

A portrait of Professor Andreas Pinkwart, a middle-aged man with short, light-colored hair, smiling warmly. He is wearing a dark suit jacket, a white shirt, and a blue patterned tie. The background is dark and out of focus.

## “We Need More Innovation Than Ever”

**Professor Andreas Pinkwart,  
the State of North Rhine-Westphalia’s  
Minister for Economic Affairs,  
Innovation, Digitalisation and Energy**

A decorative horizontal band consisting of diagonal stripes in red and black.

### Home office with sensitive data

How can organisations provide mobile workstations without compromising security?

### Dangerously versatile: Emotet

How can enterprises and authorities protect themselves against this type of attack?



**28** Edge computing in the Industry 4.0: Digitalised, networked – and secure

Network analysis for critical infrastructures: Knowing what is happening in your network **24**

## National

- 4 SINA at Deutsche Rentenversicherung Bund: Security Multiplied by 5,800
- 8 Professor Andreas Pinkwart, the State of North Rhine-Westphalia's Minister for Economic Affairs, Innovation, Digitalisation and Energy: "We Need More Innovation Than Ever"
- 11 IT security according to the BSI's requirements: Fit for Information Security Management with IT-Grundschutz 2020
- 14 Online Access Act: ELSTER: Easy E-Government Login via Smartphone

## International

- 15 Automated border control: secunet easygate – Now at a Land Border for the First Time
- 16 The new generation of the secunet easygate: Always a Sleek Transit
- 18 Pre-registration of travellers: Process Accelerator at the Land Border

## Technologies & Solutions

- 20 Emotet in large companies and public authorities: Dangerously Versatile
- 24 Network analysis for critical infrastructures: Knowing What is Happening in Your Network
- 28 Edge computing in the Industry 4.0: Digitalised, Networked – and Secure
- 30 Collaborative work with documents up to SECRET level classification: Secure CI Distribution – with a Few Clicks
- 32 Home office with SINA: Mobile Working – without Compromising Security
- 33 Revival of the thin client: Less is More



- 35 Telematics infrastructure in the German healthcare system: secunet konnektor "eHealth" Approved and Available Now
- 36 New German eHealth applications: "An Emergency Dataset is Quick to Create and Incredibly Useful in Action"
- 38 From the Pentest Lab: LLMNR: The Underestimated Danger

## News in Brief

- 40 European External Action Service Uses SINA
- 40 Secure mobile working: BWI procures SINA Workstations S for the German Federal Armed Forces
- 41 Goodbye ISDN. Hello All-IP.
- 42 Evolution Instead of Revolution: secunet in the New Corporate Design

## Service

- 43 Dates – September to December 2020
- 43 Imprint

## Dear Reader,

Much has already been written about how challenging the times are – and indeed they are, beyond a shadow of a doubt. However, it is also remarkable how quickly many companies and public authorities have been able to adapt. At the start of the pandemic, they were suddenly confronted with the need to ensure almost their entire staff could work from home – and without weakening security. This was not merely a question of technical feasibility; many of them were also forced to change their company cultures overnight.

In hindsight, the latter has proved to be the bigger challenge – after all, the necessary technology already existed. The crisis has thus demonstrated just how far advanced digitalisation already is. The connected world and flexible working have long ceased to be visions of the future as they are still often portrayed – they are now a reality. When we order goods digitally using our smartphones, we set a supply chain in motion that is also coordinated digitally. Then, the retailer digitally restocks its warehouse. Such possibilities have existed for some time, and it is no different with the home office; most public authorities and companies had already gained some experience of remote working before the corona crisis, albeit not to the extent that such work has now become necessary. Fortunately, the crisis has only boosted the process of digitalisation; it was not the starting point.

In the last few months, it has also become clear that digitalisation must go hand in hand with security. This is because only those who are sure that digital infrastructures are secure will be happy to use them. This applies regardless of the coronavirus pandemic. When the crisis abates, the digital transformation will switch gears, moving from high speed to a more normal pace. Nevertheless, it will continue and will therefore require secure solutions.

In the latest edition of *secuview*, we discuss some possible examples. I am especially delighted that North Rhine-Westphalia's Minister for Economic Affairs, Innovation, Digitalisation and Energy, Professor Andreas Pinkwart, has offered his perspective on the digital transformation and the impact of coronavirus in his interview.

By the way: We have updated our corporate design and company logo. *secuview* is therefore also boasting a fresh look. We hope that this will help to further enhance your enjoyment of our magazine.

Stay safe and well!



Axel Deininger



SINA at Deutsche Rentenversicherung Bund

# Security Multiplied by 5,800

Deutsche Rentenversicherung Bund (DRV Bund) is an authority with close to 25,000 employees who look after 23 million policyholders. According to the CRITIS regulation issued by the German Federal Office for Information Security (BSI), DRV Bund is classed as a critical infrastructure and is therefore especially worth protecting with regard to cyber threats. In 2018, DRV Bund therefore decided to retrofit all existing mobile and home office workplaces with secure SINA S Workstations by the end of 2019. After all, this was about setting up over 5,800 workstations. Together with technical service provider Samhammer AG, secunet turned around the mass roll-out on schedule.

Once a large authority has made the decision to adopt a SINA solution, plans for the roll-out and the design of the overall infrastructure are set in motion. At this scale, however, there is a lot of work to be done: in addition to the actual tasks, design and installation of the technical solution, logistics need to be organised, partners involved, installation offices set up and, not least, users and SINA administrators need to be trained. In this instance it pays off for the client to be able to plan the entire project with a partner. In the case of DRV Bund, secunet acted not only as a supplier of solutions, but also as the partner for the roll-out.

The company had already amassed the relevant experience. Indeed, the SINA Workstation was originally designed to be a high-quality IT security solution for small groups of users. Over the past decade, however, secunet has implemented numerous large-scale official projects with the product, including installing it throughout several Federal ministries. This made it clear that the SINA Workstation S was suitable for mass roll-out. SINA automation tools were developed at that point to facilitate the configuration of larger installations. At DRV, too, these tools helped to keep the project efficient.

This wasn't the first SINA installation for DRV Bund. Since 2017, the authority has been using a SINA solution which enables around 100 administrators at DRV Bund to dial into the authority's central IT environment securely while being physically located elsewhere. As the experience with this installation was positive throughout, nothing more stood in the way of setting up a SINA infrastructure on a large scale.



## Main office of the Deutsche Rentenversicherung Bund, Berlin

### A complex starting point

This time the scope was far more extensive, which entailed a few challenges when it got down to the nuts and bolts: users of the mobile workstations that had to be re-equipped with SINA were spread over DRV Bund's five administrative sites, various external sites such as the customer contact centre and rehabilitation clinics as well as 19 inspection offices with over 2,000 auditors. In addition, there were approximately 900 home office workstations across Germany that had to be visited in turn in order to install the devices and train users.

A further detail increased the pressure of the deadline: DRV Bund had decided to carry out the SINA installation as part of a migration from Windows 7 to Windows 10 that was due to take place anyway. Combining the two made sense from an organisational point of view, since it amalgamated two IT projects into one, thus saving considerable workload for DRV Bund. Nonetheless, it also meant there was a hard deadline for the SINA installation and roll-out: the manufacturer support for Windows 7 ended as 2019 drew to a close, therefore all users at DRV Bund who were affected had to be provided with a SINA Workstation S at that point on a device running Windows 10.

### Extensive preparations

This meant that, at the end of the design phase in November 2018 when concepts for operation, networking, clients, training, installation and rollout had been coordinated and set up, about a year remained. It was the task of the DRV Bund rollout team to develop a distribution plan for the well over 5,000 future SINA users.

In the first phase DRV Bund and secunet built up the SINA infrastructure to which the SINA S Workstations could be securely connected as mobile clients.

Using a **SINA** solution, authorities whose employees handle sensitive or even classified information can set up secure mobile and home office workplaces. Thanks to a variety of interlocking security components, SINA ensures that third parties are unable to read any data if the user accesses the authority's network via a Virtual Private Network (VPN). Even if a SINA laptop gets lost, the data remain protected thanks to two-factor authentication and hard disk encryption.

For further information go to: [www.secunet.com/en/solutions-services/securenetworks/sina/](http://www.secunet.com/en/solutions-services/securenetworks/sina/)

It was designed to have a high level of availability, to enable the clients to be used reliably at any time; and scalable, so that future extensions of the installation would be straightforward to implement. During the implementation of the SINA Box clusters and their integration into the existing DRV data centres, many detailed questions arose to which the DRV Bund and secunet had to find suitable answers.

For the planned marathon – the mass installation of the clients – in tandem with DRV, secunet established two installation centres on DRV's premises with a total of 120 installation spaces. A panoply of issues had to be clarified for these centres, on topics such as power supply, waste heat, access to a freight lift, protected access and network technology, among others.

A comprehensive roll-out also requires tailored logistics design. The SINA Workstations were initially housed in anti-theft wire mesh containers.

**Deutsche Rentenversicherung Bund** is the largest provider of German pension insurance. The company's headquarters are located in Berlin and it has offices in Brandenburg, Gera, Stralsund and Würzburg. Close to 25,000 employees look after around 23 million policyholders and almost 10 million pensioners in Germany and other countries.

In addition, approximately 11,000 smartcards for authentication to the clients – each user received two copies – first had to be written and then sensibly labelled and stored.

Another important part of the preparations were the compatibility tests of the DRV Bund applications in conjunction with Windows 10 as the guest system of the SINA Workstation. Once all hardware and software combinations had been approved, the go-ahead was given for the mass installation of SINA Workstation S.



This installation office was set up especially for the project.



As part of the project,  
more than

11.000

SINA smartcards  
were created.

#### Successful choice of partner

secunet brought an experienced partner on board for the technical implementation of the project in the shape of Samhammer AG. The technicians at Samhammer carried out the large-scale installation of the SINA S Workstations within DRV's premises, distributed the devices to employees at DRV Bund as part of training sessions, fixed any technical issues and wrote the more than 11,000 smartcards.

The installation was controlled in accordance with the distribution plan drawn up by the DRV Bund. It was clear at all times which SINA device was to be installed for which person and who was to receive which device and when. The Samhammer rollout coordinator took over seemingly unimportant but time-consuming tasks such as making appointments with the home office users – which turned out to be approx. 1,000 – and the Samhammer on-site technicians. The technicians delivered the clients separately to the home office users, brought the devices online and demonstrated the basic functions to users. Finally, they took care of the removal of the old hardware.

In order to supply the 19 test offices distributed throughout Germany with SINA workstations for the approx. 2,000 company auditors, collective transports were organized and carried out by Samhammer. In the process, anti-theft wire mesh containers full of SINA devices were delivered. On site, the auditor then exchanged his old device for a new SINA Workstation S. At the same time, Samhammer organized and carried out the removal of the old hardware.

To complement the personal training sessions offered to users, secunet created 30-minute long SINA video tutorials especially for DRV Bund that clearly explained the most important features of the SINA Workstation S. Over and above the standard training sessions, a small group of specialist IT staff at DRV received a more comprehensive, five-day training course in the SINA training centre at secunet in Dresden.

#### You cannot plan for every contingency

In every mass roll-out there are uncertainties: do the actual technical conditions on site match expectations? Does the error rate for Windows installations fall within the usual range? Where discrepancies arise the project lead can take countermeasures, e.g. by modifying the processes. With the DRV roll-out, too, those in charge had to overcome various unexpected challenges. Nonetheless, by the scheduled date in December 2019 all affected users had been provided with a SINA Workstation S and connected to the infrastructure – exactly according to plan. Since then, users not only work with Windows 10, but also access the IT infrastructure of the DRV Bund on a very high security level, mobile and highly available.



Ulrich Hoffmann  
[ulrich.hoffmann@secunet.com](mailto:ulrich.hoffmann@secunet.com)

Professor Andreas Pinkwart, the State of North Rhine-Westphalia's Minister for Economic Affairs, Innovation, Digitalisation and Energy

# “We Need More Innovation Than Ever”

Measured in terms of gross domestic product, North Rhine-Westphalia (NRW) is Germany's economically strongest federal state. The IT security industry is one of the state's most promising industries and has an especially strong presence in the Rhine-Ruhr region. **secuview** spoke to North Rhine-Westphalia's Minister for Economic Affairs, Innovation, Digitalisation and Energy, Professor Andreas Pinkwart, about cyber security, digital administration and current challenges during the Covid-19 pandemic.

**Professor Pinkwart, though beneficial, digitalisation in the economy is also associated with risks. In your opinion, are companies – and SMEs, in particular – adequately protected against cyber threats?**

In my experience, many companies have already actively expanded their IT infrastructures and skills in recent years. This has not only entailed heavy investment in hardware, but has fortunately also driven investment in upskilling the workforce.

