as confirmed by the BSI approval – as well as, and this is the third point, very easy to use. Fourthly, we had a flexible framework agreement that we could use to access SINA."

The issue of delivery capability was not a trivial one in the midst of a pandemic, since there was a shortage of IT components on the global market. Already during the refugee crisis, however, secunet had proven to be a reliable partner at a critical time. This time, too, secunet was able to act fast, delivering large numbers of units very quickly. In several waves, the BAMF purchased several thousand SINA Workstations. Currently, almost all workstations at the BAMF are equipped with SINA clients. While many organisations were taken by surprise by the revolution in the world of work that was so abruptly set in motion by the pandemic, the BAMF was able to make the transition via a series of smaller steps. The roll-out is therefore ongoing. The collaboration involves three different partners: the BAMF; its IT service provider ITZ Bund; and secunet. Consultants from secunet are continually on site to drive forward the implementation of the project and provide operational support. "We very much appreciate the close collaborative partnership," says Norbert Müller from secunet. "This has played a major role in the success of the project."

> **"We had to find a partner who could be completely trusted to deliver, since it was also about trust."**
>
> Kausik Munsi, CTO, BAMF

Looking to the future

"The trend for mobile working is clearly set to continue," says Munsi. "Additionally, there is a distinctive dynamic at play at the BAMF: we have a very large development team, some of whom are based abroad and some of whom travel between different locations. This is another reason why we will still need SINA."

The collaboration between the BAMF and secunet has also borne fruit over and above SINA. The federal authority now uses secunet's Session Border Controller (SBC) to secure its telephony, and separate audio and video in accordance with BSI stipulations. Further IT-related issues are currently under discussion for the future. Kausik Munsi: "Our employees want to offer our clients and partners the best possible service. We want to support them in this endeavour with our IT, helping them to achieve their goals as well as enjoy coming to work. We therefore want to enable seamless communication and create an optimally networked work environment with no media interruptions."

✉ Christian Eisenried
christian.eisenried@secunet.com

With a **SINA** solution, employees of pulic authorities or companies can securely handle sensitive or even classified information. Whether they are in the office, at home, or out and about is irrelevant. Thanks to a variety of interlocking security components, SINA ensures that third parties are unable to read any data if users have opted to access the authority's network via a Virtual Private Network (VPN). The **SINA Workstation** functions as the client in the SINA network, uniting security with operability, and is available in a variety of desktop, laptop and mobile formats. Even if a SINA Workstation gets lost, the data remain protected thanks to two-factor authentication and hard disk encryption. SINA components are available for a range of applications and the different versions are authorised for a spectrum of classification levels by the German Federal Office for Information Security (BSI).

For further information please visit: www.secunet.com/sina

Highlight topic: EU Entry / Exit System

The Schengen area comprises 26 states with more than

1,800

BORDER CHECKPOINTS

at land, air and sea borders

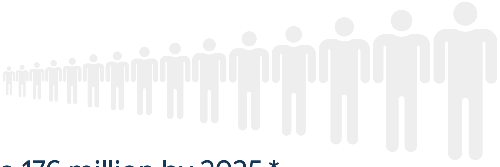
source: eu-LISA Conference Report 2015

48° 35’ N
7° 45’ O

The operational management of the central Entry / Exit System is done by eu-LISA in Strasbourg.

source: eu-LISA, EES-Leaflet

In 2019, over 115 million Third Country Nationals entered the European Union, and the number is expected to rise



+53% to 176 million by 2025.*

* Due to the COVID-related passenger decline in 2020 / 2021, forecasts on this point currently vary significantly. Nevertheless, a strong increase can be expected from 2025 onwards.

source: Frontex; Technical Guide for Border Checks on EES related equipment (05 / 2021)

As a result of Brexit, the UK population, i.e.

+66.65 million

people, are now considered Third Country Nationals when travelling to Schengen Area countries.

source: Embassy of Belgium in the United Kingdom

The new European identity database, the Common Identity Repository (CIR), will have

300 million ENTRIES

The data of the Entry / Exit System will also be included here.

source: www.biometricupdate.com

89 SECONDS

Handling time for Third Country Nationals at the border control counter before and after the introduction of the Entry / Exit System

34

source: Report on the Smart Borders pilot project, Federal Office of Administration

Interview with Matthias Oel

"The most advanced Entry / Exit System in the world"

The European Entry / Exit System (EES) was initiated by the EU Commission as part of their Smart Borders agenda. Today, the Commission oversees and coordinates its Europe-wide introduction from a legal perspective. secuview spoke with Matthias Oel, Director for Schengen, Borders and Innovation in DG (Directorate-General) Migration and Home Affairs, European Commission.

Could you please briefly describe the roles and responsibilities of DG Migration and Home Affairs with regards to the EES?

Matthias Oel: The European Commission is responsible for monitoring whether EU law is applied correctly and on time. As part of the preparations for the rollout of the Entry / Exit System, the Commission's main tasks have focused on overall coordination and governance of the system. In the past three years, this meant mainly preparing legislation setting out how the system should be implemented at technical level. To this end, we worked with a committee, bringing together our technical experts, EU countries and the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), in charge of developing the system. Currently, we mainly focus on monitoring the preparations for the timely rollout of the Entry / Exit System in EU countries. We are in very close contact with them through technical meetings and visits.

How is the EES implementation progressing?

The development of the Entry / Exit System is progressing very well. Together with eu-LISA and EU countries, we are preparing for the rollout of the system and work to resolve any potential issues ahead of time. According to current planning, we will have the most advanced entry-exit system in the world in the first half of 2022. The system will work together with other large-scale EU IT systems and will contribute to managing migration and enhance security. The system will make it easier and quicker for bona fide travellers to cross the EU's borders while also identifying more efficiently overstayers (people remaining in the Schengen area after the end of their authorised stay), as well as cases of document and identity fraud.

The Entry/Exit System is intended to replace the manual stamping of passport, and marks a first important step towards more automated and smoother border crossing. Thanks to the Entry/Exit System, more travellers should be able to use automated border control checks and self-service systems. These are quicker to use than queueing at a border guard booth and more comfortable for the traveller. In the future, we would potentially also like to see returning travellers using a mobile app to perform their border check.

We are now entering the final stage in the preparation of the system. The necessary legal base is in place and eu-LISA is now developing the system. In parallel, preparations for testing of member states' connection to the system are ongoing. This is a critical phase for the system, and we are confident that the meticulous preparation will pay off.

What were the biggest challenges?

The Covid-19 pandemic has brought challenges in the preparations for the Entry/Exit System. For example, preparations of physical spaces where hardware will be located were impacted by access restrictions during the pandemic. Teams working on the project are multinational and travelling for meetings became very difficult. We have worked very hard together with EU countries and eu-LISA to mitigate any negative consequence of the pandemic on the rollout of the Entry/Exit System. I can now say with confidence that up to now we have managed to deal with these challenges without significant impact on the project.

> "The Entry/Exit System will help speed up border crossing, as travellers will be able to use self-service systems or eGates at the borders instead of having to line up for their passports to be stamped manually."

As we are approaching the planned date for entry into operation, we are now focusing on the support to EU countries to prepare for the operation of the system. EU countries, Schengen Associated Countries, eu-LISA and the Commission are sailing in a convoy. The latest ship reaching the harbour will decide when the Entry/Exit System can become operable. That is why we need to ensure that preparations are ongoing at a similar speed and that every EU country is ready on time. The Commission is also providing member states with significant funding to support the rollout of the Entry/Exit System at the national level.

The Entry/Exit System is planned to enter into operation in the first half of next year, in time ahead of the overall deadline at the end of 2023 for EU information systems for security, border and migration management to become interoperable and work together in an intelligent and targeted way.

The Covid-19 pandemic also cast new light on the potential of modern technology. This also applies to border management. The Entry/Exit System will help speed up border crossing, as travellers will be able to use self-service systems or eGates at the borders instead of having to line up for their passports to be stamped manually.

What's next after the EES will have been implemented?

Our work of course does not end with the Entry/Exit System becoming operational. On the contrary, the EES is only one part of our work towards putting in place a state-of-the-art external border management system and making sure that information systems work together in an intelligent and targeted way.

We are currently upgrading the Schengen Information System (SIS), which is the most widely used and largest information sharing system for security and border management in Europe. The upgraded SIS will be in place before the Entry/Exit System. We are also upgrading the Visa Information System, the database allowing Schengen States to exchange visa data. Its infrastructure connects consulates in non-EU countries and all external border-crossing points of Schengen States. In the future, we would like to move towards digitisation of the entire visa application process.

Shortly after the SIS and the Entry/Exit System, the European Travel Information and Authorisation System (ETIAS) will become operational. ETIAS will help identify security, irregular migration or high epidemic risks posed by visa-exempt visitors travelling to the Schengen area. The system will give travellers an early indication of their admissibility to the Schengen member states, making legal travel across Schengen borders easier. Once ETIAS is in place, non-EU citizens travelling to the Schengen area who are exempt from

Matthias Oel

Matthias Oel is Director for Schengen, Borders and Innovation in DG Migration and Home Affairs, European Commission.

Before assuming this position in May 2017 he was Director for Migration and Security Funds in the same DG from January 2016, Head of Unit for Asylum (as of April 2012) and Special Adviser in the Cabinet of the President of the European CouncilHerman Van Rompuy (as of January 2010).

