



## European Technology Autonomy

**Luigi Rebuffi, Secretary  
General of ECSO, on trusted  
cyber security from Europe**


### **Secure Connection in Times of Crisis**

Audio and video telephony at the German Federal Ministry of Health

### **Departure into Orbit**

Cyber high security for space



**19**  Cloud Computing: secure enough for medical research

## National

- 4 Audio and video telephony at the German Federal Ministry of Health: Secure Connection in Times of Crisis
- 7 Migration to IPv6: ELSTER – Fit for the Digital Future

## International

- 9 European technology autonomy: Public-Private Cooperation for Developing Trusted European Cybersecurity Solutions
- 12 European border control in Bulgaria: SSARM and secunet Will Implement the First EES Project in Europe

## Technologies & Solutions

- 14 Cyber high security for space: Departure into Orbit
- 19 Cloud computing, AI and distributed computing: Secure Enough for Medical Research
- 21 From the pen test lab: Fatal Interaction
- 22 Highly Secure Voice Communications via VoIP and SCIP: Wiretapping is Pointless
- 24 Business Continuity Management: Nothing Works Anymore – So How Do We Keep Things Moving?
- 28 SINA Workstation S with optimised graphics performance: Turbo for the Secure Home Office
- 31 Central administration of the SINA Workstation S: Ready for the Mass Roll-out

## News in Brief

- 34 New ENISA Threat Landscape Report available
- 34 Sterntaler Bonn: “Social sponsoring” for children

## Service

- 35 Dates – January to June 2021
- 35 Imprint

**27**  Business Continuity Management: nothing works anymore – so how do we keep things moving?



## Dear Reader,

A year that has demanded a lot from people is now drawing to a close. The coronavirus pandemic has, in some areas, brought public life to a virtual standstill for a second time. One can only hope that 2021 will herald a gradual return to normality, and that the negative consequences for the economy and society will not be too serious.

However, it can also be seen that the crisis has accelerated an inevitable, albeit partially protracted development: it has been the catalyst for the digital transformation. The prime example of this is how the world of work has changed. Since March 2020, secunet's customer teams have equipped a number of companies and public authorities with technology that makes it possible to work securely with sensitive data on the go. In doing so, they have helped to usher in a change that is sure to have a lasting impact. Anyone who has seen that online meetings from the home office can sometimes deliver the same results as a business trip halfway around the world does not necessarily want to return to the old model.

A further example is eGovernment. With its current coronavirus-induced economic stimulus package, the German government is, among other things, targeting the accelerated implementation of the German Online Access Act (Onlinezugangsgesetz). This law will require the German federal government, states and municipalities to offer all administrative services digitally by 2022. Here, too, the crisis could offer a boost to digitalisation. The technology for secure eGovernment has already existed for some time.

The pandemic has also thrown a spotlight on global supply chains and our dependence on non-European resources. How can we strengthen our technological sovereignty?

I was pleased to see that Luigi Rebuffi, the General Secretary of the European Cyber Security Organisation (ECSO), decided to tackle this topic (one that has long occupied secunet) in his contribution to this issue of secuviv.

Incidentally, our customer magazine is currently undergoing its own digital transformation. The printed version you currently hold in your hands will still be published every six months. However, it will soon also be supplemented with the new secuviv website, which will offer the usual mix of news, background reports, guest articles and interviews from the world of cyber security in a digital format. I would be delighted to see you visit us more often!

I wish you a very happy winter break – despite the current restrictions – and a wonderful start to the new year. Make the best of it and stay well!



Axel Deininger



Audio and video telephony at the German Federal Ministry of Health

# Secure Connection in Times of Crisis

As for many people, companies and public authorities, the year 2020 has been especially challenging for the German Ministry of Health (BMG). In spring, the BMG found itself in the centre of the Corona crisis, and confidential internal and external coordination became more important than ever before. Within a very short time, the BMG developed a security concept for a user-friendly video telephony solution and built it in collaboration with secunet and other partners and service providers. Since then, the solution has been in constant use – most notably for daily exchanges with institutions in the healthcare sector.

In March 2020, events came thick and fast. The Covid-19 epidemic, which had increasingly dominated the headlines since the start of the year, was declared a global pandemic by the World Health Organisation on 11 March. On 17 March, the Robert Koch Institute (RKI) upgraded its risk assessment for the German population from 'low to moderate' to 'high'. Later, on 26 March, it upgraded its assessment again to 'very high'.

When it became clear that a serious crisis was just around the corner, the BMG had already begun setting up a situation centre where all relevant information is compiled and all necessary coordination sessions are organised. During the pandemic, it is also especially important for the BMG to stay in constant contact with other countries. For such purposes, it is vital that authority staff can rely on secure, user-friendly communications tools.

In mid-March, the BMG contacted secunet to implement a new web conferencing solution. Despite the time pressure, it was self-evident that the solution would also need to satisfy the highest possible security requirements. The Netze des Bundes (NdB) network infrastructure used by the federal authorities in Germany sets clear security standards, for example.





### **Balancing security and useability**

In addition to the connection to the NdB, the solution needed to be linked to a variety of other existing networks, applications and technologies, ensuring that it can be used as widely as possible. This includes video conferencing systems already utilised by the BMG, SIP video conferencing solutions, and browser-based video calling via WebRTC. Last but not least, in addition to all these Voice-over-IP (VoIP)-based applications, a connection would be needed to the traditional public landline network. It was important to the BMG that virtual conference rooms could be easily booked for the new solution. Room numbers and PINs were to be assigned dynamically for each individual conference in order to achieve a suitable balance between security and user-friendliness.

The project started with a kick-off meeting on 23 March, a few days after the first contact on this subject. In addition to the BMG and other project partners, the project team included secunet, FRAFOS, a provider specialising in VoIP solutions and security, and VoIP-GO, a company that provides technical support for VoIP solutions. Both are long-standing partners of secunet.

### **A variety of technologies under one roof**

In addition to the restrictions imposed by the coronavirus pandemic, there were technical challenges to overcome. The project team had to integrate a variety of components, some of which came from different manufacturers. Networks, firewalls, existing video conferencing technology, a booking system, a virtualisation server, management

networks and more besides all had to work together seamlessly in the final solution. It was therefore advantageous that a key component was already available as a standard product: the secunet Session Border Controller (SBC). Among other things, this is used to securely connect different VoIP networks and to protect them from external attacks by means of an integrated firewall.

Development and installation progressed rapidly, and on 30 March – just one week after the project started – the BMG was already able to use the new solution for its first secure video conferences. The project team then reached further milestones in quick succession; on 2 April, browser-based video calls were made available via WebRTC, and on 6 April – just two weeks into the project – the BMG crisis centre used the solution for the first time.