The SMEs in this country must now continue along this path. IT security has to be implemented in a professional manner. Only if a company's own data is well protected and handled responsibly do customers and business partners develop the trust needed for a close, long-term relationship. I am therefore always telling the representatives of all companies and industries that IT security is a top priority and investments in secure, digital business processes are an increasingly important factor in commercial success.

**One of your key concerns as Digital Minister is the digitalisation of administration. You have set yourself some very ambitious goals. How much have you already been able to achieve?**

We have brought forward full digitalisation from 2031 to 2025 and are getting universities and almost all state authorities involved. We are also investing an additional €600 million in making public administration simpler, faster, and more cohesive and transparent – and therefore more customer-friendly. With the amendment of the E-Government Act, we are introducing regulations for the NRW service portal as a platform for digital administrative services, and are therefore preparing the ground for the implementation of the Online Access Act (Onlinezugangsgesetz). This in turn means that we will also be offering a large





proportion of our administrative services electronically via online portals by the end of 2022.

The pilot municipalities Aachen, Gelsenkirchen, Paderborn, Soest and Wuppertal are currently setting up service-ready digital citizens' offices and will eventually make their solutions available to other cities and municipalities free of charge. The services offered will range from registration for full-time schools and nurseries to waste disposal and the levying of the dog tax. Last but not least, there are also a growing number of digital services for companies. The Trade Service Portal (Gewerbe-Service-Portal) is a national flagship project that is currently being expanded into a Business Service Portal (Wirtschafts-Service-Portal). Even today, founders in North Rhine-Westphalia can advertise, register or deregister their businesses – and pay for this – electronically and without media discontinuity.

**During the shutdown due to Covid-19, some public authorities had to set up and provide masses of home office workstations within a very short time. In your opinion, was adequate thought given to cyber security? After all, many government employees work with sensitive or even classified data.**

The corona crisis is posing a major challenge for information technology in state administration. We have successfully risen to this challenge together, but the corona crisis has naturally also shown us where we still have more to learn and where we could optimise our processes.

All in all, we can be proud of the fact that we have been able to significantly expand our infrastructures within a very short period of time, without compromising security or data protection – something which

is particularly important to me. Within two months, more than 14,000 workstations in ministries and state authorities were transformed into home office workstations.

In order to cope with this workload, we doubled the capacity of the central IT infrastructure for teleworking within just a few weeks. A similar development was also achieved with the video conference platforms operated by the state, for which we more than tripled capacity.

**Will the shutdown drive digitalisation by leaps and bounds, as is now often predicted?**

It is well known that every crisis brings opportunity. The coronavirus pandemic has given a boost to digitalisation in public administration. Thanks to the measures implemented in recent years to digitalise our administrative work, we in the Ministry of Economic Affairs and Digital Affairs were able to set up the Corona NRW Emergency Aid Program (Soforthilfeprogramm Corona NRW) in just a few weeks, even with a large number of employees working from home. Together with our dedicated colleagues in the district governments, we have therefore been able to quickly help more than 400,000 self-employed workers and SMEs without the headache of red tape. This would have been unthinkable a few years ago and encourages me to continue to promote a consistent digital transformation in business and wider society.

**The Rhine-Ruhr region is one of Germany and Europe's main IT security hubs. How do you intend to position the strength of this region in the future?**

The Rhine-Ruhr region is indeed one of the most important IT security hubs in Europe.

## eurobits Security Summit

Professor Andreas Pinkwart is set to take over the patronage of a week-long event organised by eurobits e.V., the European competence centre for IT security. The eurobits Security Summit explores various topics under the heading of IT security. Due to the current pandemic, the event, which was originally expected to take place in May, will now run from 30 November to 4 December 2020.

And I am delighted that I am not only talking about excellent science here; our entrepreneurial landscape is in outstanding shape.

Start-ups from North Rhine-Westphalia have particularly made a name for themselves in the field of IT security, and we want to continue supporting our state's brightest minds by getting their business ideas off the ground. In the time of corona, we need more innovation than ever. We want to continue funding research and development in the fields of IT, AI and digitalisation, thus enabling us to support innovative projects.

In addition to direct financial support, I am very keen to promote knowledge exchanges between science and business. This is not simply a matter of exchanging information within sectors but, most importantly, making the many SMEs in all sectors of our economy fit for the future when it comes to IT and cyber security. For this reason, we will be announcing a cyber security competence centre for businesses in North Rhine-Westphalia this year. Our goal is to strengthen businesses' IT security and create the best possible environment for innovation and ideas. The combination of outstanding research and innovative, highly specialised companies in the field of IT security will increasingly become one of our state's most important calling cards, both nationally and internationally.

## In interview:

**Professor Andreas Pinkwart** was born in Seelscheid, North Rhine-Westphalia, in 1960. After completing an apprenticeship in banking, he studied economics and business administration at the University of Münster and the University of Bonn, where he obtained his PhD in 1991. In 1994, he became a professor of economics and business administration at the North Rhine-Westphalian University of Applied Sciences for Public Administration in Düsseldorf. Later, in 1998, he moved to the University of Siegen to accept a professorship in business administration. During a sabbatical from 2002 to 2011, Professor Pinkwart was a member of the German Bundestag (2002–2005), as well as both Minister for Innovation, Science, Research and Technology and Deputy Prime Minister of the State of North Rhine-Westphalia (2005–2010). In 2011, Professor Pinkwart was appointed Dean of HHL Leipzig Graduate School of Management and has held the Stiftungsfonds Deutsche Bank Chair of Innovation Management and Entrepreneurship ever since. Finally, he became the State of North Rhine-Westphalia's Minister for Economic Affairs, Innovation, Digitalisation and Energy in 2017



**Professor Andreas Pinkwart**  
The State of North Rhine-Westphalia's Minister for Economic Affairs, Innovation, Digitalisation and Energy

IT security according to the BSI's requirements

# Fit for Information Security Management with IT-Grundschutz 2020


The German Federal Office for Information Security (BSI) revises its IT-Grundschutz Compendium every year to reflect current threats and IT products. This can create a great deal of work for the public authorities and companies that apply the IT-Grundschutz methodology for information security management, as they have to adapt their security measures accordingly and document this in their security concepts. **secunet compass, the solution for automated IT-Grundschutz compliance checking, now provides functions to facilitate this migration. In addition, users can monitor the progress of the migration and the security level of their IT infrastructure at all times thanks to clearly structured reports for IT security officers and senior management. The German Federal Police, which has relied on secunet compass since 2017, is now using these new functions with great success.**

With the BSI's IT-Grundschutz, public authorities and companies can effectively and verifiably increase their level of security in full compliance with ISO/IEC 27001. Part of the well-established methodology for information security management is to create security concepts for a variety of "information domains" and to continuously monitor their implementation. However, increasingly complex and fast-moving IT infrastructures are leading to higher costs for IT-Grundschutz, because a growing number of security concepts must be developed – and almost as soon as this task is complete, they have to be revised again. To keep its use of resources within reasonable limits, the German Federal Police has been using secunet compass to implement IT-Grundschutz largely automatically since 2017. The solution is also available to other public authorities and companies.

secunet compass enables the tool-supported establishment of information security in accordance with the specifications of IT-Grundschutz. The solution automatically checks technical components and creates complete IT security concepts according to the requirements of the BSI. Central to this are the so-called security modules, which relate to the requirements of the modules of the IT-Grundschutz Compendium for various IT assets, such as systems and applications. While these requirements are kept quite general in the IT-Grundschutz manual, the security modules put them into specific terms, based on best practices and hardening recommendations.

Where possible, requirements are mapped to detailed configuration settings of individual products, allowing them to be checked fully automatically by compliance software. The requirements that can't be tested technically are audited in a web application by questionnaires with multiple choice



 The German Federal Police has been relying on **secunet compass** since 2017.

answers. The questionnaires can be delegated to different groups and individuals via fine-grained role and rights management. The results of the implementation audit can then be documented in a security concept at the push of a button. **secunet compass** currently provides more than 90 security modules for various products and aspects, and this catalogue is being continually expanded in consultation with the customers.

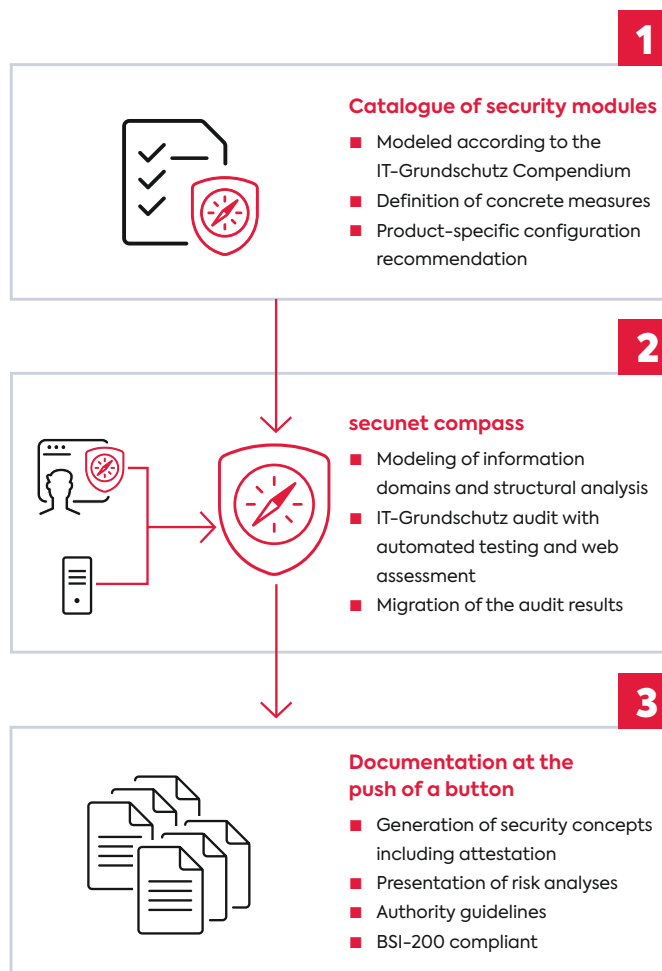
Since IT and the corresponding vulnerabilities are constantly evolving, the security measures implemented must be continuously updated to reflect new threats and products. The BSI therefore updates the modules contained in the IT-Grundschutz Compendium every year. In the current 2020 edition, a number of requirements have been changed, added or removed. The revised Compendium also contains two new modules. **secunet compass** has already reflected the changes made in edition 2020 in its security modules and is therefore fully up to date.

Nevertheless, for the institutions deploying IT-Grundschutz, the regular updates of requirements pose a challenge. Information on implemented security controls, which was previously collected at great expense, must either be collected from scratch for all assets or manually migrated to the new requirements. The resources required for this migration are then often lacking elsewhere, e.g. for implementing urgent measures or important projects.

In order to minimise the time and costs of migration, **secunet compass** offers a function for transferring existing audit results to the new security modules. For those requirements that have not changed, the results of the implementation audit are accepted automatically. For requirements that have changed, the previous and current audit questions and the results of the implementation audit are clearly

displayed side by side. The user can then decide whether or not to transfer the audit results for each requirement. After this step in the migration process, all that remains is to check the implementation of newly added or updated requirements, for which audit results have not yet been accepted. For technically verifiable requirements, this check can even be carried out fully automatically.

The functionality for migration of audit results minimizes the time and expense required to conduct an implementation audit. Nevertheless, it may be necessary to implement additional measures for new or updated requirements. **secunet compass** offers suitable functions for planning the implementation of such measures, including deadlines, responsibilities and costs.



The current implementation status and the corresponding security level achieved can not only be viewed in the IT security concept, but can also be seen at a glance in various reporting views for individual information domains. Coloured diagrams clearly show which proportions of the requirements have been implemented, have not been implemented, are not needed, or have not yet been audited. The reports compiled for the IT security officer show the level of implementation for each security module, as well as an implementation summary for each layer of the IT-Grundschutz model. The management report condenses the display even more and summarises the implementation status for requirements relating to systems and processes.

The reporting views enable the relevant employees to monitor the implementation status and to precisely identify the most pressing issues. This means that they always have an overview of their information networks' current security level and can better prioritise the remaining measures to be implemented.



Johannes Merkle  
[johannes.merkle@secunet.com](mailto:johannes.merkle@secunet.com)



**BUNDESPOLIZEI**

**“secunet compass is an essential tool for the German Federal Police to establish a uniform level of security. The security modules tighten the general requirements of the IT-Grundschutz Compendium and, therefore, support target group-oriented implementation within our decentralised organisation with its heterogeneous infrastructure. Thanks to the new visualisation tools in secunet compass, we can immediately identify the current implementation status of the security level and determine key metrics as a basis for further planning.”**

Thomas Schonhof, German Federal Police

For authentication via smartphone  
no additional token is required.