Matthias Oel started his career in the German Federal Ministry for Economics and joined the European Commission for the first time in 1995 as Seconded National Expert in the Cabinet of Commissioner Dr Monika Wulf-Mathies (Regional Policy). In 1997 he moved to the Permanent Representation of Germany to the EU where he worked as Counselor for Industry and Regional Policy during the German EU-Presidency 1999. Afterwards he became a Commission official and worked as Parliament and Coucil coordinator and Assistant to the Director General for Personnel and Administraton. From 2004 to 2006 he was Member of the Cabinet of Vice-President Günter Verheugen mainly covering the Industry Policy dossier.

In 2006 he was seconded to Berlin where he worked as Head of the Task Force "2007 EU Presidency" and subsequently Director for European Union Affairs in the German Federal Ministry of Interior until joining the Cabinet of President Van Rompuy.

> "The EES is only one part of our work towards putting in place a state-of-the-art external border management system and making sure that information systems work together in an intelligent and targeted way."

the visa requirement will need to register and obtain an authorisation before travelling. In a vast majority of cases (expected to be over 95%) this will result in automatic approval. The process will be simple, fast and affordable: the ETIAS authorisation will cost €7, which will be a one-off fee, and will be valid for 3 years and for multiple entries.

In addition, looking further ahead, we need to both be aware of and drive technological innovation, which will shape travel and border management in the future. Over the last years, the Commission has funded research that went into the development of systems and technologies for today, including the Entry/Exit System, and for the future. Today's research studies and prepares the systems of the next decades. This is important not only to enable European technological capabilities, but also to understand how technological developments may interact with citizens' and non-EU nationals' fundamental rights, to make sure that our systems are up-to-date, secure and compatible with EU values.

All the large-scale EU IT systems are not stand-alone projects, but they form an interoperable whole. The interoperability will allow these EU IT systems to complement each other and enhance the use of information in many areas, such as borders, visa process, security, migration management and law enforcement while fully respecting fundamental rights and data protection rules.

Installation of secunet easygates at Sofia Airport, Bulgaria

Introduction of biometric border controls in the Schengen area

Who is ready for the EES?

The European Entry / Exit System (EES) has been on the agenda of border control authorities and technology providers for years. In the meantime, a lot has happened on this topic in Europe: even though some countries are still in the middle of preparing their EES tenders, the technological course has been set in the vast majority of states. secuview gives an overview of what it is all about and shows practical examples from countries where secunet is currently implementing EES projects.

EES in a nutshell

The introduction of the Entry / Exit System will modernise the Schengen external borders in the future. The EU Commission's EES project aims to increase the security of the Schengen area and make border control more efficient by automating processes in order to cope with the ever-increasing number of border crossings.

The EES serves to electronically register Third Country Nationals at entry and exit and to automatically calculate the permitted duration of stay in the Schengen area. Starting in mid 2022, travellers from third countries will therefore have to register with four fingerprints and a facial image when entering one of the countries of the Schengen area at land, sea and air borders. The current practice of manually stamping travel documents will be replaced by a digital entry in the EES. The system is intended to make it easier to detect so-called "overstayers", i.e. persons who exceed their authorised stay. The use of biometrics further facilitates the identification of undocumented travellers during domestic controls within the Schengen area.

The flip side of the coin is that the entire passenger process will take much longer due to the more extensive checks and the necessity of capturing biometric features at the border. While the pandemic has hit the travel sector hard, the border authorities have to be prepared for increasing passenger numbers when the situation returns back to normal. It is therefore very likely that queues at the border control counters become even longer then. This must be avoided – in addition to passengers, both airports and border police have a great interest in preventing this scenario as far as possible.

Therefore, projects are currently underway in almost all European states to ensure the implementation of the EES requirements, such as the installation of facial image cameras and the integration of EES processes at manual border control. At the same time, however, many states are opting for a general modernisation of their border control infrastructures. This includes automation and/or process optimisation at key border control points, which can absorb the additional time needed to check people and help manage the continuously increasing number of passengers.

With the border gears product portfolio secunet offers solutions that enable customers to achieve this. It consists of eGates, self-service kiosks, camera systems and border control applications that ensure the necessary process optimisations for the EES implementation.

EES in practice

secunet is currently supporting several countries in implementing the requirements of the EES. Read more on the next page.

Border control officer at
Burgas Airport, Bulgaria

SWITZERLAND

COMPLETE RENEWAL AT ZURICH AIRPORT

The Zurich Cantonal Police has commissioned secunet to renew and further develop the border control infrastructure at Zurich Airport. On the one hand, the contract includes adapting border control to the EES regulation in order to meet the legal requirements. On the other hand, the installation of automation technologies is intended to counteract a slowdown in passenger flows caused by the additional steps necessary for enrolment and verification of Third Country Nationals.

In the previous project "Greko NG", secunet had already completely modernised the approximately 100 stationary workstations on behalf of the Zurich Cantonal Police and equipped them with a new border control application: The software clearly summarises all results of the optical and electronic document check on one screen, thus considerably simplifying and accelerating the control process.

CZECH REPUBLIC

EES WORK IN PROGRESS

In February, the Czech Border Police commissioned VÍTKOVICE IT SOLUTIONS and secunet with the first and most extensive part of their implementation of the EES. Components from the secunet border gears product portfolio will help to ensure that border control at Czech international airports remains fast, simple and secure – even after the introduction of the EES. This is particularly important here, as UK citizens for example make up a large number of travellers at Prague Airport, who – since Brexit – must also be treated as Third Country Nationals. secunet delivers:

- secunet easykiosks for pre-registration by Third Country Nationals
- secunet easytowers for capturing high-quality facial images at stationary border control counters
- software for process visualisation and monitoring of data capture and verification as well as the checking processes running in the background
- the central server component, secunet easyserver, which will connect the various border control components and communicate directly with the central EES of the EU

Vítkovice as general contractor will provide maintenance and support as well as hardware peripherals for manual border control. The rollout of all components is planned for the end of 2021.

BULGARIA

"BOARDING COMPLETED": AIRPORTS ARE EES-READY

In cooperation with the Bulgarian general contractor SSARM, secunet has implemented a secure complete solution for EES-compliant border controls at the international airports in Sofia, Varna and Burgas. Bulgaria is one of the first EU countries to have prepared its air borders with secunet border gears for the EU-wide Entry/Exit System and is ready for operation long before its official launch.

The overall solution includes eGates (secunet easygate), self-service kiosks (secunet easykiosk) as well as camera systems (secunet easytower) and fingerprint readers for the stationary border control counters. All passenger groups, i.e. EU citizens as well as Third Country Nationals, will thus benefit from more convenient, automated processes at border control. The project was completely realised during the Covid-19 pandemic and the installation – despite all the challenges – was completed on time.

Read the interview with Nikolay Dimchev, Managing Director at SSARM, on the next page for more information.

Varna Airport, Bulgaria

Interview with Nikolay Dimchev

New EES Technologies at Bulgaria's Aviation Hubs

SSARM is the largest IT systems integrator in Bulgaria and was awarded a major contract to equip Bulgaria's aviation hubs with EES-compliant border control solutions following a tender by the Bulgarian Ministry of Interior last year.

In the meantime, SSARM has fully installed a secure turnkey solution at Sofia, Varna and Burgas airports in cooperation with its German partner secunet. In the following interview, Nikolay Dimchev – Managing Director of SSARM – talks about the project, its most interesting findings and the added value for passengers, border control and airports.

Congratulations on the successful EES installation. What exactly did you install at the airports in Varna, Burgas and Sofia and why?

Nikolay Dimchev: The reason for implementing new border control systems is closely related to the EU's decision to introduce the Entry / Exit System throughout the Schengen area in 2022. By taking facial images and fingerprints, all member states will in future know better which Third Country Nationals are entering the EU and ensure that individual passengers do not overstay. This enhances the security for all of us.

However, the integration of these additional process steps at primary border control threatens to cause a collapse if infrastructures remain unchanged, because clearance takes an average of 40 to 45 seconds longer – per passenger! Therefore, process automation at all possible steps, i.e. also at stationary border control counters, is inevitable. The Ministry of the Interior therefore decided to comprehensively modernise the border control technology and commissioned us with the implementation. We then installed – in collaboration with our project partner secunet – eGates, self-service kiosks as well as camera systems and fingerprint readers for the stationary counters at the three aviation hubs in Bulgaria. The technologies fulfil very different functions and are sometimes intended for different passenger groups – but all technologies together will noticeably speed up the border control process and greatly reduce the workload of the responsible officers.

Why did you choose the German partner secunet? SSARM actually operates exclusively in the national market and is also a well-positioned IT system integrator itself.

We have been working with secunet in the area of high-security technologies for a long time and they have consistently proven to us in previous projects that the quality of their products is not only right, but comprehensively meets the requirements of our customers. That's why we also contacted secunet for the EES project. Although we are in an excellent position ourselves as system integrator who is very familiar with the Bulgarian market, we don't have our own product portfolio in this area.