#### A sprint a day

This speed was made possible thanks to agile project management. Development was incremental, meaning it took place in clearly defined stages. The individual development cycles – so-called ‘sprints’ – were deliberately made as short as possible and, in most cases, there was a sprint a day. The project team kept up to date on the status of the project across organisations using daily status calls.

In addition, not only did the BMG’s cooperation with secunet and its partners run smoothly in the spirit of partnership, but other BMG service providers were also well-integrated – an important prerequisite for a successful project.

As a result, the solution meets all the requirements of the BMG, makes no compromises in terms of security, and is very easy to use. A specially developed mechanism provides protection against brute force or denial-of-service attacks, for instance, without requiring any additional measures that would have been included at the expense of usability. Last but not least, the 24/7 support provided by secunet’s partner VoIP-GO also contributes to high user acceptance.

The solution thus enables simple, secure communication, helping the BMG and its department to remain capable of taking action during the coronavirus crisis. Additional steps have been implemented since the project began. In particular, the web conferencing solution has been expanded, both in terms of performance and functionality, and is now available for use by the BMG’s departmental authorities.



Marcel Göhler  
marcel.goehler@secunet.com

The **secunet Session Border Controller (SBC)** provides an optimum connection between different VoIP networks and serves as a central access point for them. Furthermore, it boasts a firewall function that protects the internal network and defends against external attacks with fraud detection and prevention measures. The secunet SBC can be transparently implemented into any existing IT infrastructure. It operates in an isolated container on the firewall platform secunet wall. This architecture enables the complete protection and filtering of data flows at the network, transport, voice and application levels. The German Federal Office for Information Security (BSI) has verified the trustworthiness and high quality of the solution: Under the code BSI-DSZ-CC-1089, it is certified for the highest attack intensity CC EAL 4+.

## Migration to IPv6

# ELSTER: Fit for the Digital Future

Some technological upheavals have far-reaching effects, but go virtually unnoticed by the wider public. This includes the replacement of the IPv4 internet protocol, in use for decades, by IPv6. The update, inevitable in the long term, was a high priority for the ELSTER electronic tax return. The solution needed to be based on a stringent security concept, but also needed to be implemented as soon as possible – all while ensuring ongoing operation. Together with secunet, ELSTER was able to plan and implement the project.

The history of IPv6 began back in the 1990s, when it became obvious that IPv4 could not provide enough IP addresses to meet the rapidly growing global demand. As a result, internet service providers resorted to emergency solutions like network address translation (NAT), which allows the multiple use of IP addresses. This made it possible to postpone resolving the shortage of addresses for many years. However, in the 2010s, it became clear that a switch to IPv6 was the only remaining option.

IPv6 offers a much larger address space than IPv4, as well as a slew of other benefits, e.g. concerning cyber security and mobile networking. Incidentally, IPv5 was the name of an experimental IP variant from the early 1990s, so the successor of IPv4 was directly assigned the number six.


### Version 6 on the rise

A gradual transition to the new version of the protocol has been taking place for some years now. Google reported an IPv6 adoption rate of around 50% in Germany as of October 2020. Meanwhile, smaller, regional internet service providers can no longer allocate IPv4 networks and have therefore switched to supplying their customers with IPv6 networks. They then use NAT to provide access to IPv4 where it is still needed (for now). As a result, the number of end users working with IPv6 has grown rapidly in recent years. Problems can occur if German internet users receive IPv6-only access when travelling abroad. In this case, IPv4-based web services cannot be used.

Consequently, the time has come for online service providers to move to IPv6. This is especially true for governmental bodies that offer socially relevant





 ELSTER, the electronic tax return, is the largest and probably most successful eGovernment procedure in Germany.

eGovernment services. On the part of the federal government, there is a requirement for German authorities to switch to IPv6 as soon as possible. However, one hurdle is the technical challenges involved in completing the migration during ongoing operation.

#### Armed for the transition period

The largest and probably most successful eGovernment process in Germany is the ELSTER electronic tax return, which is operated by the Bavarian Regional Tax Authority (Bayerisches Landesamt für Steuern, BayLfSt). “It was important for us to implement IPv6 on time to continue offering all end users the high-quality online services they are used to,” said Leo Fleiner, Head of Unit at the BayLfSt. “We therefore considered a dual-stack solution, meaning that the Mein ELSTER portal would be available in the IPv6 address space, but would also continue to be available in the IPv4 address space during a transition period.”

In the migration project, the BayLfSt worked with secunet, a company which has contributed to ELSTER’s secure online authentication processes since 1998. On the basis of an address plan provided by the BayLfSt, secunet supported the authority in developing the migration concept. The BayLfSt and secunet also adapted the security concept of the ELSTER environment to the modern conditions, which, among other things, allow the secure configuration and operation of new and existing network components and, in particular, firewalls.

#### Step-by-step implementation

Then came the migration phase. Service downtime is naturally not an option for an eGovernment service used by millions. The BayLfSt implemented the migration plans, which had been quality assured by secunet, in several chronologically sequenced steps. The Mein ELSTER portal remained available to end users at all times as usual.

A further challenge was the migration of the data centre’s internal services during ongoing operations with as little downtime as possible or none at all. The migration strategies and concepts developed by the BayLfSt – once again quality-assured by secunet – were implemented by the BayLfSt with the expert support of secunet. In this way, a smooth migration to dual-stack operation within the data centre was achieved. In the meantime, the internal services are almost exclusively operated with IPv6. secunet also carried out internal training, for example on the security aspects of IPv6.

At the end of August 2020, a public IPv6 address was assigned to the Mein ELSTER portal. Since then, the [www.elster.de](http://www.elster.de) domain can be resolved with IPv6 – and thanks to the dual-stack solution, it can also still be resolved with IPv4. The project was also well on schedule: with ELSTER, the BayLfSt is the first German authority to have completed a full migration of a data centre to IPv6. “We have implemented the IPv6 migration in a way that is technically sophisticated, but offers a number of advantages where continuous operation is concerned,” says Ralf Käck of BayLfSt.



Oliver Wolf  
[oliver.wolf@secunet.com](mailto:oliver.wolf@secunet.com)



## European technology autonomy

# Public-Private Cooperation for Developing Trusted European Cybersecurity Solutions

By Luigi Rebuffi, Secretary General, European Cyber Security Organisation (ECSO)

We see today that one of the envisaged priority actions for the European Commission is the development of a European “technology sovereignty”. This Brussels jargon could be better understood translating it into “technology autonomy”, i.e. Europe needs to increase its autonomous capabilities in the digital/technological domain.