## Online Access Act

# ELSTER: Easy E-Government Login via Smartphone

The current economic stimulus package of the German Federal Government has now placed greater focus on the digitalisation of public administration. Therefore the Online Access Act (Onlinezugangsgesetz, OZG) is to be implemented more quickly. In order to make it easy for citizens and businesses to register for a variety of e-government offers, the tax ID will serve as an administrative identifier in the future. The online account of ELSTER, the German electronic tax return, is therefore gaining central importance for e-government. ELSTER also uses the technology of partner secunet to provide users with simple and secure two-factor authentication via smartphone.

The new authentication path is particularly easy for users, as they can utilise their smartphone as a token and do not need any additional hardware. The technology is based on secunet protect4use, a user-friendly authentication solution for web services which supports all relevant platforms and browsers. The solution flexibly covers a wide range of security requirements.

The Online Access Act (OZG) commits the German federal government, states and local authorities to provide all government administrative services digitally by 2022. The act also lays the foundations for the portal association (“Portalverbund”), which will link several federal and state e-government offerings. In case the ELSTER account can be utilised to log in to all online offers of the portal association in the future, then all ELSTER users will already have a digital identity which they can use for many e-government services. Furthermore, a nationwide uniform authentication process for companies and organisations is now being implemented which also uses secunet technology.

ELSTER is a project of the German tax authorities of all states and the federal government in order to process tax returns and tax registrations via the Internet. The Bavarian State Office for Taxes (Bayerisches Landesamt für Steuern, BayLfSt), Munich, is the nationwide coordinator of the project and operator of the “Mein ELSTER” portal. secunet has been contributing to secure online authentication for ELSTER since 1998.

More information regarding  
secunet protect4use:  
<https://protect4use.secunet.com/en/>



Christian Eisenried  
[christian.eisenried@secunet.com](mailto:christian.eisenried@secunet.com)

Automated border control

# secunet easygate – Now at a Land Border for the First Time


At the Hungarian-Serbian border crossing in Rösztke, four secunet easygates have been ensuring efficient control of bus passengers since April 2020. This installation, which secunet undertook together with its partner Adaptive Recognition Hungary (ARH), represents the first automated border control systems (eGates) at a bus terminal throughout the Schengen area.

The Rösztke border crossing is part of the external Schengen border. The new secunet easygates are used to relieve border control officials: Travellers entitled to freedom of movement use the eGates while officials monitor the process and can otherwise concentrate on passengers requiring further checks.

The secunet easygate optically and electronically checks the authenticity of electronic identity documents such as passports and personal IDs. In addition, the system reads the facial image from the chip in the electronic identity document and compares the biometric data with the passenger's actual appearance, which is captured using a facial imaging camera.

The new eGates in Rösztke complement 14 other secunet easygates that the Hungarian authorities have been operating since 2019 at the international airports in Budapest and Debrecen. In total, more



 At the Hungarian-Serbian border crossing in Rösztke, four secunet easygates are available to bus passengers.

than 350 secunet easygates are now used at international airports, such as in Germany, Austria, Czech Republic, Poland, Hungary, Lithuania, and Iceland. Travellers have already used these eGates around 100 million times.

secunet easygates are also part of preparations by border control authorities in Europe for the introduction of the European Entry/Exit System (EES), which will change the border control process from 2022 at the external boundaries of the Schengen area. With this system in place, biometric data will be collected directly at the border from all members of third states who wish to travel into the Schengen area. Automating elements of the border control process will help absorb border control officials' additional workload.

secunet border gears represents a complete border control product portfolio with components that can be implemented both quickly and flexibly. Elements can be individually integrated into existing infrastructures, or brought together to create a dovetailed, modular border control infrastructure that is already EES-ready.



Michael Schwaiger  
[michael.schwaiger@secunet.com](mailto:michael.schwaiger@secunet.com)

For more information on the European Entry/Exit System (EES), please visit the following website:  
<https://ees.secunet.com/en/>

Further information on Adaptive Recognition Hungary (ARH) can be found at <https://adaptiverecognition.com/>

## The new generation of the secunet easygate

# Always a Sleek Transit

**The secunet easygate is proving its worth at land and air borders in many countries around the world. Although the automated border control system has been continually updated over the years, its external appearance has changed very little.**

**It is now time for a new version, which is sure to impress thanks to a complete design overhaul. Further, innovations to the easygate's technology and security mechanisms are also incorporated.**

The secunet easygate eases the workload of border control officers, helps airports to achieve greater passenger throughput, and shortens waiting times for travellers. This means that it benefits everyone involved in the border control process – all without leading to weaker security. The system has already proven itself at major international airports, where it has facilitated around 100 million border crossings.

However, even the most technologically advanced product can be further optimised. The new secunet easygate therefore boasts a number of improvements. Alongside updated technology and a revised construction, secunet's developers have implemented feedback, suggestions and requests from



customers and users, particularly regarding the automated border control gate's design and security features.

### A modern high-tech design

The most eye-catching change is the design, which has been reworked from the ground up, making the secunet easygate lighter and more transparent. The previous stainless-steel components have been slimmed down and replaced with light, high-quality surfaces, while the more generous use of glass creates an inviting, open, modern impression. The result is a high-quality design that perfectly complements and enhances the aesthetics of the modern airport. The new design also offers security benefits, as it enables officers supervising the automated border control gates to better monitor the process from outside and follow what is happening inside the gate.

### Quality down to the last detail

A sophisticated construction and modular components make it quick and easy to integrate the secunet easygate into existing infrastructures. As a result, it adapts to its environment, not the other way around. Modifications can now be completed with ease, additional components can simply be retrofitted. The new easygate is therefore perfectly suited to fit tight schedules and infrastructures with limited space. The secunet easygate makes no compromises when it comes to materials, motors and controllers, as well as to good workmanship. The automated border control gate is designed to be high quality down to the last

detail for long, low-maintenance operation – making it a cost-effective solution for operators.

### Border security at the highest level

The secunet easygate has also had a security upgrade. The tried and tested technology has now been updated with a new generation of state-of-the-art security components, such as new sensors. The technology that detects so-called 'presentation attacks' – fraudulent attempts using face masks or similar items – has also been improved. The colour camera delivers high-quality facial images and has been further optimised to meet the requirements of the upcoming European Entry/Exit System. In short, innovations like these will ensure that the new secunet easygate can offer an unmatched level of security.



Michael Schwaiger  
[michael.schwaiger@secunet.com](mailto:michael.schwaiger@secunet.com)

Anyone interested in seeing – and trying out – the new secunet easygate is welcome to arrange an appointment at the secunet showroom in Essen, Germany. Please send us an email to: [info@secunet.com](mailto:info@secunet.com).

Further information on the product can be found at [www.secunet.com/en/easygate](http://www.secunet.com/en/easygate).



The new secunet easygate's design perfectly complements and enhances the aesthetics of the modern airport.





A traveller is using the secunet easykiosk at the border crossing point in Obrežje.

Pre-registration of travellers

# Process Accelerator at the Land Border

In preparation for the EU Entry/Exit System (EES), the Ministry of Interior's Information and Telecommunications Office in Slovenia conducted a 6 months pilot project for the use of self-service kiosks – secunet easykiosk – at land border crossings. The results show that kiosk systems speed up border control processes not only at airports, but also at land borders.

The objectives of the pilot were to evaluate the technical feasibility of self-service kiosks to fulfill EES requirements and to determine adequacy for the integration with police background systems. The work environment at land border crossings after the introduction of the EES was also taken into account, considering – among others – the available space and respective workflows.

In collaboration with the local partner and prime contractor Cifra (Cifra komunikacijski sistemi, d.o.o.),

secunet installed the self-service kiosk – secunet easykiosk – at the border crossing point (BCP) in Obrežje, between the Republic of Slovenia and the Republic of Croatia. As the largest land border in Slovenia, this BCP handled a total of 45 million travellers in 2018, whereby 20% were Third Country Nationals (TCN), i.e. people to whom the rights of free movement of the European Union do not apply.

In the pilot phase, the secunet easykiosk was used for the self-pre-registration of TCN-travellers crossing the border in buses. For the travellers, participation in the pilot project was voluntary. If they decided to participate, they were prompted at the self-service kiosk to enter their passport data by putting their passport onto the integrated passport scanner. They were also asked to capture their biometric data (face and fingerprints). Through the integrated camera with automated height adjustment and a feedback screen, the biometric acquisition process, that was still new for many of the land border passengers, was intuitive and easy to handle. Via touchscreen the passenger could easily follow the entire process visually and intuitively complete the process. During each process step, the required component of the kiosk to be used by the traveller was highlighted on screen and the expected interaction was depicted.

Once completed, the pre-registered data was checked against police information systems (National, SIS, VIS, Interpol database searches). After the pre-registration, the TCN proceeded to the manual border control booth, where the border control officer had access to the pre-registered information via a web-based border control application. Using a passport scanner, the officer read the data from the passport's machine-readable zone, and then re-retrieved the information from the kiosk. secunet biomiddle, the versatile biometric middleware, was used to manage the integrated hardware at the manual border control booth through the web application.

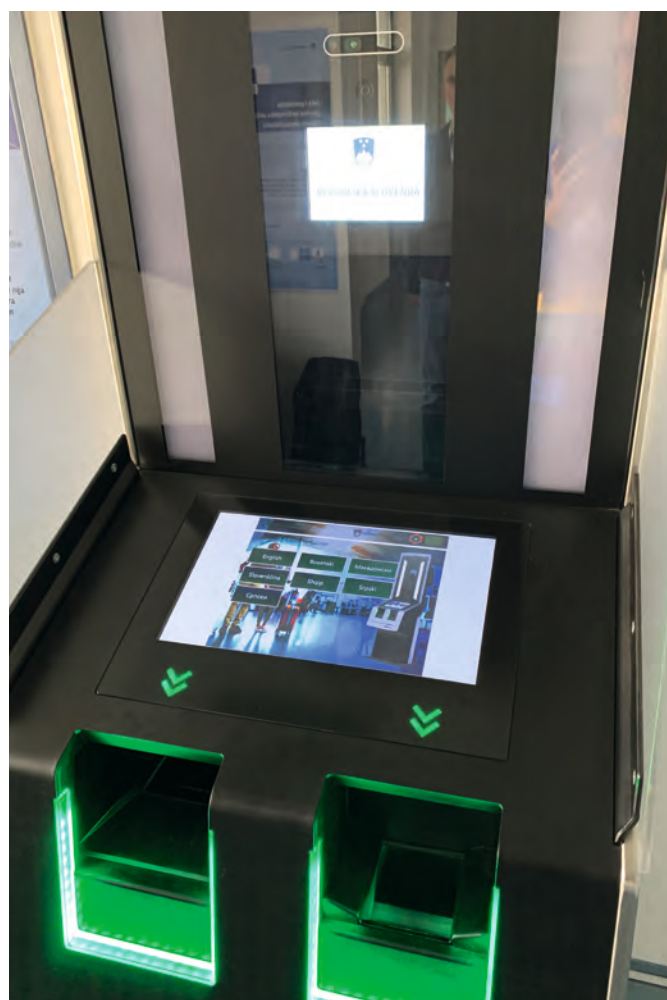
TCN-travellers from 26 nations voluntarily used the secunet easykiosk during the pilot phase. The kiosk's GUI was customised according to the specific project requirements by the customer. The duration of the different processes were logged and analysed for the pre-registration process – proving that kiosk systems are feasible and efficient to speed up the border control process at the land border. The document authentication and biometric acquisition at the self-service kiosk including other interaction by the user (i.e. reading instructions, locating buttons on touchscreen, physical handling of document) took 45 seconds on average.

Compared to existing pilot projects at airports using kiosks for the pre-registration of passengers in future EES scenarios, the pilot project at the land

border had similar results. Self-service kiosks – and automated systems in general – are process accelerators for all types of larger border crossing points and shorten the overall time for border control. While the processing times vary between frequent travellers and non-frequent travellers, secunet easykiosk – thanks to visual user guidance, intuitive processes and advanced technologies – allows for an efficient document check and biometrics acquisition in self-service mode.



Holger Funke  
holger.funke@secunet.com



The intuitive user guidance contributes to the fact that pre-registration at the kiosk takes only a short time.



Emotet in large companies and public authorities

# Dangerously Versatile

The Emotet malware has been circulating in the internet since 2014, causing millions of euros worth of damage. Emotet is a family of Trojans distinguished by a high degree of automation, modularity and a pronounced ability to adapt – essentially, intelligent malware. Control takes place via a command and control server; from there, Emotet can reload a variety of functional modules. The malware's preferred targets are large companies and public authorities. The good news: organisations can protect against this type of cyber attack.