The EES solutions from secunet then also convinced us: they deliver EES-compliant biometric solutions, that assure the best possible quality of the biometric capture and are designed to be highly resistant to circumvention and forgery. This is extremely important, especially for unattended systems where the officer is not standing right next to them monitoring each passenger. And last but not least, all products have a very eye-catching, modern design – not to be underestimated considering today's innovative airport architectures.

The modernisation of the border control infrastructure was certainly a major investment. What advantages does it bring for passengers, airports and border control?

The benefits are quickly summed up: passengers – wherever they come from – now have access to automation technologies at the Bulgarian airports in Sofia, Varna and Burgas. If you like, they have at least a part of their border crossing in their own hands. Thanks to intuitive user guidance and innovative security mechanisms, passengers can be sure that their data will be captured quickly and is processed securely and in accordance with data protection regulations. The high-quality biometric acquisition is of course especially important for the border police. The officers are moreover ideally supported by the technologies and not put under additional strain. And the airports benefit from the fact that despite more extensive border control processes, which actually take more time, there are no significantly longer queues and missed connecting flights.

What are your most important insights from this EES project?

Actually, we were confronted with the same challenges in the EES project as in almost every IT project: When things become more concrete than a description on paper, it is not uncommon that new or changed requirements arise from the customer side that have to be implemented in the running project at short notice. This is completely normal and we can deal with it very well.

In the case of the EES installations, for example, we installed the most modern, secure products and had to realise that this alone was not enough. Border control projects are about more than "just" installing technologies. The products should optimise passenger processes and fit perfectly into the respective environment and infrastructure, which is different

Nikolay Dimchev

Nikolay Dimchev is an engineer in telecommunications and has an MBA from Cotrugli Business School.

He gained his 20 years of experience in IT as Solution Consultant, Sales and Business Development Manager in companies like Atos, Symantec and DXC. He joined SSARM in 2017 as Head of Sales. In January 2021 Nikolay Dimchev was promoted to the position of Managing Director.

His strong technical background in combination with his experience as a team leader helps him to run the company's daily operations, to develop the team and to manage the company's most complex and strategic projects.

at every airport and at every land border. This was an important and new insight for us. In this specific case, we also have integrated functional enhancements into the current project that were not planned beforehand. The installation of glass walls between stationary and automated border control or the construction of racks for the fingerprint scanners, which otherwise would not be perfectly positioned for the passengers, are small examples. Fortunately, together with secunet, we were able to offer all new customer requirements quickly and as needed, integrated them into the project implementation and still delivered on time.

Another important insight yet certainly not new is: You have to react flexibly right up to the end and remain focused on details if you want installations that fit perfectly and are also visually attractive.

Are there further points you would like to particularly highlight?

The EES installation was our first border control project, our premiere, so to speak. We are proud and relieved that we fulfilled the task to the fullest satisfaction of the Bulgarian Ministry of the Interior. Having secunet's people on board, who are very experienced, was of course an enormous advantage for us. In times of this pandemic, we learned a lot together and supported each other in the best possible way, even if we were forced to do so "remotely" for most of the project. Through this perfect collaboration, we succeeded in implementing the installations on time and achieving the customer's declared goal: Bulgaria is one of the first countries in the EU to be equipped with an EES-compliant overall solution at the three aviation hubs, long before the official launch of the Entry/Exit System. We are proud of this.

Established 10 years ago, **SSARM** is the fastest developing IT system integrator in Bulgaria. The company specialises in delivery, installation and integration of IT and communication equipment, hardware and software, as well as data security, protection, and storage solutions. SSARM also works in the field of state security and automated border control solutions. In the past 4 years the company has delivered complex projects for the Bulgarian state administration and the finance and corporate sector. SSARM is continuously expanding its expertise in the field of innovative solutions for border control, drone-based solutions and others.

Biometrics quality as a key factor

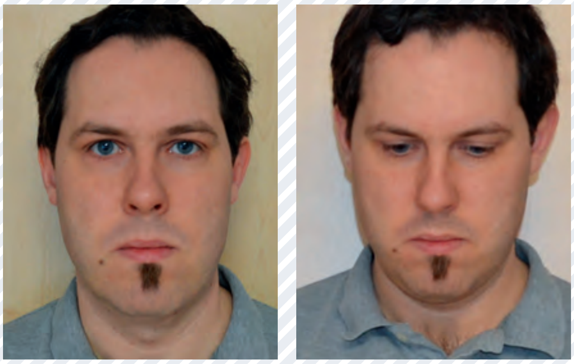
The EES is just as good as its data

In future, an EES dossier will be created in the EES register for every traveller from third countries, containing the biometric data together with the identity data of the traveller and other information taken from the travel document as well as the date and place of entry or exit. The biometric information includes a facial image and four fingerprints. These datasets enable the automated identification of travellers. The comparison with the EES serves, among other things, the purpose of determining whether someone has already entered the country under a different identity.

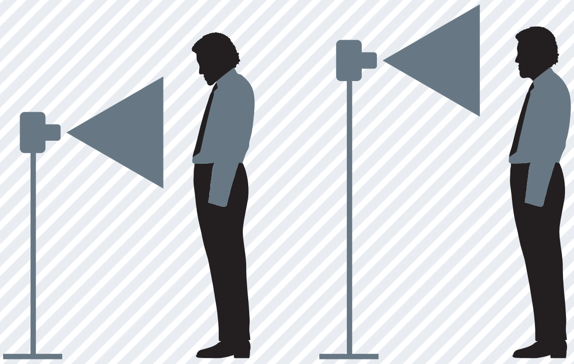
In automated identification applications two types of errors are basically possible: In the case of a **false positive identification,** the algorithm decides on the basis of a person's facial image and / or fingerprints that his or her biometric data already exist in the database, although it does not. In the case of a **false negative identification,** the algorithm decides that a person's biometric data is not present in the database, although it is.

Low error tolerance required

For the EES, the EU has issued a decision stating that the false positive identification rate must be below 0.1%, i.e. in less than 0.1% of total border crossings someone may be falsely identified as another person. There is a similar specification for the false negative identification rate. According to the EU, this must be below 1%, i.e. in less than 1% of all border crossings, the system may not assign a traveller to his or her stored dossier. The EU Commission expects that the EES register will have a size of about 100 million dossiers after 2025. At every border crossing it must then be possible to conduct an efficient and, above all, correct search and identification in the EES register.



Two variants of a facial image. In the left example, the image meets the requirements for a frontal image according to ISO/IEC 19794-5 (the person looks directly into the camera and has a neutral facial expression). In the right example, the image violates the requirement that the person must look directly into the camera.



Two variants for capturing facial images. Variant 1 (left) with a height-fixed, horizontally oriented camera is not suitable for capturing frontal images. Variant 2 (right) with a height-adjustable capture mechanism enables frontal capture of neutral faces of people of different sizes.

Each Schengen state is itself responsible for implementing and achieving the specified quality targets. In the area of facial recognition, Germany has already gained valuable experience from EasyPASS, the automated border control of the Federal Police. In this border control system, which was rolled out by secunet in consortium with Bundesdruckerei, a live facial image is compared with the image stored in the travel document.

With EES, special quality requirements apply to the live image captured at the border: According to the ISO/IEC 19794-5 standard for frontal facial images, the image must be illuminated homogeneously, the person must look straight into the camera and have a neutral facial expression. It therefore makes sense to use a height adjustable camera to ensure a frontal, non-tilted position of the head of the respective person. It is obvious that the use of an automatic as opposed to a manual height adjustment speeds up the process of capturing facial images. When this is implemented, the quality of the images increases, which in turn reduces identification error rates and makes it easier to meet EU requirements for error tolerance.

Algorithm recognises quality of fingerprints

The EU also sets minimum requirements for fingerprint scans: for example, they must have a resolution of 500 or 1000 ppi and their quality is evaluated using the NFIQ 2.0 algorithm of the US standards institute NIST.

The NFIQ algorithm returns a quality score as a measure of how many details in a fingerprint are usable for matching purposes. Since 2017, the algorithm has been available in the most recent version NFIQ 2.0. This version is mandatory for the EES and was further adapted for this purpose. On behalf of the BSI and in cooperation with NIST, secunet experts were involved in this optimisation. Additionally, secunet developed a modular software framework to further train and improve NFIQ 2.0 for future smart border control using machine learning methods.

secunet easytower at
Varna Airport, Bulgaria

When the EES starts operations, expected in mid-2022, the appropriate infrastructure must be in place at the Schengen external borders to be able to capture the biometric data in the specified quality. This is a basic prerequisite for achieving the requirements and for the EES to fulfil its purpose of significantly increasing the security of the Schengen area.

Benjamin Tams
benjamin.tams@secunet.com

HIGH QUALITY AND QUICK BIOMETRIC ENROLMENT AT STATIONARY BORDER CONTROL

The **secunet easytower** ensures fast and high-quality facial image capturing at stationary border controls. It guarantees the highest biometric data quality in accordance with the EES regulation. With the help of automated height adjustment of the camera and additional diffuse lighting, the quality of the frontal facial image is ensured in accordance with ISO 19794-5:2011. Thus, all EES quality requirements are fulfilled.