Indeed, the Covid-19 crisis has shown in many sectors, including the digital one, the need for a higher level of “autonomy” in Europe. The Commission has stated that our European digital sovereignty (again mixing the concepts of autonomy and sovereignty) rests on three inseparable pillars: computing power, control over our data and secure connectivity. What they mention less often however, is that there are several other strategic technologies to be considered in a comprehensive view and that cybersecurity is the glue that holds all of these pillars together.

It is of course difficult to talk about entirely autonomous technological capabilities at the European level in a world where supply chains are so interconnected and dispersed geographically. In this case, to build up a trusted supply chain, how can we control certain components, equipment, systems that are not produced in the country (or continent)? European national administrations can certify that certain components or equipment manufactured somewhere in the world and possible updates/patches (following certain rules) are compliant with national security laws (in this case indeed sovereignty laws) and that they can be used with trust in the supply chain. The final system or service can thus be considered as “sovereign” as it is respecting national legislations and we can then talk about “sovereign capacities”.

The diversification of suppliers also contributes to this concept as sovereignty, for a country and for Europe, also implies being able to provide secure or vital services to its citizens, society or economy independently from the (potentially) critical situations

 Luigi Rebuffi



# Luigi Rebuffi

**Luigi Rebuffi** is the Secretary General and founder of ECSO (European Cyber Security Organisation) as well as founder and Secretary General of the Women4Cyber Foundation. After graduating in Nuclear Engineering from Politecnico di Milano (Italy), he worked in Germany on the development of high-power microwave systems for the next thermonuclear fusion reactor (ITER). He continued his career at Thomson CSF/Thales in France where he took on increasing responsibilities for European Affairs (R&D) in different sectors: telecom, industrial, medical, scientific, becoming in 2003 Director for European Affairs for the civilian activities of the Group. He suggested the creation of EOS (European Organisation for Security), coordinated its establishment in 2007 and was its CEO for 10 years. Until 2016 and for 6 years, he was an advisor to the European Commission for the EU Security Research Programme and President of the Steering Board of the French ANR for security research. In 2016 was one of the founder of ECSO and signed with the European Commission the cPPP on cybersecurity. In 2019 he created the Women4Cyber Foundation to promote participation of women in cybersecurity and became its present Secretary General and member of the Administrative body. In 2020 he was nominated in the list of "IFSEC Global Influencers in security – Executives"



(e.g. European dependency on health equipment at the beginning of the Covid-19 crisis in only one country and a too limited number of suppliers).

## The German contribution

Especially now, with the German presidency of the Council of the Union, it's important to appreciate how German companies and business associations are taking the lead on this. For example, secunet's CEO Axel Deininger, has been a key ambassador for ECSO's new Cybersecurity Made In Europe label, showing secunet's commitment to harmonising the European cybersecurity ecosystem through this key marketing innovation for small cybersecurity companies.

Additionally, prominent German associations such as TeleTrusT and eurobits e.V. (the latter a partner in the ECSO Cyber Investor Days in Bochum 30 November – 1 December) are strong collaborators with ECSO. TeleTrusT for its part was one of the founding members of ECSO with the support of Gerd Müller, also from secunet, so it's clear then that this need for truly European cybersecurity solutions is felt strongly by Germany companies and associations.

Moreover, this issue is of course felt nationally at the institutional level. The support from the German Federal Ministry for Economic Affairs and Energy for the GAIA-X project, although focusing more on data than cybersecurity, shows the understanding at the national administration level that Europe needs to develop common European solutions in the various fields of emerging technologies in order to have a

better control on national security and economic development supported by the digital transition.

Europe as a whole is steadily improving its digital maturity level and is progressively understanding that in this domain a stronger cooperation is needed, maybe in the future, compromising some national sovereignty to build up a stronger common European sovereignty. But this will take time.

## The added value of public-private dialogue

In this maturity process, the public – private dialogue will be essential to identify the path of common European sovereignty and support an increase of digital (strategic) autonomy, particularly when linked to the needed investments and procurement rules for sensitive applications. This is exactly the area where ECSO with its public and private members are bringing a high level of added value to Europe.

ECSO has just created the Cyber Security Sovereignty and Autonomy (CYSSA) Working Party, with the participation of members of ECSO, to find possible answers to some of the questions considered in this article and discuss what priorities to develop and use to increase European strategic cybersecurity autonomy.

The objective of the ECSO CYSSA is to develop and convey "common messages" on European Cybersecurity Sovereignty and Strategic Autonomy, supporting the development of opportunities for European solutions and growth of our industry.

The activities of CYSSA will also be in line with ambitions of the European Commission on “technological sovereignty” and would meet institutional expectations of the Competence Centre Regulation approach. This stance should help the European members of ECSO, such as secunet, to develop their market and make ECSO recognised as the leading voice for European cybersecurity autonomy and sovereignty, attracting more support and participation from EU industry and administrations.

The discussion with the public sector will allow the best match between sovereignty legislation and technical (increasingly autonomous) solutions, also considering the need to use non-EU solutions when not truly European solutions are available in Europe. If the application is not sensitive, there could be no need to restrict this kind of supplier. Yet, in case of sensitive applications (identified by national administrations), non-EU solutions implemented in the systems/services should be validated by national administrations providing a kind of “sovereign validation”.

### The future of European cybersecurity in a rapidly evolving world

Many questions lie ahead: What strategic technologies/components/equipment/systems/services will be needed to ensure national security (following guidelines from national administrations) and

for (strategic) economic growth? What capabilities and capacity are present in Europe, what is missing, what should/could be developed and when (and which investments are needed) and what should be purchased outside and made “trusted” (via validation/certification, when needed)?

In this complex future, ECSO will continue to federate the public and private cybersecurity community in Europe, develop the competitiveness of its members and the European cybersecurity ecosystem, supporting the increase of the European digital autonomy.

We stand at a critical juncture in global technological competition and we need bold, radical, transformative action to ensure Europe is cybersecure for the future to come. We must work together through public-private fora to ensure we are addressing common issues collectively, speaking a common language. Only in this way can we gather and federate the European cybersecurity community to ensure that Europe is capable of producing the cybersecurity solutions to protect its future in this uncertain world.

## SECUNET: ECSO MEMBER FROM THE VERY BEGINNING

On 5 July 2016, a public-private partnership was concluded between the European Commission and the newly founded ECSO as part of the EU’s cyber security strategy. secunet played a decisive role in the establishment of the ECSO and continues to support its activities to this day.