A notorious danger in the Internet: attackers capture confidential information from users, such as usernames and passwords for corporate accounts or online banking. In this act of 'phishing', falsified emails are sent that appear to come from reputable senders and induce the recipient to enter their login data on websites that also falsely pretend to be legitimate. In this way the authors of the phishing emails can 'reel in' the valuable login data and use it for their own nefarious purposes.

Due to the increasing level of awareness on the part of companies and individuals, ever fewer recipients are falling victim to these poorly formulated, generic phishing emails. To keep with the fishing metaphor: the fishing net contains such large holes that only a small number of the catch remain caught.

#### **In the attacker's net: login data and passwords**

Attackers do not sleep, however: phishing has evolved into 'spear phishing', where phishing emails are not sent out en masse but are targeted at carefully selected recipients. The content is better researched and thus far more customised than conventional phishing, just as the name of the method suggests. For the most part, spear phishing emails concern a topic the recipient is actively engaged with, encouraging them to believe they have

received a legitimate email because, consciously or subconsciously, they are expecting an email on the subject in question.

Naturally, the spear phishing approach results in a greater proportion of recipients following the instructions in the fake email than would be the case with conventional phishing emails. It is also, however, more labour-intensive: before launching a successful attack, the attacker must gather extensive information about the target, either through social engineering or even infiltrating the company by means of an insider. Spear phishing was primarily used in the past where the target was so valuable that the high initial investment yielded good returns. It was often the case that attackers worked for government or state-affiliated organisations.

### The evolution of malware: from spear phishing to dynamite phishing

Emotet represents the next level of the phishing evolution: the careful personalisation that has to be done manually with spear phishing is now automated. To do this, Emotet uses the victim's address book and email contacts and can thereby reconstruct their network of contacts. In addition, the malware automatically exploits content from the victim's real email conversations. This puts Emotet in the position of being able to send phishing emails that fit almost perfectly into the context of existing working relationships and email conversations – which it does on a large scale. Emotet's approach is therefore described as 'dynamite phishing' since it can be deployed on a grand scale and leads to enormously high catch quotas of victims.

### Emotet: infection by means of macros

Initial infection by Emotet generally begins with a cleverly falsified, seemingly reputable email that includes an Office document attachment. When the user opens this document and, as prompted, activates the macros, the infection takes its course. Once Emotet has infiltrated its target it sets up a connection with its command and control server; this determines the malware's subsequent behaviour remotely, which can vary considerably depending on the instructions received.

One of Emotet's core functions is further dissemination by sending phishing emails from within the network of contacts, which it is able to identify from the device that is currently infected. Emotet uses the Windows MAPI (Messaging Application Programming Interface) function to read its victim's email contacts.

### Reloading modules, reproduction as a worm

Once Emotet has wormed its way into a workplace computer, it can reload further modules in the working memory without these being saved as files. This is therefore known as fileless malware, which makes identifying it difficult.

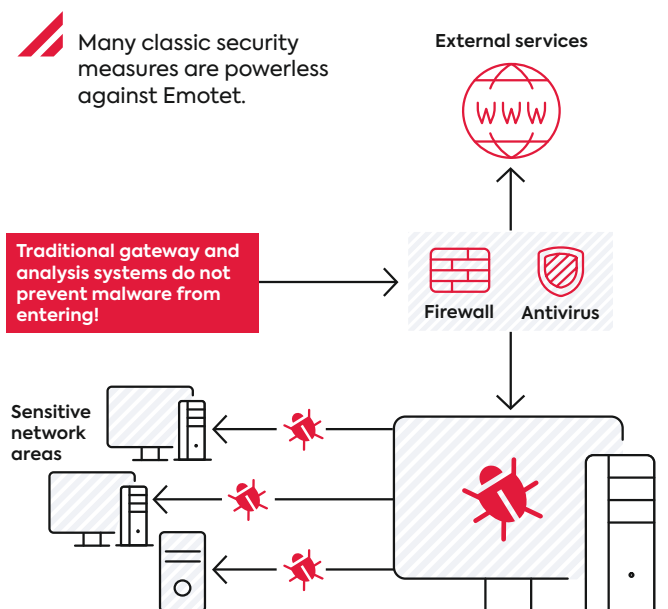
Emotet also functions as a worm and can spread from one infected computer to others in the same network, without their users having to actively become involved. To do this it utilises Microsoft's SMB protocol (Server Message Block), reads sign-in tokens from the local Windows storage and also carries out brute force attacks on user accounts using password lists.

At the highest escalation level of an Emotet infection the attackers also explore the infected system manually and identify and, for example, remove particularly important data for which they then issue demands for a sizeable ransom. Another blackmailing scam: captured sensitive information is encrypted locally and also copied by the attackers. If the victim doesn't pay, the extortionists publish the data on the internet.

In some circumstances, it can take months to identify that the system has become infected. There have been cases where Emotet and its modules have been present in the system for over six months and up to 18 months, changing data there unnoticed. The insidious thing is that, if the data are not destroyed, a backup is useless. This is because it is impossible to reconstruct which data have been altered and need to be restored from the backup.

### Prevention is critical

There is a range of measures, however, that promise success in the fight against this type of attack.



As with all phishing attacks, educating company employees is also of great importance in preventing Emotet infections. Coordinated measures such as internal emails and posters raise awareness. Specialised training sessions, e.g. on the topic of email security, provide employees with the necessary expertise. The much-discussed “human factor security risk” thus becomes the human security factor, which actively helps to defend against cyber attacks like Emotet.

In order to arm an IT infrastructure technically against Emotet, the first thing to do is to ascertain how secure it actually is. An information security quick audit offers an initial approximation of the situation. This is carried out by IT security experts and is based among other things on the “IT-Grundschutz” information security concept from the German Federal Office for Information Security (BSI). The experts draw up an audit report with a management summary and representation of the deficiencies identified as a basis for further measures.

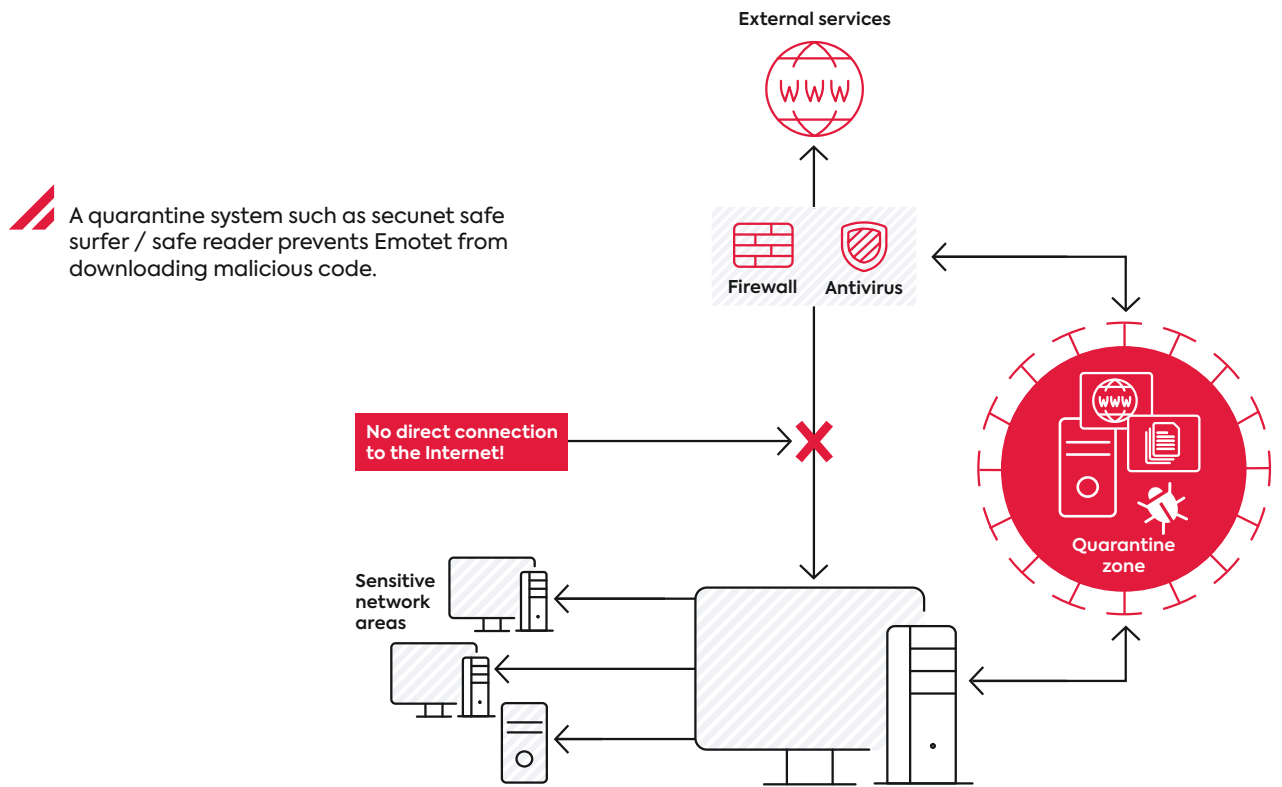
A penetration test supplies a practical starting point from a technical perspective. To do this, IT security experts simulate a malware outbreak so as to answer a series of questions: how effective are the protective measures implemented? Are there weaknesses that need to be shut down in the short term? Are there existing authorisations in the network that an attacker could exploit? As part of the test the experts also look for indications that an infection has already occurred but has not yet been identified.

To impede Emotet’s spread, it is generally advisable to check the authorisation management: users should only be granted the level of authorisation they require in order to carry out their responsibilities. In particular, there should be no admin-level access across the board.


**Identifying and combating Emotet**

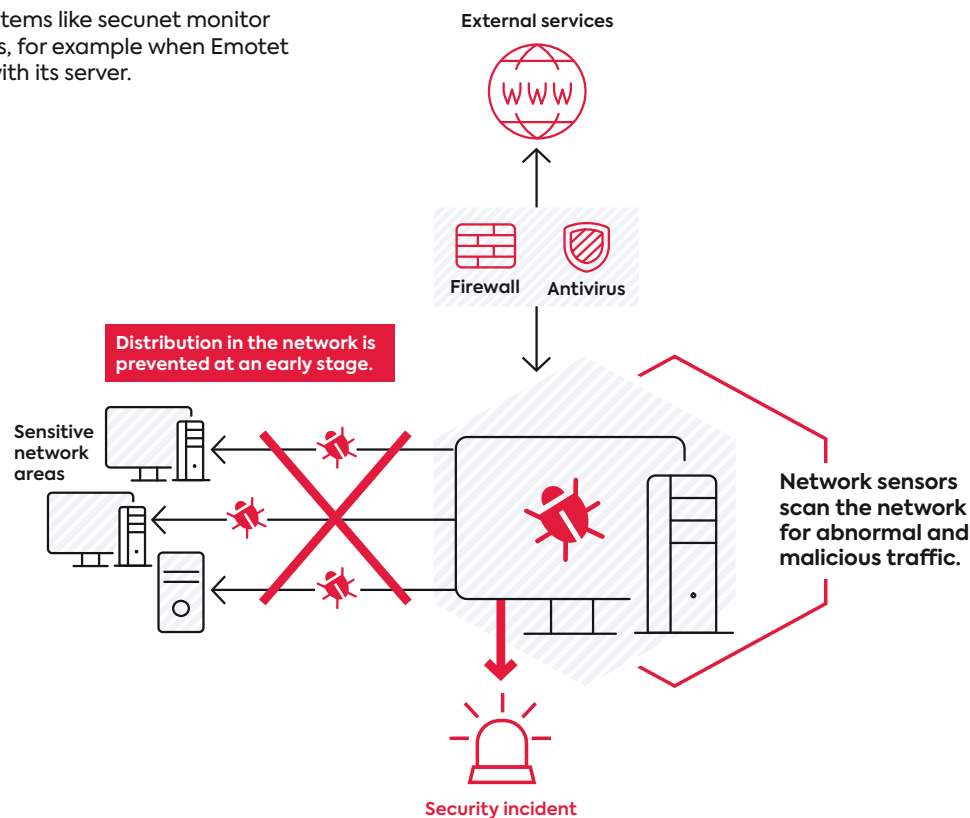
Traditional gateway and analysis systems such as firewalls and anti-virus software are powerless against Emotet attacks. Instead, there is demand for measures that go deeper – like the secunet safe surfer quarantine system. This prevents Emotet from gaining access to the computer and, from there, the network, as a result of a thoughtless click on an infected link. With secunet safe surfer the compromised website is not opened in the user’s normal work environment, but in a sealed-off browser on a quarantine system, which the user controls ‘remotely’. Emotet cannot cause any damage since the malware cannot leave the quarantine system. Using the additional safe reader function the infected email attachment can be blocked effectively. If the user opens a compromised attachment with safe reader Emotet cannot reload any malicious code, since there is no direct connection to the internet.