Thanks to an intuitive user interface, the easytower is easy to use for both travellers and border officials. A built-in feedback screen displays the "live" footage from the facial camera. The traveller looks into a digital mirror with additional user guidance, which – available in several languages – ideally supports the traveller. Depending on requirements, a fully automatic or manual capture mode is selected. Due to the intuitive process, the easytower guarantees a short capture time and thus speeds up the border control process. The integrated lighting ensures high-quality, well illuminated images and homogeneous exposure of the face even in poor lighting conditions.

Cooperation between armed forces

Multinational cooperation – thanks to or despite cyber security?

By Marcel Taubert, Head of Division Defence & Space, secunet Security Networks AG

It is part of the Bundeswehr's remit to "strengthen European integration, transatlantic partnership and multinational cooperation" – this is the statement made within the Conception of the Bundeswehr (KdB). [1] The multinational focus is founded on political will, but also offers military advantages such as a better picture of the overall situation, coordinated deployments and exercises, and faster decision-making across organisational boundaries. What does multinational cooperation look like in practice, however? Where do the challenges lie and what role does cyber security play?

There is a disparity here at the strategic, operational and tactical levels. On the strategic side of the spectrum, distinguished by a high level of abstraction and a limited number of people taking action and making decisions, multinational cooperation can usually be implemented effectively by means of existing approaches. One example is the Multinational Joint Headquarters Ulm, which assumes leadership of global crisis management operations on behalf of the UN, NATO or the EU. Here, the interlocking takes place on a level on which specific strategic and military-political specifications are implemented in plans and commands for the armed forces involved. Any sticking points that arise at this high level are manageable. There are also technically sophisticated, highly secure IT solutions.

If we look further at the operational and tactical end of the spectrum, the challenges become greater. It's not just IT that plays a role here. Cultural aspects also carry more weight, for instance differing leadership styles of the armed forces involved. Moreover, different legal framework conditions and provisions apply, which can lead to difficulties. The high personnel turnover rate, which is typical for military organisations, makes shared experience building more difficult.

A multitude of security domains

At the technical level, the specific security requirements of all participating countries need to be taken into account and reduced to the lowest common

[1] Konzeption der Bundeswehr, July 20th, 2018, p.19. https://www.bmvg.de/de/aktuelles/konzeption-der-bundeswehr-26384

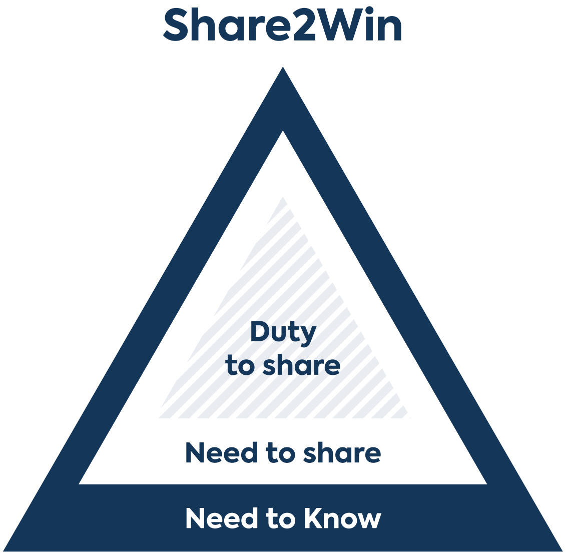
denominator. The technological concepts are less of a problem than the lack of interoperability standards and shared architectural approaches. The many different security domains, which span the national classifications of the countries involved, as well as shared NATO, EU or mission-specific requirements, present an obstacle. The inteoperability of high-security infrastructures is significantly hampered by this spectrum of posibilities – even though the security domain requirements sometimes only differ very slightly. From a technical perspective, standardisation would definitely be welcome at this juncture.

A prerequisite for achieving common standards and architectures is political and military will – and this already exists. As an example of strong interlocking at the operational-tactical level is the 1st German-Dutch Corps, where, among other things, German officers lead Dutch soldiers and vice-versa. In addtion, ten other nations work together as part of this corps. The fact that close-knit collaboration already takes place when it comes to joint advancement and procurement is demonstrated by the multinational Tactical Edge Networking programme (TEN).

Not just "need to know"; now it's "share to win"

In the multinational context, it has been shown again and again that the exchange of military information between partners can be crucial. When dealing with sensitive information, the "need to know" principle is therefore complemented by the "need to share" and even "duty to share" principles. Today, the technology used to do this is extremely sophisticated: SINA Workflow – a collaborative tool and digital management system for confidential information up to the German GEHEIM level and corresponding international classifications (SECRET) – ensures that sensitive information only ends up in the right hands and that those in possession of this information can be clearly identified. "Share to win" is the new buzzword, while the "need to know" principle continues to remain in place at all times.

Marcel Taubert



When working with different levels of classified information on a daily basis, many individuals in multinational offices wish for what became a reality at a national level a long time ago: highly secure data transfer across a variety of security domains and levels – and on a system without "swivel chair interfaces", i.e. without the user having to physically move between multiple workstations. Another demand relates to synchronous and asynchronous communiction and collaboration tools, including real-time exchange via video – with growing requirements vis-a-vis mobility. The infrastructure needs to be ultra-scalable and fail-safe (georedundant). Factors like resilience and flexibility are becoming increasingly important and, what's more, the solution should be "made in Europe" from the consideration of digital sovereignty.

Creating interoperability

All these requirements can be implemented technically today – using tried-and-tested solutions that have proven their worth on a national level for many years. One barrier to this is multinational interoperability, which is often still lacking. In many cases, standards will first need to be established and implemented. Where this has already been achieved to some extent, it often required very long development phases due to different premises for cryptography (algorithms). To counter this issue, interoperability standards should be kept to a minimum from a technical viewpoint.

In principle, approval requirements must be set sufficiently high to ensure the information is trustworthy and to prevent it from being misused. However, if the approval requirements are set too high, the usability and the value of a solution in specific use can suffer. The use and operating conditions must therefore be considered in the security requirements in order to achieve a balance between usability and security.

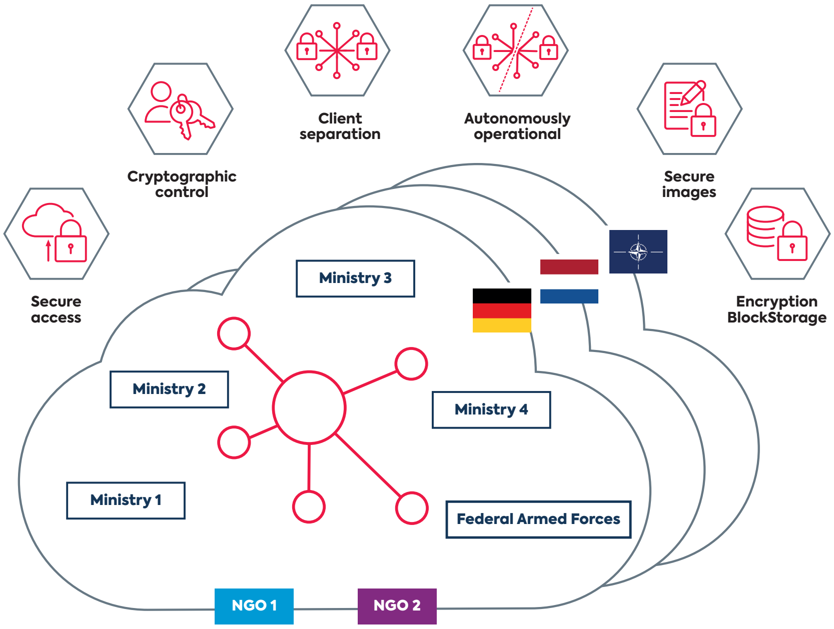
Market-available solutions

As a technical basis for highly secure multinational infrastructures, market-available solutions can be considered that offer multisession-capable clients at the front end, which can be used across all domain and security levels. The Secure Inter-Network Architecture (SINA) can achieve this. At the backend, instead of having a division at the hardware level, highly secure private cloud systems could be used in the medium to long-term. These have to enable strict client separation with controlled domain transitions.

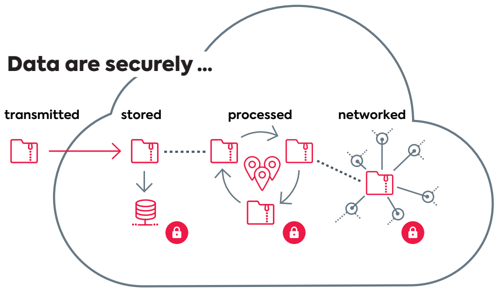
Highly secure cloud infrastructures could also be used as part of a whole-of-government cloud approach to promote interdisciplinary collaboration between various ministries and states and, on occasion, NGOs as well. This is becoming increasingly sought-after in ongoing conflicts and operations. To deal with these types of deployment scenarios a cloud must fulfil special requirements – e.g. in terms of client separation, protecting sensitive data, and handling proprietary cryptographic keys in a secure way. Proprietary cloud stacks, provided that they fulfil these requirements, cannot be easily procured, nor operated confidently; in addition, the security of these kinds of solutions cannot be evaluated. secunet closes these gaps with its highly secure, open source-based cloud operating system, SecuStack.

“Share to win” works – even if multinational cooperation still poses a considerable number of challenges. The current technologies already show what will be possible in the future. Cyber security aspects do not, therefore, act as a barrier to further interlocking, but point the way to it.