### Axel Deininger

- since September 2020 Member of the Board of Directors

### Gerd Müller

- for TeleTrust (until August 2020): Vice Chairman of the Board of Directors, member of the Partnership Board, participation in the Financial Committee and Strategy Committee
- since September 2020 for eurobits e.V. Bochum: Member of the Board of Directors

### Peter Rost

- Vice Chair Working Group (WG) 2 Market deployment, investments and also on the Strategy Board, participation WG 3 and 4

### Christine Skropke

- Member of the Women4Cyber Council and Partnership Board and participation in WG 4 SME / Regions





European border control in Bulgaria

# SSARM and secunet Will Implement the First EES Project in Europe

In preparation for the planned European Entry/Exit System (EES), Bulgaria has opted for border control technology from SSARM and secunet. The overall solution will relieve the Bulgarian authorities and compensate the additional workload that will arise in the future from the collection of biometric data at the border.

As part of the Smart Borders Initiative, the European Parliament decided to establish the common biometric Entry/Exit System (EES) for the registration of all travellers from third countries. Therefore, as of 2022, Third Country Nationals (TCN) will have to register with four fingerprints and a facial image when entering the Schengen area through land, sea and air borders.

Following a recent tender, the Bulgarian Ministry of Interior has commissioned the company SSARM as general contractor to implement the first EES project in Europe. secunet acting as industry partner to SSARM will deliver and install 20 secunet easygates

for automated border control including face and fingerprint verification and 8 secunet easykiosks for the self-preregistration of TCN. For stationary border control counters, secunet provides 66 easytowers as well as fingerprint scanners for the high-quality biometric acquisition (facial images and fingerprints). The EES components will be installed at the airports in Sofia, Varna and Burgas.

Automated and self-service systems play a key role to compensate the additional efforts due to biometric enrolment at the border as required by the EES. The solutions will simplify and speed up the border control process. With the EES solutions from secunet's border gears portfolio, Bulgaria will implement the latest technology for future-proof, secure and efficient border control.

The newest generation e-gates – secunet easygate – incorporates highly sophisticated face and fingerprint verification including latest biometric fraud detection mechanisms, known as presentation attack detection (PAD).

secunet easykiosk and secunet easytower assure ISO-compliant high quality acquisition of face and/or fingerprints. This is of utmost importance to ensure the reliable and efficient identification at border control points against data of this scale – the ESS will contain an estimated 300 million entries from TCN.

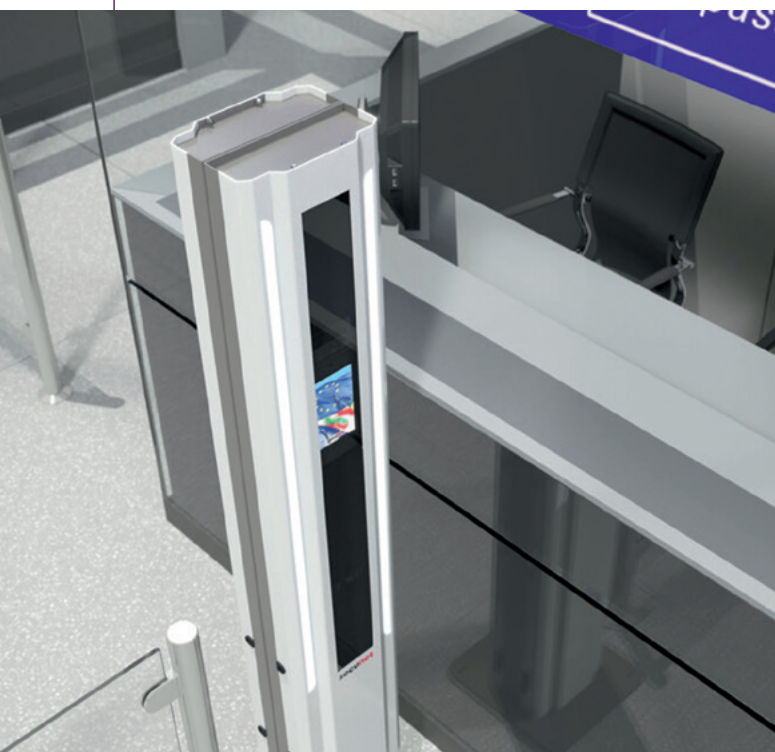
SSARM is the prime contractor and responsible for the project management as well as installation and support services. The installation starts at Sofia airport. The participating companies currently expect the entire EES project to be completed before summer 2021.



Walter von Weber  
[walter.vonweber@international.secunet.com](mailto:walter.vonweber@international.secunet.com)

## QUALITY AND SPEED FOR BIOMETRIC ACQUISITION AT STATIONARY BORDER CONTROL

secunet easytower ensures fast and high-quality facial image acquisition for stationary border control, delivering the highest biometric data quality according to EU Regulation 2017/2226. An automatic height adjustment and the additional diffused illumination provide ISO/IEC 19794-5:2011 compliant facial images as required by the European Entry/Exit System (EES).



Thanks to its intuitive user interface, the easytower can be easily operated by both travellers and border guards. A built-in feedback screen displays the "live" image of the facial image camera. The traveller looks into a digital mirror with additional user guidance, which – available in several languages – ideally supports the traveller. A fully automatic or manual capture mode is selected according to requirements. Thanks to the intuitive capturing process, the easytower guarantees a short recording time and thus accelerates the border control process. The integrated lighting ensures high-quality, well-lit shots, providing homogeneous exposure of the face even under unfavourable lighting conditions.



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



Cyber high security for space

# Departure into Orbit

For some years now, innovative technologies have been giving new impetus to space travel: rockets and satellites are becoming ever smaller. This makes them cheaper than their larger, more complex predecessors and allows them to be put into orbit more flexibly and in larger numbers. There they take over useful, sometimes vital functions that are now an integral part of our everyday lives. As launchers, satellites and spacecraft exchange sensitive information with their ground stations and with each other, there is no way around cyber security in space. However, security technologies must be adapted to the extreme conditions in orbit.

Space travel is increasingly making headlines again. As recently as November 2020, news went around the world that the US space company SpaceX had brought four astronauts to the International Space Station ISS as part of the first regular manned mission by a private company. But anyone interested in innovative space projects does not necessarily have to look across the Atlantic. In Europe, too, especially in Germany, a dynamic technological development is taking place which is repeatedly being talked about and is also attracting international attention.