Moreover, operators of an IT infrastructure should always be up-to-date with what is happening in their network and whether there are suggestions of a malware infection. Early warning systems continually assess communication in the network with respect to anomalies, such as suspicious data streams.



**A quarantine system such as secunet safe surfer / safe reader prevents Emotet from downloading malicious code.**

 Early warning systems like secunet monitor detect anomalies, for example when Emotet communicates with its server.



For instance, it becomes evident if Emotet communicates with its command and control server or reloads malware. Once the infection is recognised, its further spread within the network can be prevented.

Public authorities and companies that use the SINA Secure Inter-Network Architecture in order to handle sensitive or even classified data digitally are at a further advantage with respect to Emotet. The SINA Workstation, which functions as a client within the system, uses a virtualisation technology to construct numerous guest systems that are strictly sealed off from one another. These guest systems can be operated simultaneously, even if they are located on differing security levels. Users can then, for example, work with classified data and also surf the internet. Malware is incapable of surmounting the barriers between the guest systems, rendering its attempts to access the network futile.

The security of SINA is also based on a plethora of other interlocking security measures: SINA networks are built from IPsec-secured VPN connections and, depending on requirements, offer strong to very strong encryption. The SINA Workstation interfaces are controlled to prevent malware from infiltrating the system via this route. Furthermore, hard disk

encryption and two-factor authentication ensure that company or authority data does not end up in the wrong hands.

#### Compiling protective measures

The evolution of types of attacks has fortunately gone hand in hand with the evolution of IT security measures. Public authorities and companies are therefore not left defenceless against Emotet. Measures that promise success in the fight against this type of attack generally engage at a deeper level. As always, it is important to put together appropriate measures in view of the existing circumstances and the respective network's protection requirements.



Christian Eisenried  
christian.eisenried@secunet.com

## Network analysis for critical infrastructures

# Knowing What is Happening in Your Network

Operators of critical infrastructures (CRITIS) are legally obligated to report IT security incidents to the authorities. However, in order to do so, they must first be able to detect such incidents. This is not easy, as in many cases there are few noticeable changes at first. IT security monitoring solves this problem – while also helping to significantly increase network security.

In accordance with the German IT Security Act, industry-specific security standards and the IT security catalogues of the German Federal Network Agency, CRITIS operators must set up and operate an information security management system (ISMS). They are also required to report IT security incidents to the competent supervisory authorities, such as the German Federal Office for Information Security (BSI).

However, an IT security incident must first be detected and identified. If there are no noticeable or visible changes and no damage has been caused, this is often hard to do. IT/OT security managers and administrators therefore have to actively seek them out. Even if there is a noticeable or visible effect, it is often not possible to reconstruct how the incident occurred and how it has developed.

The IT Security Act requires operators to take appropriate measures taking into account the “state of the art”. This includes being able to assess the cyber security situation in IT and OT networks. Such measures are also important for companies’ internal reporting on the overall security situation, since the IT security officer or CISO’s report to the management should not only include (IT) risk management evaluations, but also data collected from the company’s operational divisions. For this purpose, it can be useful to evaluate key performance indicators (KPIs) derived from observations of the IT and OT networks, for instance.

Technical IT/OT security monitoring creates transparency, making it easier to compile a situation report and quickly view, evaluate, contain or directly prevent potential security incidents. It also facilitates evaluation by the management and the competent public authorities. Companies are thus



able to develop and implement short, medium and long-term strategies and measures in a much more targeted manner.

In order to be able to best exploit the advantages of IT security monitoring in an efficient manner, organisations need a security situation reporting tool. secunet has therefore developed the secunet monitor solution, which consists of the previous Advanced Security Analytics Platform (ASAP), new functions like asset recognition and management, and a selection of third-party tools. The result is a modular solution for network analysis, detection, compliance and prevention.

**“IT security monitoring without a security situation reporting tool is like network management without a control system.”**

Steffen Heyde, Industry Division,  
secunet Security Networks AG

### Network analysis

Due to the progressive integration of OT networks into IT, IT managers now face the challenge that, in addition to IT, they also have to understand and manage OT. secunet monitor offers the possibility of achieving transparency in OT with the existing knowledge of IT managers – requiring limited additional effort and using tools already familiar to them.

secunet monitor enables an automated, real-time analysis of common protocols from the IT and OT world. By contrast, specialised OT security monitoring solutions are often only able to understand OT protocols, meaning they are unable to cope with the known threats from IT that are increasingly spilling over into OT today. By default, secunet monitor's network analysis is performed passively and does not influence production networks. Consequently, the functionality of the respective plants remains unaffected. In addition, all communicating components (assets) are detected, identified and inventoried. The software thus also makes a significant contribution to asset management within the scope of information security management.



**Behavioural analysis (detection)**

secunet monitor detects behavioural abnormalities (anomalies) and recognises evidence of targeted attacks (advanced persistent threats or APTs) in the network. Once attacks and anomalies are visible, they can often be dealt with. Companies can therefore react quickly, reduce damage, and prevent further spread or an escalation to an emergency or crisis situation.

**Vulnerability analysis (compliance)**

Many systems and protocols have vulnerabilities. It is especially problematic that operators often do not know where these compromised systems and protocols are being used. secunet monitor automatically detects vulnerabilities, such as the use of older SMB protocols or weak encryption algorithms, and generates a report so that they can be addressed.

The solution also identifies and analyses unknown communication links.

This information can be incorporated into an automatically generated management report setting out the current security situation for the management and those responsible for IT/OT.

**IDS/IPS (prevention)**

In combination with the Industry 4.0 security solution secunet edge, secunet monitor boasts an intrusion detection and prevention system (IDS/IPS). This function prevents the spread of attacks and ensures network functionality.

All in all, secunet monitor provides a comprehensive overview of IT and OT networks. Users can detect events that could develop into IT or OT security

# One solution, many insights

**Expert system/analysis**

Based on intelligent analytical functions, the system facilitates the evaluation of data collected in the network.

**Situation report evaluation**

Within the scope of its reports, the system enables the aggregation and evaluation of events and security incidents. These evaluations are based on pre-defined criteria such as the frequency and criticality of a security incident. This data can then be further processed for the full report and provides the CISO and other managers with important grounds for decision-making.

**Real-time monitoring**

The system offers a real-time display of network traffic, thus permitting the evaluation of current network processes.

**Service monitoring**

An additional module offers service monitoring functionalities. This allows problems and bottlenecks in the IT infrastructure to be identified and the detected components to be displayed in the existing topology. Network data logging can be used for forensic analyses, for example.

**Advanced threat detection**

Different processes in the network can be aggregated for a convenient overview, allowing users to evaluate the data with regard to complex attack scenarios such as advanced persistent threats. This involves a special type of sensor which usually monitors the interfaces between network segments with different security classifications (IT-OT or IT-Internet).

incidents at an early stage, allowing them to react quickly and prevent similar incidents. The system prepares data in such a way that it can be immediately forwarded to the management and can be used in the scope of governance, risk management and compliance processes. This facilitates quicker, more accurate decision-making and the approval and evaluation of measures – all with the aim of ensuring business continuity.



Steffen Heyde  
[steffen.heyde@secunet.com](mailto:steffen.heyde@secunet.com)

## secunet monitor in the energy supply sector

A distribution network operator installed secunet monitor in several locations in its control centre network. While operating the solution, they noticed that only about 40% of their assets were recorded in the asset inventory. In addition, secunet monitor detected legacy systems using protocols with known vulnerabilities or outdated software versions. After the analysis, these systems were migrated to current versions and hardened. Remote maintenance interfaces that had not previously been included in asset management could then be identified and integrated into the centrally administered solution. The interfaces to office communications were also monitored and analysed. The result was a complete overview of the interfaces between IT and OT networks. The data collected by the system is regularly aggregated and reported to the management.

## secunet monitor at EGLV (Emschergenossenschaft und Lippeverband)

EGLV, one of the largest water management companies in Germany, uses secunet monitor as a service. Its aim is to better protect its own infrastructure and implement the requirements of the German IT Security Act for CRITIS operators.

IT and OT-supported business processes are standard fare at EGLV, meaning that the smooth, uninterrupted operation of its IT infrastructure is a more important factor than ever in its success. In addition, attacks on critical infrastructures have become more professional and varied. Cyber attacks can potentially endanger a population's water supply, as well as reveal trade secrets. Appropriate investments in IT and OT security are therefore a vital prerequisite for maintaining the supply service. secunet provided EGLV with a solution which, with its innovative approach to protecting modern IT and OT systems, is both trusted and flexible enough to meet any future requirements.

EGLV's goal was, in view of its compliance requirements, to be able to identify and control its processes and activities in connection with information security risks more comprehensively and sustainably. The system generates a security situation report that records the current security level of the IT infrastructure and certain IT-connected systems at the two main stations in Essen and Bottrop, and also provides corresponding recommendations.

The solution provides EGLV with an overview of all processes taking place in the network, and can identify and analyse attacks and reduce risks. secunet monitor as a service has thus become a crucial extension of EGLV's IT security infrastructure.

## Edge computing in the Industry 4.0

# Digitalised, Networked – and Secure

In many industrial companies, digitalised and networked production linked to current technologies is still in the process of being established. However, a mixed operation of old and new and the hasty introduction of new technologies also create risks that need to be addressed.


Even in the tenth year after Stuxnet, the threat of cyber attacks to industrial companies continues to increase – as can be seen in various destructive ransomware infections. At the same time, current efforts such as the planned German IT Security Act 2.0 with its concept of “secure core components” show that the urgent need for reliable and truly secure solutions is increasingly being recognized by regulators. For operators, the need for action is thus increasing – not only as a result of external pressure, but also because they are more and more realizing how much cyber security is also in their own interests.

So where is a good starting point for a secure overall solution? A central concept in the digitalisation of industrial plants is edge computing. Here, data is not processed at the central nodes, but at the edges of the networks, and in some cases is also stored there. A major advantage is that by shifting data processing to the periphery, bandwidths and resources, which are often limited, are relieved and reaction times are accelerated. This is particularly relevant in the industrial environment and in Operational Technology (OT).

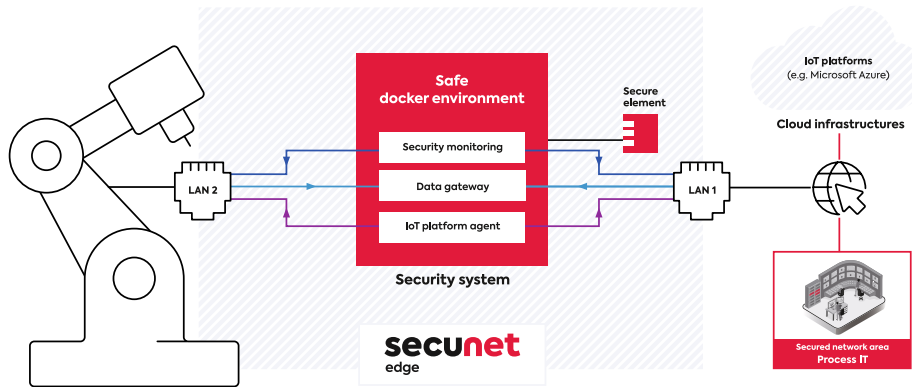
Edge computing is also essential if already existing structures are to be digitalised retrospectively. This is called a “brownfield” with dated legacy systems, as opposed to a fresh “greenfield” that can be built from scratch. Another field of application is the individual retrofitting of individual systems with more computing power and more up-to-date interfaces. Edge computing is thus an integral part of digitalisation – as application- or machine-oriented data processing, as part of Industry 4.0 or in the Industrial Internet of Things (IIoT).

### Potential and risk

Digitalised and networked plants, machines, actuators and sensors using edge computing thus create great potential for more added value, profitability and new business models. In addition, they ensure that even long-established organisations keep pace

 In industrial plants there is often a mix of old and new technologies.





with technological developments. At the same time, however, attack vectors for malware and targeted cyber attacks are also emerging – the risk of operational disruptions or even production downtimes that threaten the company’s existence is increasing. The new digital functionality and connectivity must therefore be secured with comprehensive protection against digital threats.

secunet edge addresses this challenge as a cost-efficient, convenient and ultra-secure holistic solution consisting of an edge computing platform and applications. The platform comprises a software and a hardware part. The software consists of a hardened operating system with a secure application environment. The hardware is based on industrial PCs (IPCs) and the security components built into them. secunet offers software and hardware as a combined appliance.