Marcel Taubert
marcel.taubert@secunet.com



In the whole-of-government cloud approach, the cloud must meet special requirements.



The SINA Workstation H R RW11 is specially hardened for harsh operating conditions.

SINA technology for NATO rapid reaction force

NATO's Very High Readiness Joint Task Force (VJTF), also known as the "NATO spearhead", is a rapidly deployable intervention force and part of the NATO Response Force. It is multinational, with strong involvement of the German Federal Armed Forces (Bundeswehr). The VJTF enables NATO to react even faster and more flexibly to developments in security policy.

The Bundeswehr has commissioned secunet to supply a significant quantity of SINA components intended for the IT infrastructure of the VJTF. The devices can be used to transfer, edit and store classified data. The order is due to be supplied by the end of 2021, and totals a double-digit million euro sum.

The order includes several hundred of the high-performance SINA Workstation H R, the design of which is based on a hardened notebook. It is intended for mobile use in particularly harsh operating conditions. The underlying hardware platform is especially protected against shock, vibration, dust and moisture and can also be operated at extreme temperatures. secunet is also supplying a large quantity of the highly secure SINA L3 Box H network components.

secunet acquires stashcat

Getting the message across securely

stashcat, the messenger that competes with Slack, Teams and Co., is based not in Silicon Valley but in tranquil Hanover. Since its founders, Christopher Bick and Felix Ferchland, launched the app on the market in 2016 it has continued to grow in popularity: the messaging service currently has over 1.3 million active users in companies, federal authorities and schools, as well as healthcare organisations, the police and the Federal Armed Forces – everywhere, in fact, where handling confidential information securely is particularly vital. The recent takeover by secunet offers exciting prospects.

stashcat founders Christopher Bick (left) and Felix Ferchland

It all starts with the idea of a social network that digitally maps all in-school communication in teachers' and students' day-to-day school lives. Two Hanoverians, Christopher Bick and Felix Ferchland, establish their first company and try to gain a foothold in the education market. It quickly becomes clear that, alongside emails, the majority of day-to-day communication in parent groups and classes takes place via messaging services like WhatsApp. These solutions are unsuitable for everyday school life, however, because they do not fulfil data protection and security requirements. It's not simply a case of falling back on existing alternatives to address the issue – and this is a problem that also affects very different industries and institutions.

The idea was born for a highly secure messaging service that would be made and hosted in Germany. In 2015, the two young founders start work on stashcat GmbH. The goal: to combine simple operability and the most stringent security standards in one messaging service and thereby to create an alternative to solutions with non-transparent data protection – the demand is monumental. After just two years the company wins key major clients such as the Federal Armed Forces and the police. In the educational market, too, the schul.cloud offshoot positions itself successfully and, today, is used by over 7,500 schools throughout Germany. The coronavirus pandemic has brought the focus back to digitisation in companies and federal authorities and has made the necessity of communication independent of time and place especially important. Small and medium-sized companies and authorities in particular are dependent on digitising their work processes quickly, easily and securely. In the words of Christopher Bick: "By the time the second lockdown happened, public consciousness had once again been awakened as to the huge importance of digitisation. Many users cannot be expected to rely on Silicon Valley. This is one factor determining why stashcat is already the market leader in some sectors".

stashcat's strengths

The core product is a GDPR-compliant, highly secure messaging service that, thanks to integrated file storage, extensive calendar features and a survey module, has stood the test as an accessible collaboration tool for teams in a wide range of different organisations. Additional options include video telephony and conferences. The solution combines the functionality of well-known messaging services and Cloud applications like WhatsApp or Dropbox, and is hosted in a German data centre in line with data protection regulations. stashcat offers other important features, such as a contact database kept independent from mobile phone numbers, with an LDAP interface and georeferencing. All mobile and stationary end devices are supported, and it can be used via app or browser.

The technology behind the app

When sending messages, encryption is performed at the user's device. All relevant data are therefore encrypted in transmission both to and from the server and are also stored on the servers in encrypted form. The data transferred are secured using the latest SSL/TLS encryption processes, which takes place en route between the servers and clients. The stashcat servers are located exclusively in Germany and measures are in place to prevent data loss as a result of hardware failure. These include the operation of redundant server systems and regular automatic back-ups. Users' data are stored directly in the company's own high-security data centre – and even then only the minimum data are retained. Since the messenger works independent from telephone and mobile numbers, no access to personal contacts is required.

stashcat heads to secunet – a partnership with prospects

"Messaging apps have become part and parcel of everyday life. In contrast to other messaging services, stashcat makes it clear that it prioritises security and data protection – this aligns perfectly with secunet's requirements and those of our customers," explains Axel Deininger, CEO of secunet. "secunet's acquisition of stashcat allows us to create an additional offering for secure, flexible communication and collaboration for use in companies, administration and security authorities like the police."

Lower Saxony's Interior Minister Boris Pistorius (left) presents the new police messenger "NIMes – Niedersachsen Messenger"

"We're pleased to have found a strong partner in secunet and one that wants to work with us to continue the story of stashcat's success," says CEO of stashcat, Christopher Bick.

The acquisition marked the start of an exciting process for both parties. Discussions are currently underway at the sales level for the foreseeable future, however there are plenty of opportunities for collaboration in the future. Aljona Wehrhahn-Aklender, the Product Manager at secunet in charge of the topic "SINA Collaboration", highlights a possible integration of the stashcat application into the SINA Workstations' guest systems for classified data as an exciting opportunity to integrate an intra-organisational messaging app into confidential networks. All of stashcat's benefits could be deployed for internal communication involving classified information, which would be a logical step towards expanding the functional remit of SINA Workstations. In terms of the future, stashcat and secunet remain in intensive discussions with regard to pan-institutional communication. Christopher Bick is excited about the future: "Both companies embody innovative strength and highly dynamic products. The shared requirements in terms of security in the software and hardware provided, combined with the experience and expertise that both companies have to offer, will lead to new and innovative solutions in the future".

✉ Christopher Bick
c.bick@stashcat.com

The Klinikum Fürth

Web isolation in hospitals

A healthy level of security

Hardly any sectors face a greater wave of challenges right now than healthcare – even without the difficulties caused by the ongoing pandemic. Long-standing staff shortages have come up against dynamic technological progress and networking, consolidation of sites, collaboration between a wide range of specialist groups working under extreme time pressure, as well as, of course, patients who quite rightly demand to be treated with respect – which also applies to sensitive data about them. How can we guarantee cyber security without creating a burden on the day-to-day running of medical care? Klinikum Fürth has had positive experiences using secunet safe surfer.

Free flow of information is one of the most crucial prerequisites for successful diagnosis and treatment: patient files must be accessible; doctors must be able to access the latest research findings; and the transfer of information between specialist groups within the hospital and external specialists must be seamless. Hospitals are therefore becoming increasingly reliant on their digital infrastructure. At the same time, they are exposed to the attack scenarios that all networked companies face. Time and again, malware such as ransomware – and other incidents like phishing attacks – affect even healthcare institutions, causing damage that is not just financial in nature.

Cyber attacks in hospitals put people's lives at risk

The last major attack on a hospital was committed in September 2020: the Universitätsklinikum Düsseldorf was infiltrated by the "DoppelPaymer" ransomware. This encrypted 30 of the university clinic's servers, incapacitating large parts of research and patient care. According to the

> "Even during the one-month trial, safe surfer proved a success with users due to it being easy to use."
>
> Alexander Zetlmeisl, Head of IT at Klinikum Fürth.

extortion letter, the attack had in fact been targeted at Heinrich Heine University – this didn't change the fact, however, that the functional failures in the clinic affected its patients. Some of them had to be moved to medical establishments further away.

Back in March 2020, the university clinic in Brno in the Czech Republic was also affected by a ransomware attack. Here, in the midst of the first wave of the coronavirus pandemic, one of the largest SARS CoV 2 laboratories in the country was incapacitated – and here, too, patients had to be relocated to clinics further away.

Security through separation of workplace and internet access

Internet access at work often becomes the gateway for malware and phishing – despite common security measures such as virus scanners, firewalls and content filters. Preventing internet access entirely is, however, not an option in an organisation as disparate and dependent on information as a hospital. What is actually needed is a solution that provides users with convenient access to resources in the network and, in parallel with this, successfully prevents malware from infiltrating the network.

secunet safe surfer functions as a browser isolation solution and data lock for using the internet securely. The solution has been developed based on the German Federal Office for Information Security's Remote-Controlled Browser System (ReCoBS) and Browser-in-the-Box security architectures. Every browser session therefore takes place in a sealed-off environment within a specially hardened Linux system that in turn runs in a separate network segment. This remote browser session is controlled remotely from the workplace solely via video stream – only images and sounds are transmitted. This extremely fundamental separation ensures that even hardware-related attacks can be fended off – alongside all common hazards, such as infected websites. Nonetheless, safe surfer also allows users to create personal favourites, and upload and download files like a native browser. Using the additional safe reader function any infected email attachments can be blocked effectively. If the user opens a compromised attachment with safe reader, the malware cannot reload any malicious code, since there is no direct connection to the internet.