In addition to traditional players such as the European Space Agency (ESA), the German Aerospace Center (DLR) and the relevant corporations, a lively ecosystem of space technology start-ups has emerged. In Augsburg, Munich or Neuenstadt

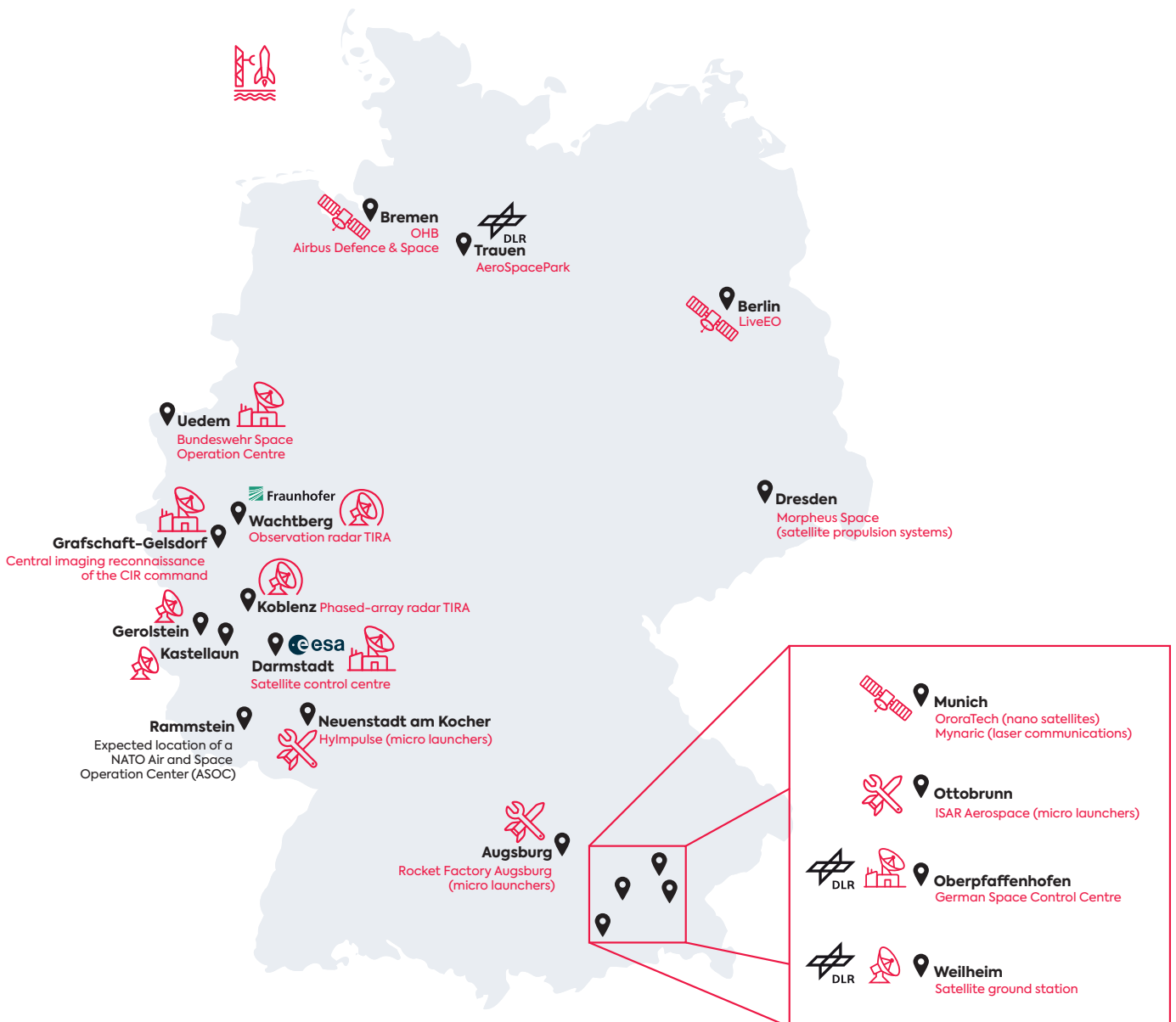


am Kocher, young companies have set up in business to develop powerful smaller rockets. Other start-ups or research institutions are building satellites that analyse climate phenomena or forest fires or improve Internet access. This “New Space” scene shines with innovation and is driving the established big players forward technologically.

**Mini, micro, nano, pico, ...**

One trend that all players must take into account is the miniaturisation of space technology. Current nano-, cube- and cluster satellites are sometimes no larger than a shoebox. They show their true size when they work as a group and perform a wide variety of tasks in large numbers as so-called constellations. Their compact dimensions and relatively low weight have a further advantage: for many current satellite projects, more moderately sized launchers, so-called micro-launchers, are sufficient. These are less complex and costly than the classic large launchers such as the European Ariane. This makes the new space technology much more agile – an enormous advantage for both civil and military application scenarios.

 Exemplary space relevant locations in Germany



Satellites are becoming more and more versatile and cover more and more functions that are important for our daily lives. The European satellite navigation system Galileo, for example, plays a major role (alongside the US Global Positioning System) for determining positions in navigation devices in vehicles or mobile phones, and also provides time services which are used, for example, to synchronise decentralised energy networks.

Military organisations are also increasingly relying on space technology, particularly for reconnaissance, communication, navigation, time synchronisation and early warning. The first satellite of the German Armed Forces (Bundeswehr) was launched into space in 2006 as one of five small satellites of the SAR-Lupe reconnaissance system, which provides high-resolution images of the earth's surface independent of light and weather conditions. The more powerful successor system SARah is expected to be launched into orbit in 2021.


In 2009 and 2010, the two communications satellites COMSATBw-1 and -2 were launched, which made the Bundeswehr less dependent on commercial providers, particularly for international missions. Among other things, both satellites enable tap-proof telephone calls, video conferences and Internet access worldwide. Furthermore, an electro-optical reconnaissance satellite is being developed for the BND, two of which are planned.