Due to the platform concept, several applications can be operated on one appliance. In addition, there is the possibility of central administration of several apps and appliances. Together with an industry-compatible life cycle of at least ten years, this results in high cost efficiency.

**Sophisticated security**

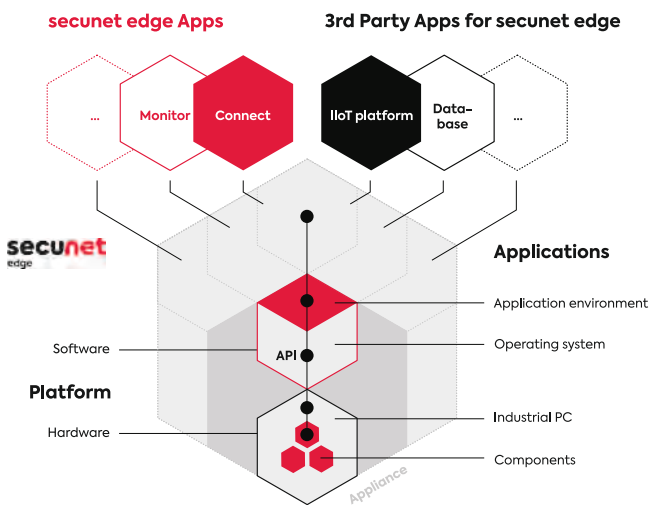
The application interface (API) concept extends from the individual components – in particular the patented CryptoCore SSD with built-in embedded secure element (eSE) – right through to the application level. This is one of the great strengths of the holistic solution designed and continuously developed by secunet: complex security features such as the creation and administration of cryptographic keys are already available as functions that can be used easily and conveniently.

secunet edge has been in use in the financial sector for more than ten years and was developed as a ultra-secure holistic solution based on the principles of Security by Design and Security by Default. Wherever possible and reasonable, this is also proven by corresponding certifications (e.g. the Secure Element certified according to FIPS 140-2 L3 or BSI CC L3 EAL5).

**Ecosystem of applications**

If secunet edge is used as a platform for applications, this enables several solutions via a reliable and long-lasting infrastructure. The Connect application for secunet edge, for example, translates obsolete and insecure protocols into current and secure variants, including SMBv1, which is exploited by various encryption Trojans, to SMBv3. The Remote application enables secure and convenient remote maintenance. The Monitor application monitors network traffic for vulnerabilities, attacks and anomalies. In addition to secunet’s own applications, an ecosystem of third-party apps, integrations (such as with Microsoft Azure IoT Edge and the IIoT platform PTC Thingworx) and customer-specific solutions is being created around secunet edge.

Machines and plants must be protected from harmful external influences and at the same time open up for increased connectivity. secunet edge fulfils this seemingly contradictory requirement. Thus, the solution has great potential for Industry 4.0, which continues to develop rapidly.



 [Aurora Monfil Herrera](mailto:aurora.monfil@secunet.com)  
aurora.monfil@secunet.com

Collaborative work with documents up to  
SECRET level classification

## Secure CI Distribution – with a Few Clicks

Digital working brings a large number of advantages: sending content quickly, making decisions rapidly, straightforward collaboration and – very relevant these days – working in a contact-free way. Previously, these advantages applied primarily to normal, non-classified information. Anyone who wanted to work digitally with sensitive data that required high-level security protection, or even with classified information (CI), had to seek out specially designed solutions which often did not have any approval and mostly still required paper-based documentation at some point in the workflow. It was SINA Workflow, the CI document management solution that secunet developed together with the German Federal Office for Information Security (BSI), that changed this. Authorities can now deploy SINA Workflow for CI in general up to the German GEHEIM (SECRET) classification level. Individual approvals are no longer required. Authorities in other countries can benefit from the solution as well.

In Germany, SINA Workflow allows implementing the German Classified Information Directive (Verschlusssachenanweisung, VSA). Information can be seamlessly processed, transferred and stored – at a suitably high and demonstrable security level, and without any media discontinuity. In June 2020, the solution received a release recommendation (“Freigabeempfehlung”) up to classification level GEHEIM (SECRET) from the BSI (BSI-VSA-10158). Customers can now deploy SINA Workflow without having to obtain individual approvals as they did previously.

Where SINA Workflow is implemented on the basis of SINA Workstations and taking the respective operating conditions (SecOps) into account, the solution protects CI and other highly sensitive data from creation to finalising. SINA Workflow supports users in, for example, developing content collaboratively, implementing internal decision-making processes with multiple sign-offs, as well as distributing content securely in line with the “need to know” principle. All features and workflows offered by the solution are VSA-compliant, cryptographically secured and embedded in a comprehensive verification function – including a CI inventory as the VSA stipulates.

In conjunction with SINA Workstations, SINA Workflow also enables contactless working with CI. This allows classified documents to be transmitted without necessitating access to (physical) registries or commissioning couriers. The security classification of the overall solution depends on the respective SINA Workstation model chosen. SINA S Workstations are authorised up to VS-NfD/RESTRICTED levels; SINA E Workstations up to VS-VERTRAULICH/CONFIDENTIAL levels; and SINA H Workstations up to GEHEIM/SECRET levels.

**Secure transfer to external parties as well**

With the help of a “point of presence” model SINA Workflow can also enable the digital exchange of classified data across organisations, as well as facilitate collaborative working on content that crosses organisational boundaries. An organisation can thus send a copy of finalised classified documents to another organisation – entirely digitally, with verification procedures and adequate protection.

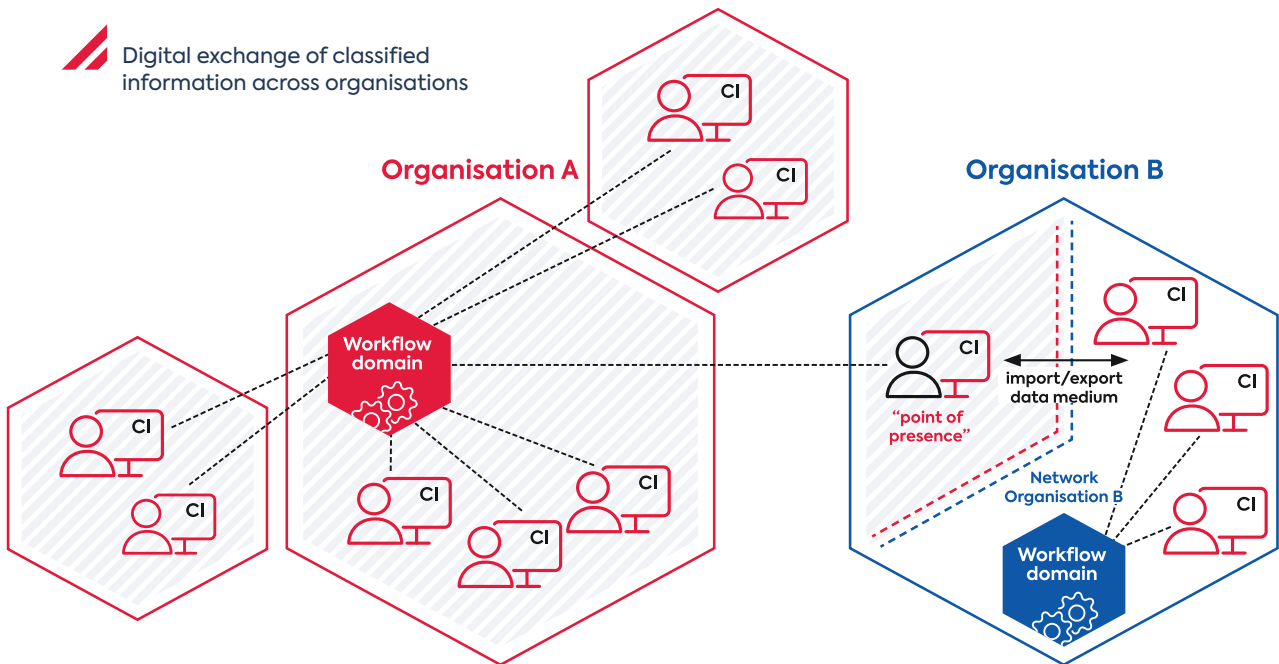
In the “point of presence” model, a SINA Workstation with SINA Workflow that is part of organisation A’s domain (i.e. the SINA infrastructure and SINA Workflow registry) can be positioned within organisation B. Employees from organisation B operate this SINA Workflow workstation. Where classified information from organisation A has been finalised and needs to

be sent to organisation B, an authorised employee from A can offer a SINA Workflow user from organisation B (who in this case is managed as a user of organisation A’s domain) to take note of this information. Where the user from organisation B accepts this, the document is transmitted securely to the SINA Workstation in organisation B and can be read and, where necessary, worked on there.

In addition, the user from B also has the option to export the CI digitally and therefore to reuse it on other systems within organisation B. The verification procedure for SINA Workflow at organisation A shows when the employee at B took note of the information and whether – and, if so, when – a digital copy was generated for use outside of the SINA Workflow domain A.

As a whole, SINA Workflow makes the digital processing of CI in German administration far simpler, and the process of handling such information is speeded up considerably. Authorities in other countries can benefit from the solution as well: right from the start, SINA Workflow was developed with the goal of being an international product.

 [Stefan Reuter](mailto:stefan.reuter@secunet.com)  
stefan.reuter@secunet.com





The topic of mobile office became urgent at short notice due to the Covid 19 pandemic.

Home office with SINA

# Mobile Working – without Compromising Security

In spring 2020, at the beginning of the corona pandemic, many public authorities had to provide their employees with mobile workplaces quickly and comprehensively. In order not to jeopardise security, many of them opted for the SINA Workstation S. Migrating existing systems to the secure SINA environment is easy.

When it comes to mobile office, public authorities are faced with a dilemma: From an information security perspective, a large number of measures need to be implemented – which is contrary to a quick and easy project implementation. This challenge is intensified for those organisations whose employees regularly handle information that requires a high level of protection or is even classified. In March 2020, the German Federal Office for Information Security (BSI) published a collection of tips for secure mobile working on its website<sup>1</sup>.

In order to implement the necessary security requirements, a large number of components are usually needed, each of which must be administered individually. If this causes too much effort, but reducing security is not an option, authorities can fall back on a proven solution: the SINA Workstation S. It is part of the SINA crypto system which secunet developed on behalf of the BSI. For years, SINA Workstation S has been the standard workstation in numerous federal

<sup>1</sup> Please follow this URL (German language only): [https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen\\_mobiles\\_Arbeiten\\_180320.html](https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen_mobiles_Arbeiten_180320.html)



and state authorities, including several German federal ministries. Thanks to its mobility and flexibility, it has revolutionised working in public authorities. To date, more than 100,000 units have already been delivered.

The solution allows existing systems to be easily migrated into the secure SINA environment. Users can then continue to work without restrictions in their familiar environment, for example in MS Windows, and access the public authority network securely. Thanks to a large number of interlinked security measures such as IPsec-secured VPN connection, hard disk encryption, two-factor authentication and interface control, sensitive data is protected at a high level at all times – regardless of whether the employees are in the office, at home or on the road. The SINA Workstation S can also replace the desktop telephone by enabling secure telephone calls via Voice over IP (VoIP). Automated tools are available for fast rollout and easier administration.

The SINA Workstation S is available in various form factors – desktops, laptops, tablets – all of which are approved for handling information classified RESTRICTED. Depending on requirements, a slim terminal server solution (thin client) is also available as an alternative to the fat client with a full PC workstation. Even slimmer is the purely software-based solution secunet Terminal powered by SINA, which can be installed on any standard Windows PC and enables secure access to terminal servers. What all variants have in common is that the user can work at home or on the road as if he were sitting at his usual office desk – and that without jeopardising information security.



Christian Eisenried  
[christian.eisenried@secunet.com](mailto:christian.eisenried@secunet.com)

## Revival of the thin client

# Less is More

**Thin clients are in high demand once again in developing IT infrastructures. A setup with thin clients and powerful servers can also be a sensible choice for public authorities or companies that work with sensitive data or classified information.**

**The SINA portfolio includes optimised hardware components that enable solutions using thin clients or slimmed-down fat clients – while maintaining the usual high level of security.**

The IT world is also subject to changing fashions. Thin clients – computers reduced to the bare essentials and which are primarily intended to display server content – see their popularity wax and wane over time. Over the last few years, the preference has been for the opposite: the fully equipped fat client. However, the pendulum has now begun to swing the other way. Both options have pros and cons from a business point of view. Thin clients can help organisations to implement IT wish lists more cheaply through the use of slimmed-down hardware, for instance. On the other hand, they require a permanent broadband internet connection and compatible terminal software. It is important here to find the solution that offers the optimum cost-benefit ratio for the application scenario at hand.