Successful installation at Klinikum Fürth

User-friendliness is the decisive factor when it comes to using an IT security solution in healthcare settings. safe surfer was developed to be used like a conventional browser with the whole suite of convenient features. This ensures a good level of acceptance among users, and IT departments are not burdened with having to manage time-consuming training sessions.

This is also confirmed by the experiences of Klinikum Fürth, which installed safe surfer throughout its facilities in 2020.

The clinic was galvanised into action to install safe surfer following reports in trade journals of cyber attacks on large clinics, as well as experiencing a direct attack (Emotet) itself in December 2019. In February 2020, the clinic contacted secunet and an initial webinar took place with selected members of the IT department. The introductory project began shortly afterwards.

Project expanded at the employees' request

The trial phase confirmed the hope that the solution would be accepted: "Even during the one-month trial, safe surfer proved a success with users due to it being easy to use. This led us to significantly increase the number of licences in the pilot project at the

About Klinikum Fürth

Klinikum Fürth – a specialised medical care clinic and university teaching hospital at the University of Erlangen-Nürnberg made up of 13 departments as well as institutes and centres – is an economically successful level 2 medical care clinic with strong roots in the region. The clinic has 771 beds, in addition to 36 beds in Geriatric Rehabilitation. Each year, a workforce of over 2,500 dedicated employees cares for 42,000 inpatients and 58,000 outpatients, providing the highest level of medical and technical care. In particular, this includes minimally invasive, robot-assisted surgery. As part of one of the largest hospital projects in Bavaria, the modernising, visionary remodelling of the Fürth hospital complex has already begun with the extensive structural expansion and renovation.

employees' request, so that now all parts of the clinic benefit from secure internet access," explains Alexander Zetlmeisl, Head of IT at Klinikum Fürth.

On account of the pandemic, installing the software took slightly longer than under normal circumstances, with the implementation phase lasting from spring to summer 2020. safe surfer has been up and running since July 2020, however. Flexible expansion will also be possible in the future since safe surfer is scalable during continued operation, with a transparent licensing model.

Acceptance on the wards as well

safe surfer was therefore used in patient areas too and did not lead to a noticeable increase in IT support requests, according to reports from Klinikum Fürth. "You use the browser almost exactly as you normally would. As an example, I can copy links in the browser bar, enter data online, or download relevant data securely. Especially in times of great change, as in the current pandemic, having a system that enables fast, uncomplicated and secure data transfer with other clinics – for instance on online portals for free treatment capacity – is vital, and essential for day-to-day work," says Dr Manfred Wagner, Medical Director and Pandemic Officer at Klinikum Fürth.

On top of this, safe surfer spares resource in the IT department: it can be managed centrally for all departments thanks to a management server. Numerous standardised interfaces help with integration and automation.

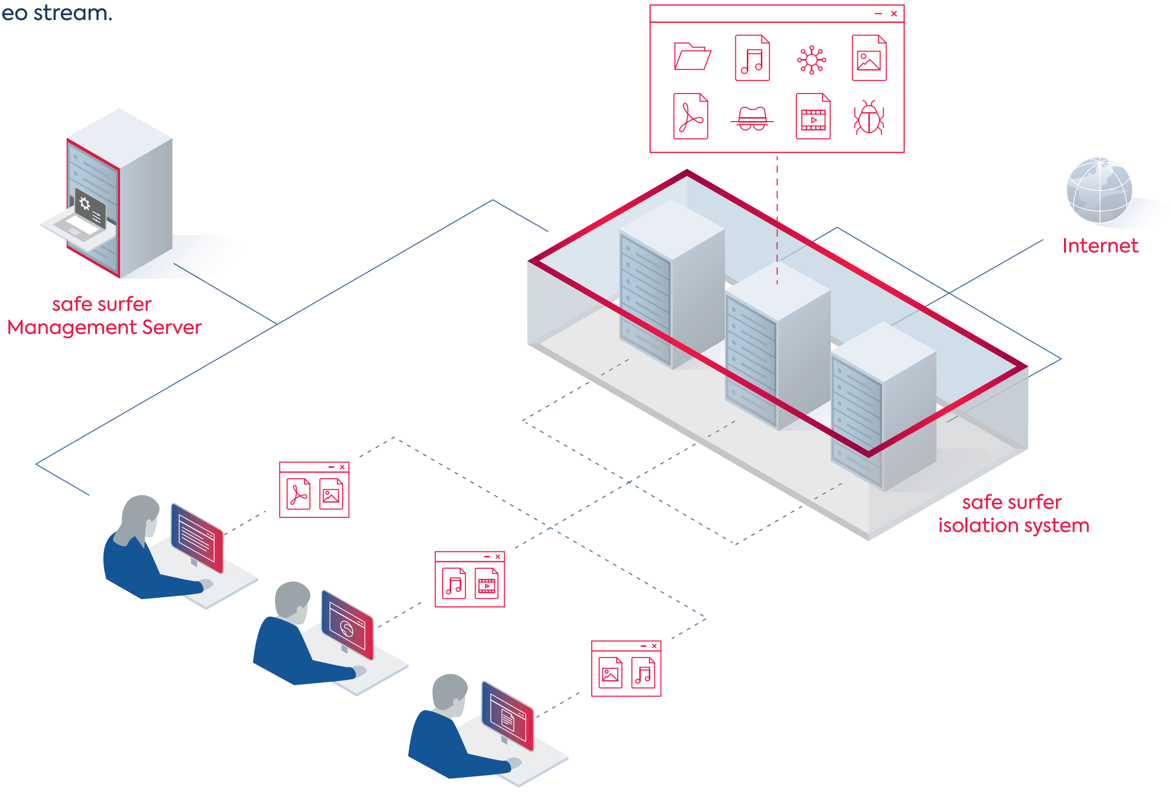
Attack vectors are fended off – and not just the well-known ones

Klinikum Fürth is confident that, with safe surfer, it has found the best solution for keeping its systems isolated from unknown sources. "The Federal Office for Information Security recommends protecting internet access via a Remote-Controlled Browser System (ReCoBS). We are pleased to have followed this recommendation by introducing secunet safe surfer, so as to comply with the stipulations of the German IT Security Act for CRITIS protection in this respect, too," says Herbert Motzel, Head of the IT Security Systems department at Klinikum Fürth.

Markus Ohnmacht
markus.ohnmacht@secunet.com

Interested institutions can obtain short-term access to the Cloud test environment for secunet safe surfer and find out more about the browser isolation solution for themselves.

With secunet safe surfer, every browsing session takes place in a sealed-off environment and is only remotely controlled from the workplace via video stream.



Information technology plays an important role in everyday work in hospitals today.

Digitisation in hospitals

A secure diagnosis

In Germany, electronic patient files are just the latest symptom of a profoundly progressive digitisation process that concerns the whole healthcare sector, including hospitals. However, digital progress requires IT security if it is to bring more benefits than risks. secunet is here to offer support thanks to its many years of experience and extensive expertise.

Digitisation in medicine is not an end in itself: large-scale pandemic situations, demographic change, acute skills shortages, challenging pathologies and optimised treatment options demand operational performance from clinics around the clock. Administrative and care processes will only work if practitioners have seamless access to medical information and applications. “The diagnosis is clear – as is the treatment: only a modern, digital infrastructure and the networking of numerous data sources and medical equipment will take the strain off hospitals and improve treatment options. In parallel to this, the increasing level of digitisation also means greater vulnerability – new attack vectors for cyber attacks, or a lack of controllability over complex IT,” says Torsten Redlich, Head of Business Development and Deputy Head of the eHealth division at secunet.

In order to protect healthcare institutions as far as possible from these hazards, the German federal and state governments have established a Hospital Future Act (KHZG) to promote digitisation in clinics. This states that a minimum of 15 per cent of the funds set aside for any funding project must be earmarked for IT security. This acts as an important basis for hospitals to take full consideration of data protection and data security within their projects right from the beginning.

Industry-specific standard defines the security requirements

To establish a uniformly high level of protection for business-critical IT, IT security measures for hospitals are aligned with an industry-specific standard (in German, “branchenspezifischer Standard”, B3S) that is also designed to provide direction for non-critical infrastructure (non-CRITIS) institutions. It is compulsory for CRITIS institutions. “To fulfil the requirements of B3S it is important not to focus purely on individual aspects of the infrastructure or selective solutions,” says Redlich. “An all-encompassing security architecture is required. In addition, IT security solutions should demonstrate a high level of user-friendliness so as to ensure that there is no detrimental impact on the clinic’s everyday workload.”

secunet safe surfer is one such user-friendly solution. This allows hospitals to make general internet usage secure in sensitive workplaces: external threats such as compromising websites, phishing links, concealed (encrypted) communication designed to establish external control or data leakage are rendered harmless. To find out what this looks like in practice, please see the “Healthy level of security” article on page 26.

Cloud on the horizon

The next phase of the digital transformation is already imminent: “The trend for data processing in healthcare is moving further and further in the direction of hyper-converged infrastructures, the amalgamation of local and central data processing, and the associated overarching processes,” explains Redlich. “Virtualised, centralised IT services are often still operated ‘on the premises’ due to compliance provisions, yet are moving strongly in the direction of storage in the Cloud.”