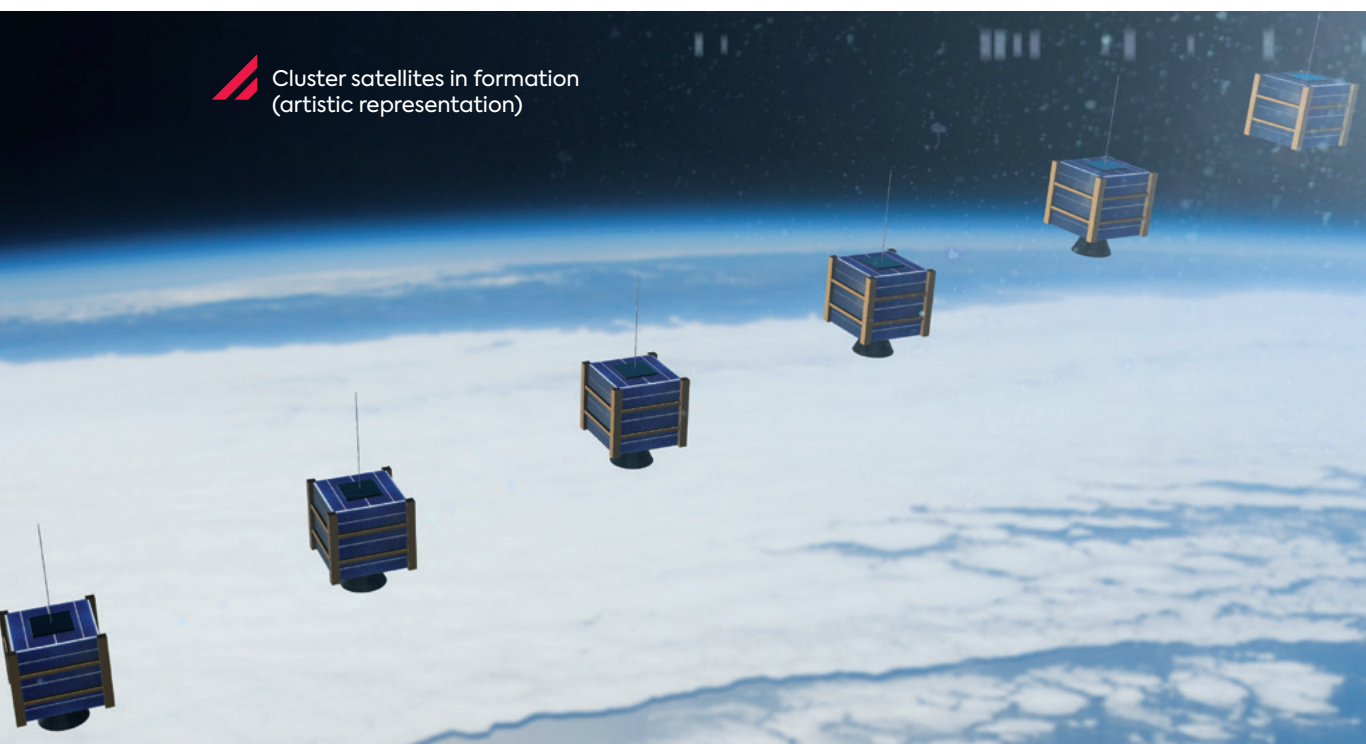
### Strategic dimension

Today, space travel is widely regarded as a key technology. The investment bank Morgan Stanley estimates that the global space market will triple by 2040, to more than \$1.1 trillion. Space-based systems perform essential tasks for early crisis detection and thus for the German government's ability to act in foreign and security policy. The Federal Government's current space strategy states: "The internal and external stability of our country increasingly depends on the functioning of our infrastructure positioned in space."

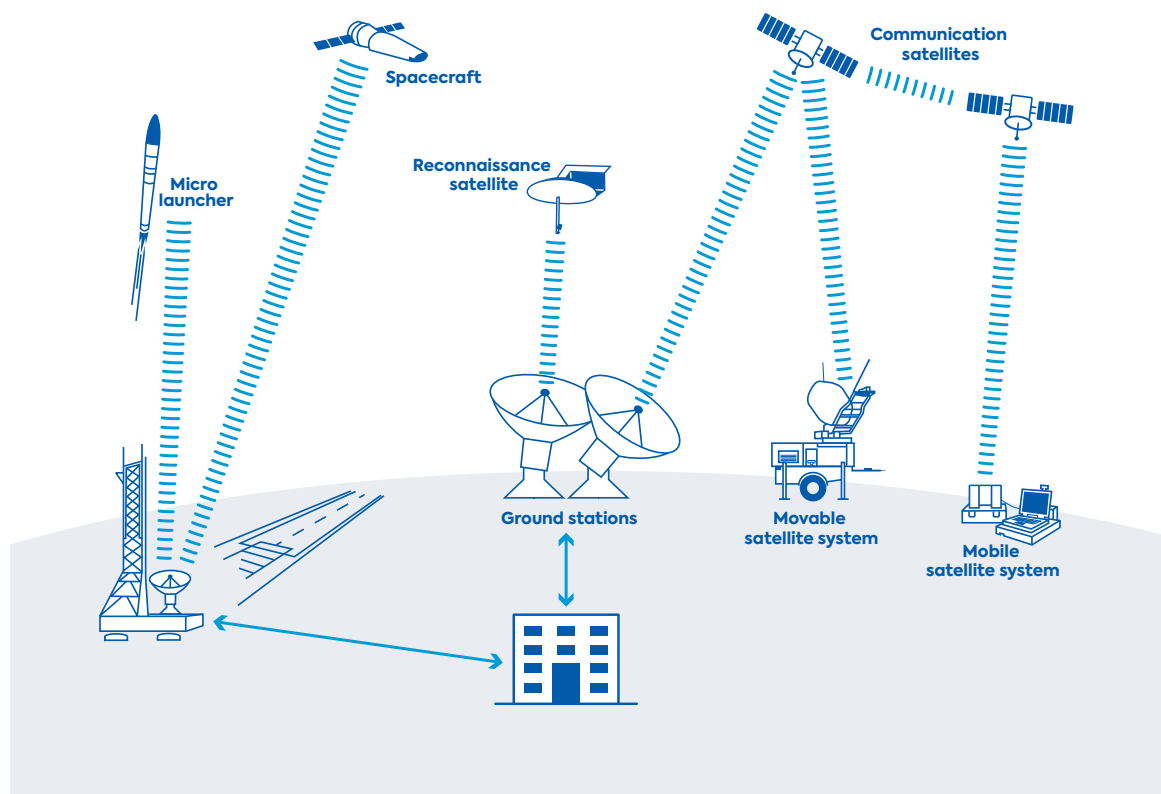
Technology in orbit can quickly become an Achilles' heel and therefore requires adequate protection. A sudden failure of a satellite system due to collision, targeted interference, manipulation or even take-over could have serious consequences.

The Bundeswehr Space Operations Centre (Weltraumoperationszentrum) focuses on the protection of both military and civil German space technology. It monitors near-Earth objects in space and carries out reconnaissance if necessary. These objects include not only satellites and other spacecraft, but also space debris, larger meteorites and asteroids entering the atmosphere. In addition, the range of tasks now also includes the planning and implementation of space operations.

 Cluster satellites in formation  
(artistic representation)



 Rough schematic outline of a space infrastructure



### Independent capacity to act

In addition, the Bundeswehr is pursuing new approaches to arm its infrastructure in orbit against disruptions and attacks – and is going to rely on miniaturised space technology from now on. In future, it should be possible to quickly restore or replace failed systems by, for example, launching small or micro satellites into orbit within a short time. This approach is called “Responsive Space”.