One factor that is currently driving thin client infrastructures is the coronavirus pandemic; when public authorities or companies have to provide home office workstations for all employees at short notice, their budget is usually limited. Thin clients can be an ideal solution.

Many public authorities use the Secure Inter-Network Architecture (SINA) to safeguard their especially sensitive networks and data. The SINA Workstation, which acts as a client in these installations, is available in different versions. It is classically operated as a fat client. It can then execute various locally installed guest systems that run in different security domains. One guest system may be designed for the open, potentially dangerous internet, for example, while another may be designed to handle classified information. Since the guest systems are strictly separated from each other, the user can work in several of them in parallel without compromising sensitive data.

However, the SINA Workstation can also be used as a thin client. The Nano Desktop, a new addition to the SINA portfolio, is the ideal hardware for this purpose. Boasting a footprint barely larger than that of a smartphone, it saves on space as well as costs.

As a SINA Terminal S, it offers more than enough power for secure thin client applications. Another option is a slimmed-down fat client. This is ideal if a fully-fledged office PC is required, but a single guest system is sufficient, for instance. The Nano Desktop also cuts a fine figure in this so-called single-session configuration. Even a fat client configuration with multi-session capability – i.e. the ability to run several guest systems in parallel – is available.

Packed with a range of additional functions, SINA clients ensure that there is no need to fear weaker security in the mobile office. In all operating modes – including in the thin client version – they enable secure telephony, thanks to the SINA VoIP Session, designed to effectively encrypt calls. More extensive collaborative functions are available in higher configuration levels.

SINA supports a wide range of application scenarios. Different hardware configurations are available depending on the customer's requirements. secunet creates tailor-made concepts for all interested parties.

 [Armin Wappenschmidt](mailto:armin.wappenschmidt@secunet.com)  
[armin.wappenschmidt@secunet.com](mailto:armin.wappenschmidt@secunet.com)

Nano Desktop



Smartphone



Telematics infrastructure in the German healthcare system

# secunet konnektor “eHealth” Approved and Available Now

The secunet konnektor in its “eHealth” software version has successfully reached the end of the multi-stage approval process. The new version was approved by gematik for active operation in the German telematics infrastructure (TI) on 17 August 2020. Medical service providers who already use the secunet konnektor will receive the new version via an online upgrade.

Healthcare connectors in the “eHealth” version offer a range of new medical applications. This includes emergency data management (Notfalldatenmanagement, NFDm) and electronic medication planning (elektronischer Medikationsplan, eMP). The new version also contains all the necessary functions (QES) to enable use of the specialist service “communication in the medical sector” (Kommunikation im Medizinwesen, KIM). These applications provide real medical added value and also facilitate workflows in practices and between medical facilities.

The secunet konnektor “eHealth” has already proven itself in combination with the new applications: Part of the approval process was designed as a field test, in which participating service providers and their patients were able to successfully use the new applications in the production environment.

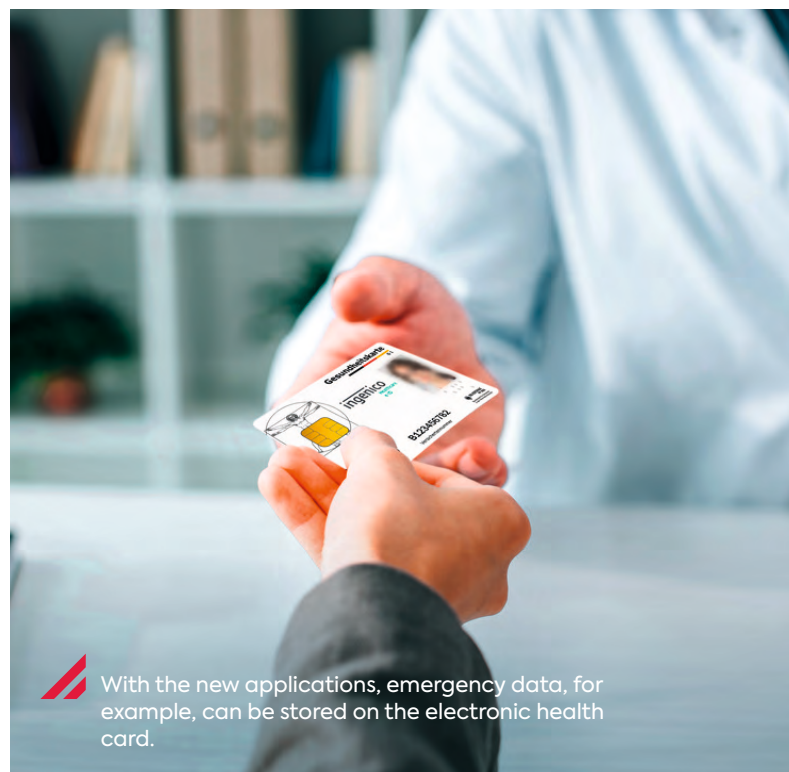
All secunet konnektors already in use are ready to be upgraded to the “eHealth” version. Users can now install the online upgrade and activate the NFDm and eMP modules with a licence. Service providers are granted access to the licences via their TI service provider. This applies to both the secunet konnektor for medical practices (one box connector) and the secunet konnektor for data centres (data centre connector), which is particularly suited to hospitals and large pharmacies. The deadline for pharmacies to connect to the TI is 30 September 2020.

The secunet konnektor has been used by service providers to connect to TI since the end of 2018. Its two designs were developed in conjunction with eHealth Experts GmbH. The secunet konnektor aims not only

to meet the technical requirements but also the customers’ needs for usability and user-friendliness. secunet anticipates over 70,000 konnektor installations by the end of 2020.



Markus Linnemann  
markus.linnemann@secunet.com



With the new applications, emergency data, for example, can be stored on the electronic health card.

## New German eHealth applications

# “An Emergency Dataset is Quick to Create and Incredibly Useful in Action”

In summer 2020 a field test of two important applications for the German telematics infrastructure was carried out in the Westphalia-Lippe region. Around 70 medical practices, an emergency care practice, several pharmacies and a hospital put the emergency data management (NFDM) and the electronic medication plan (eMP) to the test.

Dr. Thorsten Klüsener, a senior emergency doctor in the Steinfurt district and a specialist in internal and general medicine as well as anaesthesiology, was among the participants.

The general practice group in Altenberge, Münsterland, where Dr. Klüsener has worked since 2006, and its subsidiaries in Billerbeck were switched to paperless systems by the self-confessed tech geek and his colleagues many years ago. For almost two years the practice, which uses the InterARZT practice management system (PVS) supplied by InterData Praxiscomputer GmbH, has been connected to the telematics infrastructure (TI) through the DGN equipment package. In the field test, the secunet konnektor which is part of this package was tested with the 'eHealth' software version prior to its mass rollout.

“As an emergency doctor I'm naturally very interested in recording important, lifesaving emergency data on the electronic health card,” says Dr. Klüsener. In his opinion, the chip on the card should have been used for this much earlier instead of solely for the insured person's master data. Because of this, when the NFDM was developed – initially in paper form – back in 2016, he actively got involved in the design of its medical content and its testing.

### Avoiding incorrect treatment and wasting time

Especially in the case of unconscious patients, the emergency data on their electronic health card (eGK) help to ensure that they receive the best possible care and treatment – fast. “When I can see at a glance which chronic diagnoses and allergies are present, I can avoid treating the patient incorrectly out of ignorance,” explains the experienced emergency doctor. “Where the data also include the details of the relatives who are to be informed in an emergency, the patient's GP, or the presence of an advance directive, I do not have to go hunting for the relevant documents and can therefore save important time.”

The emergency dataset is informed by the patient's file stored in the PVS. "Where this has been well-maintained for long-term patients with personal data, up-to-date diagnoses and prescribed medications, the emergency data set is applied in just one to two minutes," Dr. Klüsener states. For new patients he has to invest a little more time in requesting the relevant information.

#### Functioning workflow

The medication plan can also be created in one step without significant additional effort. "After a few initial difficulties the entire workflow is now working perfectly," adds Dr. Klüsener, satisfied. "The field test gives me the opportunity to find out whether what we had imagined in theory also actually works in practice." The seamless interaction between the connector and the PVS is important. The close coordination with InterData, the company responsible for the technical support, meant that error messages and issues could be swiftly remedied and processes optimised.

There is still one more hurdle to overcome, however: to write the emergency data and medication plan to the patient's eGK, Dr. Klüsener must authenticate his identity on the card reader by using his electronic health professional identity card and entering his PIN. The patient also needs to enter their eGK PIN as a sign of consent – and this is exactly the nub of the problem: many patients have no idea what their PIN is and even spontaneously asking at the health insurer often leads nowhere. In principle, however, any patient can request a new PIN from their health insurance fund.

#### Positive reaction from patients

Especially at the beginning, the field test was made more difficult by the coronavirus crisis. "For a while, only a few patients came into the practice, meaning that we could only create a few emergency datasets and medication plans accordingly," Dr. Klüsener recalls. The situation has since returned to normal, however. His patients have so far been consistently positive about storing their data on the eGK: "There weren't actually any patients who didn't want to do this on account of data protection concerns." As far as the fear of data misuse is concerned, there is genuinely a big discrepancy between the media coverage and what he experiences when dealing with his patients.

The GP now hopes that the two TI applications will be rolled out and put into practice as soon as possible. "Most of all, I hope that the rescue vehicles here in the district will quickly be equipped with the software to read the emergency dataset," says Dr. Klüsener. "This useful new application will then make my everyday professional life as an emergency doctor much easier."

Taken from an interview conducted by Katja Chalupka (DGN Deutsches Gesundheitsnetz/InterData).



Dr. Thorsten Klüsener, a senior emergency doctor in the Steinfurt district, took part in the field test of two new medical applications.



From the Pentest Lab

# LLMNR: The Underestimated Danger

Some attack methods used by cyber criminals are not new, but they still work far too often – with sometimes catastrophic consequences.

One example is the attack via the LLMNR service.

The Link-Local Multicast Name Resolution (LLMNR) is a service based on the DNS (Domain Name System) protocol. Like the normal DNS service, it has the task of resolving names into IP addresses. However, it proceeds differently than the regular DNS service: it sends queries not only to one but to all participants in the same segment. In other words: LLMNR does not achieve its aim via a point-to-point connection, but via a broadcast.

An attacker can exploit this circumstance for his own ends. Unlike a normal system which ignores LLMNR requests which are none of its business, the attacker's system responds cheerfully to every single data packet. It claims that the requested name can be found under the attacker's IP address. LLMNR is not an authenticated protocol and the requesting systems therefore have no way of evaluating the authenticity of the response. Therefore they believe the information provided by the attacker. The victim then establishes a connection to the attacker, assuming it is the system the victim is looking for. If the attacker asks for authentication data, this is provided by the victim in the form of a hash value. The attacker can then record these hashes and attempt to reconstruct the original passwords.

This is bad enough, but it can get even worse – if the signing of data packets of the SMB protocol (Server Message Block) is not mandatory within the affected network. In this case, the attacker can go even further by using a method similar to a man-in-the-middle attack and establish a command line with system privileges on a victim system. Using this command line, he can then, for example, create a local user and add him to the group of local administrators. Or he can deactivate the local virus protection – which can often be done with a single command in Windows Defender. Once the local virus protection has been deactivated, the attacker can,

for example, use additional tools to read the clear text passwords of logged on accounts. This affects both local users and domain users.

An attacker can use this method to move from system to system, collecting new user accounts and the associated passwords until he encounters a user in the group of domain administrators. In this case, the game is quickly over – for the entire network.