Further concepts are therefore currently being tested, such as trusted Cloud infrastructures, edge platforms and (distributed) Federated Machine Learning. The objective is to securely tie together all spheres of activity within medical care, e.g. medical networks, medical technology, evaluation analysis and medical robotics – including in outsourced computing and storage environments (Cloud). The first thing to do here is to clarify trailblazing security issues in accordance with German legislation and to implement the available security technologies as a basis for many new applications. secunet provides advice on this to hospitals, producers of medical technology, and suppliers of medical software solutions and implements secure, trustworthy infrastructures.

Torsten Redlich
torsten.redlich@secunet.com

Secure access to the German electronic patient record

Since the beginning of 2021, the electronic patient record (elektronische Patientenakte, ePA) has been available to people with statutory health insurance in Germany. Doctors' surgeries, pharmacies and hospitals can access it via the telematics infrastructure. To do this, they need a connector with software upgrade for product type version 4 (PTV4). In May, the secunet konnektor was the first on the market to receive approval for PTV4.

Back in January 2021, secunet and its partner eHealth Experts launched a test phase with the upgrade for the ePA. In selected doctors' offices and hospitals, the functionality and security of the connector was successfully demonstrated in accordance with gematik's specifications. The gematik is the operator of the telematics infrastructure.

"Although secunet, together with its partner eHealth Experts, entered the connector market late, we are of course very pleased that we were the first to receive approval for the ePA upgrade. For us, this is also confirmation of the quality of our work," explains Markus Linnemann, Head of the eHealth division at secunet.

The aim of the ePA is to comprehensively network the German health care system, both between the various specialists or pharmacies and between doctors, pharmacies and patients. Many work steps that were previously carried out in analogue or paper form can be digitalised and thus simplified by the ePA. Further advantages: Medical information is available transparently and will facilitate many processes in the future. This benefits patients as well as doctors, pharmacists, therapists and other medical professionals. The establishment and use of an ePA is voluntary for patients.

Cyber security for networked vehicles

"The whole automotive sector should address the issue"

Vehicles are constantly getting smarter and more autonomous. Manufacturers are equipping them with ever more subsystems that are supplied with information by sensors. The aim is to enable vehicles to react with greater autonomy in particular traffic situations. At the same time, car manufacturers rely on sophisticated software. The objective is to make the driving experience safer and more convenient and, above all, to enable communication between vehicles and between the car and the transport infrastructure. The automotive sector is developing into a highly connected system with a correspondingly large number of interfaces. This in turn increases the possible attack surface. In the future, it is only by implementing consistent security standards and strategic system design in place of standalone solutions that we will be able to ensure complete safety in traffic.

From parking assistance to autonomous driving – vehicle software and hardware technology is becoming more diverse and complex day by day. Driving assistance systems that rely on the internet, optical cameras and radar equipment are now included as standard features, and it's only a matter of time before we see fully autonomous vehicles on public roads. This not only requires sophisticated algorithms, but also increasing amounts of external information. The disadvantage: the more connected and intelligent a transport infrastructure becomes, the more serious the effects of any potential manipulation of this system. This not only applies to individual drivers, who have to trust that the information processed by their car is correct; it is even conceivable for a whole infrastructure system to collapse as a consequence of targeted interference.

Vehicles are becoming part of a system vulnerable to potential attacks

"For full IT security in the transport infrastructure it is not enough simply to make the cars themselves secure. The more autonomous cars become, the more they depend on external information," explains Jochen Schönweiß, Account Manager at secunet, who looks after industrial clients in the southeast region of Germany and in Austria. The information is, for example, transmitted by traffic management systems – more specifically, by roadside units which process data on the condition of the roads, accidents and possible hazards, among other things. This technology aspires to optimise road safety and traffic flow, as well as reduce vehicle emissions, e.g. by means of a shorter drive time. Nonetheless, a car that meets high IT security standards yet is dependent on the functions of a potentially manipulable environment remains fundamentally at risk.

According to Schönweiβ, "Cyber security in the automotive sector cannot be achieved purely through standalone solutions – especially not in the case of a highly networked, intelligent transport infrastructure. Manufacturers and suppliers must therefore consider the entire technical chain, from hardware, control units, and internal and external communication interfaces through to backend. They then need to aim to create an all-in-one solution in the form of a comprehensive and secure system design."

The car – a special candidate for IT security

However, even guaranteeing a single vehicle's IT security is anything but trivial. One fundamental difficulty is that a car's hardware typically stays the same throughout its life cycle, i.e. for 20 years or more. This would be unthinkable in the world of fast-moving consumer electronics – as well as in other IT sectors, where hardware is completely replaced at regular intervals. In contrast, at some point in its life cycle the hardware of an otherwise still roadworthy car becomes so old that it no longer fulfils the requirements for integrating the necessary software updates. The automotive industry faces a major challenge in this respect.

In addition, while it is true that conventional standalone IT solutions like public key infrastructures (PKI) or hardware security modules (HSM) prevent data from being altered or read, this is of little use, however, if the access to the standalone solutions is itself not protected. "In the worst-case scenario, HSM and PKI continue to help perfectly with encryption and signing following an attack – but are actually helping the attacker who has infiltrated the system," says Schönweiβ. Furthermore, data integrity can be ensured using a security chip, for example. However, this measure is rendered ineffective if a second piece of software responsible for analysing the result is open to manipulation. The best protection of the key interfaces is useless if a vulnerability can be exploited and a potential gateway opened via the car's infotainment system.

One step ahead of the future

These examples show that IT security for networked vehicles needs to be approached from a holistic perspective. Flexibility is also an important concept though: requirements and technologies change, and automotive companies need to be prepared for this. Because of this, the solutions from secunet are not limited to a specific HSM manufacturer, for instance. They even allow HSMs from different manufacturers to be operated simultaneously using an in-house hardware abstraction layer. The AWS CloudHSM solution is likewise supported. Added to this, microservice

Jochen Schönweiß
jochen.schoenweiss@secunet.com

Harry Knechtel
harry.knechtel@secunet.com

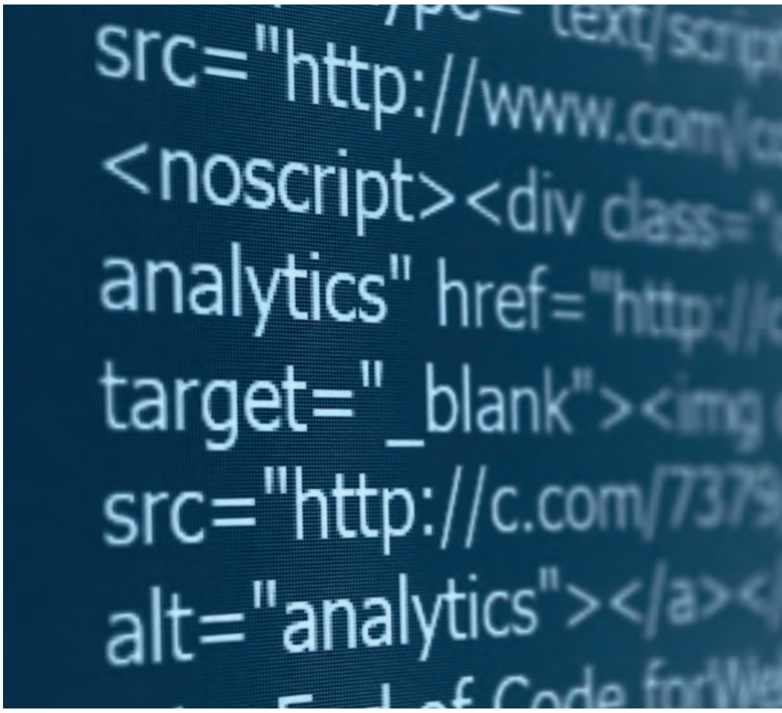
deployment is also an option, meaning secunet can make its PKI available in the form of docker containers. Furthermore, secunet is developing prototypes whose specifications are not yet covered by the market and is already implementing algorithms that are resistant to quantum computers.

The search is on for industry-wide standards

"PKIs and HSMs can be important elements within a consistent system design insofar as they work effectively in combination with other security components within a harmonious overall architecture," says Harry Knechtel, Head of Development in secunet's Industry division. He adds: "At this juncture, however, the spotlight is on the whole sector, which needs to agree on a set of framework conditions, or, better still, on specific standards for the safety requirements for certain products." A good example of the standardisation of Vehicle-to-Infrastructure communication is ISO standard 15118, which is an international standard governing communication between electric vehicles and charging infrastructure that secunet was involved in developing. It enables faster, easier vehicle charging for users – the motto is "Plug & Charge" – and, at the same time, protects associated data such as information regarding charging contracts via the use of digital certificates.

Developments such as these illustrate the opportunities that consistent IT security standards offer the industry. This is because, in addition to the crucial security aspect, consistent standards enable greater compatibility and, therefore, the sought-after flexibility of IT solutions assisted by modularisations. "All things considered," Knechtel concludes, "comprehensive regulations would also increase the cost-effectiveness of cyber security in the transport infrastructure – and thus also the level of IT security itself."