For this purpose, it would be advantageous not only to have its own nationally available launch vehicles but also to have its own launch site – as a supplement to the international launch options for more powerful launch vehicles. A number of site candidates are currently being evaluated. Consideration is also being given to a floating offshore platform in the North Sea.

In addition to space observation and agile action capability, cyber security will in future also play a major role in securing the infrastructure in orbit. Civil and military space technology is not only threatened by physical influence, but increasingly also by foreign cyber attacks – with similar consequences. If attackers manipulate the control data exchanged

between satellites and ground stations, they can quickly cause considerable damage – especially as the situation in orbit becomes increasingly complex: Several thousand active and disused satellites are currently orbiting the Earth, and their number is growing rapidly.

How can cyber security be implemented in orbit? Part of the answer is that the same technologies that have been successfully used on the ground in high-security networks for many years can be used. In order to communicate sensitive digital information, authorities and the Bundeswehr use the Secure Inter-Network Architecture SINA, which was developed by secunet on behalf of the German Federal Office for Information Security (BSI). It offers solutions for very diverse security requirements. The most secure SINA H systems with BSI approvals up to classification level SECRET are already being used on a large scale in national high-security infrastructures. Space technology providers also use them to process classified information. In addition, large volumes of data transmitted by the German Federal Armed Forces on a satellite-based basis have been encrypted in a highly secure way using SINA H for many years.



### Extreme operating conditions

Anyone who wants to communicate not only via but also with satellites or spacecraft in a highly secure manner must integrate encryption technology on board the flying objects. The requirements that high-tech equipment must meet under these conditions are quite demanding. This starts with the rocket launch, where strong vibration and acceleration forces act on the hardware. Once in orbit, the equipment is exposed to very large temperature fluctuations and high levels of radiation. The non-existent atmosphere requires different thermal concepts and device designs.

High reliability is essential for satellite systems. The partial failure of individual components can affect entire space missions. Once systems are in orbit, there are not many options left for their maintenance and necessary repairs. Therefore, they should be remotely updatable and reconfigurable as flexibly as possible. In addition, particularly important elements should be designed to be redundant from the outset.

In addition, miniaturisation is a requirement that extends to the level of assemblies and modules. This also applies to security modules. In order to exclude undesired physical influence in space or at least make it significantly more difficult, satellite systems should be designed to be tamper-proof.

secunet has been working for customers from the space sector for many years and is now strengthening its commitment to space-qualified cyber high-security technology. As a visible sign, secunet's "Defence" division will become the "Defence&Space" division from January 2021.

### Looking ahead

SINA systems are already taking off in military helicopters today, providing encrypted video transmission and communication from several kilometres above the ground – we reported on this in *secuview* 2/2019. A special hardware platform is used for this application. What remains to be done on the way into space is technically even more demanding, but feasible.

Space travel and cyber security are two complementary future-oriented high-tech fields which will benefit greatly from each other in the future. Their common path has only just begun.



Dr. Michael Sobirey  
[michael.sobirey@secunet.com](mailto:michael.sobirey@secunet.com)

 Launch of an ESA Vega rocket  
 (c) ESA - S. Corvaja





Cloud computing, AI and distributed computing

# Cloud: Secure Enough for Medical Research

For a long time, cloud computing was considered cost effective, but potentially unsecure. When security requirements are especially high, the cloud has therefore not been an option. This is now changing – thanks to the SecuStack secure cloud operating system. Take healthcare, for example: SecuStack enables machine learning with confidential patient data which is used securely across different institutions, based on the cloud. This means that new medical knowledge can be gained without jeopardising data protection. In order to make application scenarios like this a reality, SecuStack relies on cooperation with Intel and Scontain.

Industry experts have long claimed artificial intelligence (AI) to be a ‘mega topic’ that will shape the IT landscape and transform our everyday lives. Adaptive and self-improving machine learning (ML) is playing a major role in this. The number of application scenarios for ML has gone through the roof in recent years. One of these scenarios is medical research, whereby ML is used to aggregate and analyse patient data. This results in ML models that allow researchers to gain medical insights. The problem is that the necessary raw data must be collected across institutions, i.e. from other medical institutions like hospitals. Since the data is sensitive, data protection reasons often prevent this. As a result, AI-supported research often threatens to fail due to a lack of access to raw data.

The solution to this problem lies in a technology that also has been a mega topic in IT for many years – but, until recently, was considered an uncertainty factor: cloud computing. The SecuStack cloud operating system has set new standards in IT security. If the solution is combined with hardware-based technology from Intel and Scontain, new types of cloud applications can be implemented in the areas of ML and distributed

computing (multi-party computing). ML models can use the cloud to access encrypted data from participating medical facilities, for instance, while other parties like the cloud provider are securely denied access.

### What makes the cloud secure?

Cloud computing is known to work according to the 'as-a-service' principle. Typically, cloud providers offer services and application programming interfaces (APIs) to their customers, but do not release the software or source code. To a certain extent, anyone using cloud services must therefore trust the provider. This is out of the question for public institutions and highly regulated private companies like energy suppliers or healthcare providers. Without transparency and complete control over data, it has been almost impossible for such organisations to use cloud services in the past.

In order to change this, a joint venture of secunet and Cloud&Heat developed the SecuStack cloud operating system, which is based on the open-source software OpenStack. SecuStack's high level of security is primarily achieved by consistently encrypting data with the same security elements secunet has been using in high-security applications for years. These cryptographic mechanisms are transparently integrated, allowing users to set up their own cloud infrastructures for sensitive data on the basis of testable software 'made in Germany'. Sovereignty over the data and applications remains with the user at all times.

### Enclaves provide additional hardware security

For certain applications, it makes sense to provide the cloud infrastructure with additional hardware-side protection. For this reason, the developers of SecuStack established contact with experts from Intel at an early stage, having in mind the Intel Software Guard Extensions (SGX). Processors equipped with this technology can execute critical infrastructure services within trusted, hardware-protected areas, so-called 'enclaves'. This raises significant hurdles for attackers.

With the scalable Intel Xeon processors of the third generation (codenamed "Ice Lake"), Intel makes it possible to protect up to one terabyte of code and data during use in enclaves. Intel SGX is integrated

into the entire spectrum of Ice Lake platforms. This allows partners to develop their own solutions based on Ice Lake that reduce existing risks associated with data protection and compliance in highly regulated areas such as healthcare. The combination of SecuStack and Intel SGX enclaves constitutes the most comprehensive cloud protection available today.

The linking of the two technologies takes place via the SCONE platform from Scontain. With SCONE, services can be easily integrated and executed in Intel SGX enclaves. In this way, critical functions like runtime encryption, secrets management and authorisation can be implemented in SecuStack in an especially secure manner, using Intel SGX enclaves.