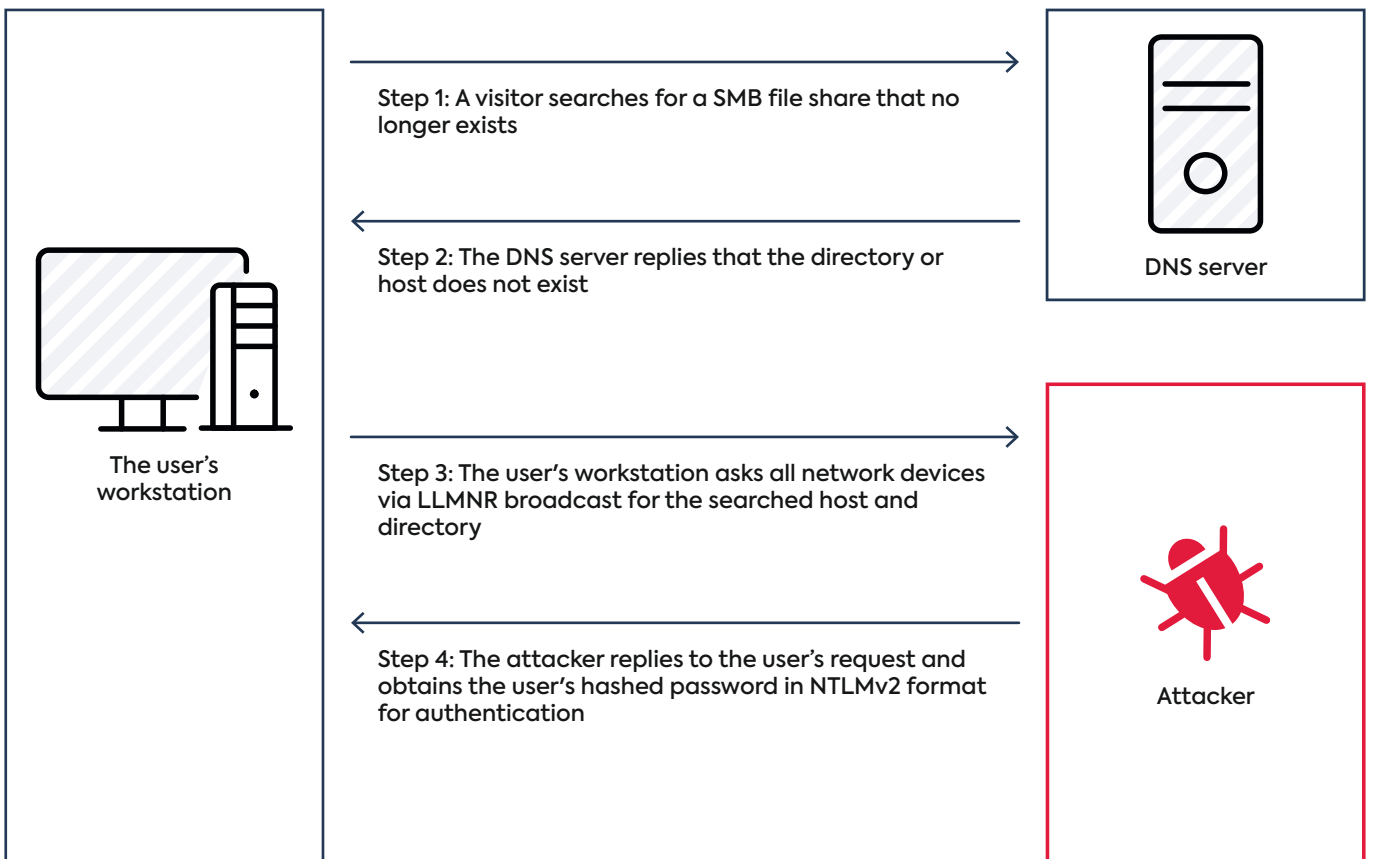
If the attacker is a commissioned pentester, he will now write his report. If it is a real attack, the victim can only hope that “only” some hard disks will be encrypted. But currently attackers often go beyond that. They place a worm that gradually changes data. These changes are hardly noticeable at first. A few months later, the affected company realizes that it can no longer trust its own data and that the unchanged data has already fallen out of the backup and is therefore lost.

One point remains open: How can companies or authorities protect themselves against the attack? This is surprisingly easy: SMB signing is set as mandatory and LLMNR is deactivated via Group Policy. However, these changes should be thoroughly tested before the rollout.



Dirk Reimers  
dirk.reimers@secunet.com

 Scheme of an attack via the LLMNR service.



# European External Action Service Uses SINA

The European External Action Service (EEAS) upgrades its worldwide network with a SINA security solution. Within the scope of a broader IT project, EEAS implements a large number of SINA components. They will enable the organisation to securely transmit and process classified information while at the same time increasing efficiency and reducing operating costs.

Primarily, SINA Workstations will be used in the project, which enable EEAS employees to access unclassified office networks as well as restricted networks with only one device. This means higher productivity, lowered costs and increased security.



Gerd Müller  
[gerd.mueller@international.secunet.com](mailto:gerd.mueller@international.secunet.com)

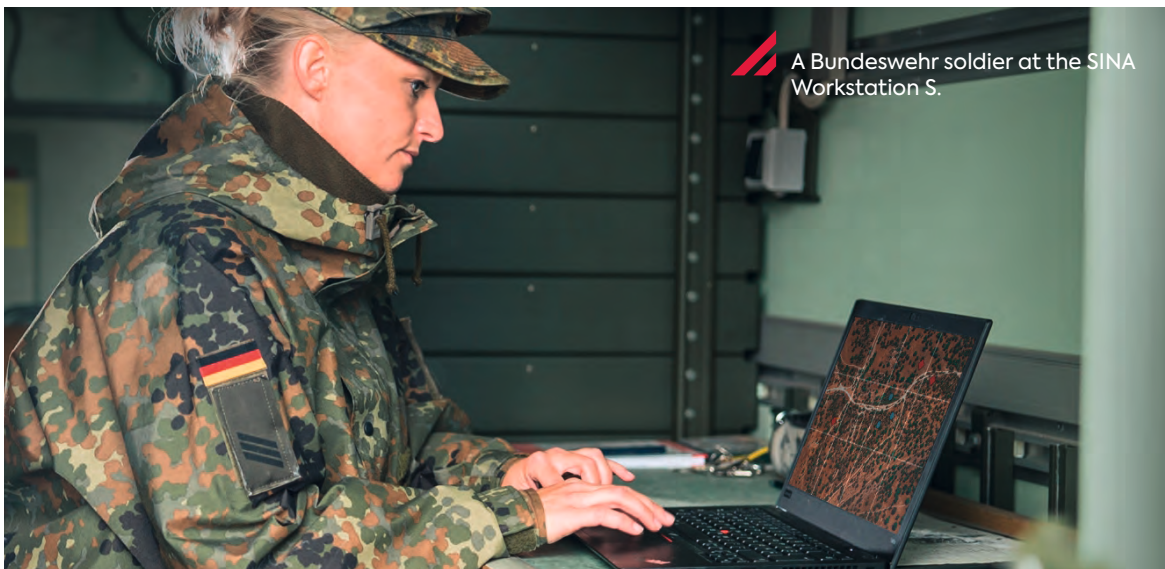
# Secure mobile working: BWI procures SINA Workstations S for the German Federal Armed Forces

BWI GmbH has commissioned secunet to supply more than 6,000 SINA Workstations S. The crypto clients are intended as a remote access service for the German Federal Armed Forces (Bundeswehr) and enable mobile, flexible working without compromising security. With this major order, BWI is continuing its successful cooperation with secunet: The company has already equipped workstations of the German Federal Ministry of Defence (BMVg)

with SINA Workstations S and provided the Bundeswehr with SINA solutions for various operational purposes and security requirements. The currently ordered devices have already been handed over to BWI on schedule.



Marcel Taubert  
[marcel.taubert@secunet.com](mailto:marcel.taubert@secunet.com)



A Bundeswehr soldier at the SINA Workstation S.





 IP telephony finally replaces ISDN.

## Goodbye ISDN. Hello All-IP.

ISDN will soon be history in Germany: Following the lines for private customers, those for business customers will also be switched off from 2020. Public authorities and companies that have not yet switched to Voice over IP are now taking this step. Many advantages go hand in hand with the changeover: IP telephones offer collaboration tools, access to user management servers and much more. With their operating systems and graphical user interfaces, they are more like computers than classic telephones. But this is exactly where the problem lies: IP-based telephones and telephone networks are generally just as vulnerable as computers and data networks.


The secunet Session Border Controller (SBC) solves this problem by filtering audio and video protocols such as SIP or RTP. It guards the entrance to an organisation's network and can be transparently implemented into any existing IT infrastructure. SBC works in an isolated container on the high-performance firewall secunet wall, which functions as a secure platform. This architecture enables complete protection and filtering of data streams at the network, transport, voice and application levels.

The German Federal Office for Information Security (BSI) confirms the trustworthiness and exceptional quality of the solution: secunet SBC is CC EAL 4+ certified by the BSI with the certification report BSI-DSZ-CC-1089. Organisations which mitigate the security risks of IP telephony can fully benefit from its advantages and make the transition a success story.



Mustafa Alaa Eddine  
[mohammed.alaaeddine@secunet.com](mailto:mohammed.alaaeddine@secunet.com)



 secuview titles in the old (left) and new design.

# Evolution Instead of Revolution: secunet in the New Corporate Design

The Corporate Design (CD) is an essential part of the corporate identity. It gives a visual dimension to the company's self-image, embodies its values and personality. In 2019, secunet's visual appearance was outdated and therefore no longer reflected the quality standards of the brand. A revision was necessary. Since the visual foundation was to be retained in order to maintain the recognition value of the established brand, secunet opted for a CD retouch - in other words, an evolution instead of a revolution.

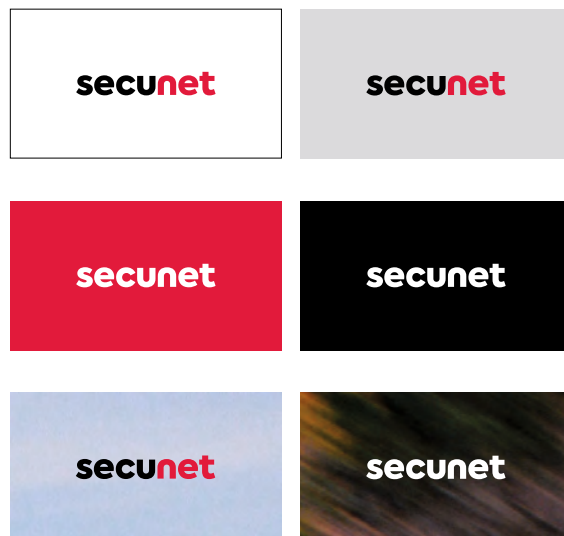
The logo was typographically reworked and got a more objective and rational appearance. Based on this, the typography was modernized. Axiforma, which is now used as the corporate typeface, combines optimum legibility with a contemporary look. The design of all media, from the product factsheet to the trade fair stand and the customer magazine secuview, was also reviewed and subsequently simplified, tidied up and transformed into a clear design language.

Last but not least, the imagery has also been redesigned. Large pictures, mostly total views - often from a bird's eye view - refer to the topics of secunet's target markets and show cities, industrial plants, airports or traffic routes.

The new CD harmonises the visual appearance with the company's high quality standards and makes secunet's visual communication fit for the future. The secunet website is currently undergoing a comprehensive redesign on the basis of the new CD.



Christian Reschke  
[christian.reschke@service.secunet.com](mailto:christian.reschke@service.secunet.com)



## Dates – September to December 2020

10 September 2020  
Workshop Industrial Security |  
Munich, Germany

15 – 16 September 2020  
StrategyDays IT Security |  
Bergisch Gladbach, Germany

29 September – 2 October 2020  
ICAO TRIP Symposium and  
Exhibition | Montréal, Canada

7 – 8 October 2020  
LEA-DER |  
Prague, Czech Republic

10 – 12 November 2020  
CODE Annual Conference |  
Munich, Germany

16 – 17 November 2020  
Rethink! IT Security |  
Berlin, Germany

23 – 25 November 2020  
KELI | Bremen, Germany

24 – 25 November 2020  
Berlin Security Conference |  
Berlin, Germany

30 November – 4 December 2020  
eurobits Security Summit |  
Various event locations

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

## Imprint

### Publisher

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

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

Marc Pedack, marc.pedack@secunet.com

### Design and Setting

sam waikiki GbR, www.samwaikiki.de

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

### Copyright

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

### Photo credits

p. 2, 14, 20, 25, 28, 41: iStock  
p. 35: iStock/LightFieldStudios  
p. 5, 32: alamy  
p. 3, 6, 12, 15, 17, 18, 19, 40: secunet  
p. 9: Land NRW  
Cover, p. 10: MWIDE NRW/E. Lichtenscheidt  
p. 37: Dr. Thorsten Klüsener

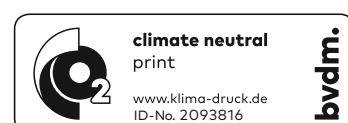
For reasons of legibility, in many cases the male  
form is chosen in the text. The information refers  
nonetheless to members of both genders.

## Subscribe to secuvview

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

[www.secunet.com/en/secuvview](http://www.secunet.com/en/secuvview)

There you can also change your preference or unsubscribe.





# Working securely – in the home office and on the move.

**Sensitive data stays ultra-secure  
with the SINA Workstation.**

The SINA Workstation offers a modern and powerful digital workspace for secure work in the home office and on the move. With a laptop or tablet, users can work with familiar applications like Office programs – anywhere and without restriction – and can access all their documents in the company network. As an IT security partner of the Federal Republic of Germany, we offer ultra-secure clients up to the SECRET security classification in our SINA Mobile range.

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

**secunet**