For more on this topic, see the cover interview in ATZelektronik, edition 6/2021:



Live hacking as a security awareness measure

Developing a digital gut feeling

"How many of you use the fingerprint reader on your mobile phone?" asks the IT security expert from secunet. Around half of the approximately 90 participants raise their hands and soon learn how easy it is to imitate a fingerprint. The two secunet experts on the podium use modelling clay to form a positive of their own previously captured fingerprints and demonstrate that this can be used to unlock a mobile phone. On this morning, it is just one of many examples that show the tricks cyber criminals can use to quickly overcome alleged hurdles. The so-called live hacking is the prelude to an awareness campaign with which the employees of a company will be made aware of the topic of IT security and their own handling of it in the following months by means of training, posters, flyers and more.

Digitalisation is advancing in companies and public authorities. In order to be able to securely provide the technology that is used every day, IT managers take many technical measures. But it is equally important that employees ask themselves questions like these: How secure are my chosen passwords? How careless am I with email attachments?

Those who develop a "digital gut feeling" are well armed against digital threats. "About 70 percent of all IT attacks are initiated by users," says Falk Gaentzsch, Senior Consultant at secunet. For example, security advisories or error messages are often ignored. "We are conditioned to quickly check the box and continue clicking. But taking a closer look is important: If something seems strange to me, a call to the IT department helps," says Gaentzsch. Sensitised employees are the biggest hurdle for email-based attacks on IT systems.

Grabbing data in front of an audience

In live events, security experts demonstrate how easy hacking has become: they show, for example, how malicious software smuggled in via email attachments can be used to read the hard drive. The prey: passwords, e-mails or secret quarterly reports. Malware construction kits are easy to buy on the internet, as a trip to the corresponding websites proves. The experts also warn against careless use of WLAN while on the move. "The mobile phone connects to the strongest signal. This knowledge is also used by fraudsters who set up a public WLAN and grab data," says Gaentzsch. The secunet experts demonstrate live that only a little technology is needed to make a WLAN signal appear on a colleague's mobile phone and on the mobile phones of the listeners.

Use long passwords

Password guessing shows how good passwords can help to make access to data more difficult. Participants in a live hacking session are asked to find out the passwords actually chosen by computer users of an anonymised company – and they usually find them: More than a quarter of the passwords can be guessed with a little creativity. These include, for example, the company name or the terms "secret", "summer" or "password". "We recommend a password with at least twelve to 14 characters," says Falk Gaentzsch. It can be remembered, for example, by choosing the first letters and numbers of a personal mnemonic. All passwords can also be securely managed in a password vault.

Develop countermeasures

Live hackings show many different facets of the methods attackers use to manipulate computer systems or obtain information. However, the main focus is always on the concrete countermeasures that each user can take personally. After all, the participants should not be demotivated, but sensitised.

Various thematic focuses

No two live hacking sessions are the same. On the one hand, this is due to the interactive format in which the audience is involved and the experts respond individually to the questions of the participants. On the other hand, there is an almost infinite number of different topics that can be presented. These range from special topics such as "Hacking SCADA systems used in industry" or "Security of Active Directory" to everyday topics such as "Email security" or "Security of USB devices" to special events where everything revolves around the topic of "Social Engineering".

In the end, however, it is important with all topics that they are presented with a certain twinkle in the eye. Even if you are not used to this from other areas of IT security, you are allowed to smile and laugh here – this is also a way to build up a digital gut feeling.

✉ awareness@secunet.com

Deutschlandstipendium scholarship scheme

Prospects for talented young people

To support students of computing and related subjects, secunet is taking part in the Deutschlandstipendium scholarship scheme. We interviewed Svenja Reinhardt, Head of Human Resources at secunet, to find out what the scheme involves and its significance for the company.

Mrs. Reinhardt, how is secunet aiming to remain competitive and future-focussed in terms of recruiting staff?

Svenja Reinhardt: Our employees are our company's greatest asset. As in other industries, however, it's getting harder and harder to find skilled specialists. It's therefore all the more important for us to make contact early on with students in order to raise awareness of IT security. Many students on computing courses are completely in the dark about just how many exciting prospects this specialist area of IT has to offer.

secunet has worked in close partnership with various universities for a long time, both in terms of research and recruiting. In addition, we are also getting involved in the Deutschlandstipendium scheme organised by the German Federal Ministry of Education and Research. By doing this, we want to give the topic of IT security a face at universities, while also supporting talented individuals and getting them excited about secunet. This year, we have awarded eight scholarship places in total. The scholarship stipend will begin this winter term.

Can you describe the selection process for the stipend to us? Are there specific criteria at play?
The Deutschlandstipendium scholarships are targeted towards students in the first semester of their undergraduate degree. The students' names are put forward by their university based on various decision-making factors that are deliberately broad in focus, such as performance, social engagement and social background. We then contact the students. It is also extremely important to us to recruit women to the field of IT security. The IT security industry is still quite male-dominated. Because of this, we made the deliberate decision to select three female students at the Ruhr-Universität Bochum for the scholarship places.

What does supporting the students look like in practice?
All students selected for the scholarship scheme will be guaranteed to receive EUR 300 per month for a minimum period of 12 months, i.e. two semesters. The funding comes from both secunet and the Federal Government. The duration of the scholarship will not be the same across the board, however, as it depends on the university in question. In some cases, the student will need to apply for the stipend annually; while other universities offer a complete programme for the duration of the course of study.

The most critical aspect for us is that we are interested in long-term collaboration with the next generation of talented individuals. This is the case anyway, irrespective of the Deutschlandstipendium scheme. We operate 12 sites across Germany, thus having footholds locally close to all the universities we partner with. Students therefore have the opportunity to get to know secunet as an employer locally via internships or as working students or while working on their bachelor's or master's degree theses.

Svenja Reinhardt

svenja.reinhardt@secunet.com

Generally speaking, does the IT security industry in Germany need to do more to make the sector more attractive to graduates?
A lot has already happened in this respect in recent years: secunet, for example, funds an endowed chair at the Institute for Internet Security at the Westphalian University of Applied Sciences in Gelsenkirchen. Commitment is worth it – and not just for the business per se: ultimately, this concerns the digital sovereignty of Germany and Europe vis-a-vis IT security, an issue that will shape the future.

The German Federal Ministry of Education and Research set up the Deutschlandstipendium scholarship scheme ten years ago. This mechanism enables the Federal Government and private sponsors to invest in the future of talented students at the start of their university careers. The scheme is also designed to motivate talented individuals and support them on their path. This way, the State and society take equal responsibility for the future of Germany.

Security for Industry 4.0

secunet and Tech Data sign distribution agreement

secunet and Tech Data, one of the world's leading IT distributors, have entered into a cooperation agreement. The focus is on the solution secunet edge, which enables secure digitization, networking and automation in the Industrial Internet of Things (IIoT) and in edge computing. This enables companies to exploit the enormous potential of Industry 4.0 while minimizing security risks.

With this contract, Tech Data is further expanding its extensive portfolio of IT security solutions in its "Advanced Solutions" unit, adding IIoT security. System integrators and sales partners of Tech Data can now offer their customers tailored IIoT solutions based on secunet edge and thus drive the digital transformation in industry and critical infrastructures.

"In the industrial environment, we are increasingly relying on indirect sales," says Axel Deininger, CEO of secunet. "In Tech Data, we have gained a strong partner for this. Tech Data's sales expertise and excellent market position ideally complement secunet's technological expertise in the field of Industry 4.0."

Ralf Stadler, Director of the Security, Mobility & IoT Business Unit at Tech Data DACH, on the new contract: "I am very pleased about the conclusion of the contract with secunet, with which we can now offer our sales partners in the industrial sector security solutions even more concretely. secunet has proven in many projects that they can set up and implement resilient, secure digital infrastructures. A perfect complement in my eyes also for our Datech Solutions partners, who address many customers in the Industry 4.0 segment."

secunet makes a donation to Aktion Deutschland Hilft

The flood disaster in western Germany and other European countries has cost many lives and destroyed livelihoods. The inhabitants of the affected regions and towns will have to deal with the effects of the events in July 2021 for a long time to come.

To support the flood victims, secunet has donated 50,000 euros to Aktion Deutschland Hilft. This alliance of German aid organisations provides coordinated aid in disaster areas.

Anyone who would like to find out more about the alliance or also make a donation can do so on the following website:

www.aktion-deutschland-hilft.de/en/

Dates – October to December 2021

Due to the corona pandemic, changes are to be expected.

12–14 October 2021
it-sa | Nuremberg, Germany

19–22 October 2021
Milipol | Paris, France

26 October 2021
inova | Ilmenau, Germany

3 November 2021
Off-the-Record (Handelsblatt Health Circle) | digital

15–18 November 2021
Medica & Compamed | Dusseldorf, Germany

22–24 November 2021
IKT Security Conference | Linz, Austria

24–25 November 2021
Berlin Security Conference | Berlin, Germany

7 December 2021
Azure Developer Community Day | Munich, Germany

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

Imprint

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

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

Design and Setting
sam waikiki GbR, www.samwaikiki.de

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

Photo credits
Title, p. 10: European Commission
p. 2, 4, 29, 31, 33: Adobe Stock
p. 3, 11, 12, 14, 18, 19, 21, 22, 23, 28, 37: secunet
p. 16: SSARM
p. 24, 25: stashcat
p. 26: Klinikum Fürth
p. 34: Bildschön / secunet
p. 35: alamy

climate neutral
print
www.klima-druck.de
ID-No. 21108075
bvdm.

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