### Secure distributed computing

In addition to infrastructure security, the Intel SGX enclaves for SecuStack offer a further advantage: they can be used to implement new types of AI and ML processes for which secure data exchanges are essential – such as in the medical research application scenario described above. The process used in this area works as follows: application services are executed in a distributed manner, i.e. across resources that are isolated from one another, via the SecuStack cloud operating system and secured in Intel SGX enclaves. The services are then orchestrated, i.e. combined to form a network, using the open-source system Kubernetes. This allows distributed computing to take place in a secure context. With this method, ML models can be trained with patient data across hospitals without any sensitive data having to leave the hospital of origin.

The approach is called 'confidential federated machine learning'. One typical challenge of cloud computing does not play a role here: whether or not the users involved trust the cloud provider is irrelevant. The data, code and models remain protected from access by the provider at all times. Data protection is thus assured, allowing medical researchers to fully exploit the potential of machine learning. In the best-case scenario, this will lead to findings that can benefit us all.



Dr. Kai Martius  
[kai.martius@secunet.com](mailto:kai.martius@secunet.com)



From the pen test lab

# Fatal Interaction

Successful attacks on IT systems are usually not due to the fact that an attacker was only able to exploit a single vulnerability. Instead, it is the interplay of several factors that can turn an attack into a disaster. Let us take an example. An attacker finds a command injection in a web portal – a vulnerability that allows them to smuggle in their own commands, which the system then executes. If the vulnerability is located in an isolated area behind a firewall that filters both incoming and outgoing traffic, this is already an undesirable security incident. But if the web server process runs with root privileges, can communicate freely over the internet for updates, and also receives data from an internal database, this combination of vulnerabilities can open the door to an advanced persistent threat (APT) being placed on the internal local area network (LAN), gradually spying on the entire organisation or, worse still, gradually changing the values of central databases.

To counteract such a fatal combination of attack vectors, IT security experts should be involved and unit pen tests should be carried out. If the analysts know in which environment a web portal is operated and which interfaces this portal has to other systems, attack vectors can already be identified and eliminated in the planning phase. The experts can use firewall and database audits to simulate attacks which got past frontline safeguards, for instance.

Successful attacks are often not merely based on missing patches or system hardening; these points can often (though not always) be adjusted after the project is wrapped up. A typical developer makes decisions based on the requirements for the application. Many of these decisions are based on assumptions about how users will and should use the newly created application. Then, components are developed and functional tests are devised based on these assumptions to check the central function of the software.

A good pen tester then checks these assumptions – only that he reacts in precisely the way a typical user will not. For example, he uses illogical value ranges, manipulates content transferred from the website, deletes existing parameters or creates new ones. Depending on the robustness of the application, these manipulations may lead to internal or external errors, be compensated by default values, or lead to a crash. The earlier in the development process these tests are performed, the easier it is to modify the solution. Furthermore, the implementation of additional functional tests containing intentionally erroneous data can be pushed forward, ultimately allowing the developer to create a more robust application.

The same applies to the systems used by the web portal under review, such as databases, reverse proxies or firewalls. The earlier system operators understand that none of the components can rely on the others to be 100% trustworthy, the higher the resilience of the overall system. This also enhances the ability of the individual components to act in a secure manner despite possible errors.



Dirk Reimers  
[dirk.reimers@secunet.com](mailto:dirk.reimers@secunet.com)





Highly Secure Voice Communications via VoIP and SCIP

# Wiretapping is Pointless

The end of ISDN is dragging on a little, but that does not change the fact that the digital telephony standard has had its day. In the near future, German network operators will switch off the 'Integrated Services Digital Network' introduced in 1989 and IP telephony will then finally take its place. This poses a challenge for public authorities that depend on secret voice communications, as ISDN-based encryption systems are still used for this purpose across the board. With the SINA Communicator H, secunet now offers a compact, easy-to-use desktop solution that makes IP telephony highly secure – up to the **SECRET** classification level.

In Germany, telephony encryption solutions based on the ISDN standard are currently still used in public administration and by the German Armed Forces, in particular. In order to extend the life of these solutions, some rely on ISDN IP gateways. However, since the two underlying technologies, ISDN and IP, are very different – ISDN is line-oriented, while IP is packet-oriented – there are compatibility problems that can never be completely eliminated. Gateway solutions can facilitate the transition, but they will have to be replaced by new security technology specifically designed for IP telephony in the medium term.

secunet first took up this challenge several years ago. It was clear on what a new solution could be based: the SINA security architecture, which secunet had developed on behalf of the German Federal



With SINA Communicator H, users can easily switch between different classification levels.

Office for Information Security (BSI), is essentially a concept for securing IP-based networks. In the meantime, SINA has proven itself over many years in numerous federal and state authorities and has become the leading security architecture in the Federal Republic of Germany. SINA is also used in other countries. A variety of versions are available for different application scenarios and security requirements, with German and international approvals for classification levels from RESTRICTED to SECRET.

On this basis, secunet developed a highly secure telephony solution for the post-ISDN era: the SINA Communicator H. Designed as a desktop device in telephone format, the solution can be used for voice and data communication and is capable of being approved for the German classification level GEHEIM and its international equivalents (SECRET). The SINA Communicator H can be operated both within public authority networks and directly over the internet. It uses proven internet standards for Voice over IP (VoIP), supporting existing, commercially procured session initiation protocol (SIP)-capable switching infrastructures. In addition, it implements NATO protocols such as the Secure Communication Interoperability Protocol (SCIP), thus enabling secure communication with international allies.

## “The SINA Communicator H combines the requirements of secret voice communication with the everyday practices of our modern working lives.”

Jan Leduc, Senior Product Manager at secunet

Thanks to SINA Communicator H’s multi-level capability, users can easily switch between different security classification levels, such as VS-NfD, VS-VERTRAULICH and GEHEIM in the German national environment, and RESTRICTED, NATO SECRET or EU SECRET/SECRET UE in the international environment. Native telephone calls can also



be answered. “The SINA Communicator H combines the requirements of secret voice communication with the everyday practices of our modern working lives,” says Jan Leduc, Senior Product Manager at secunet. “With this solution, we have once again shown that high security and user-friendliness do not have to be mutually exclusive. As soon as a user has authenticated themselves with a security token and PIN, the solution’s functions can be accessed via convenient touch-screen controls.”

The 10.1-inch display enables numerous other applications in addition to pure voice communications. Text communications, video telephony and even thin-client functionality – with an optional external monitor – are all planned for later expansions, for instance. Further applications can be added as required, such as web clients, operational fax support, file and document exchange or multi-party messaging.

The migration of ISDN solutions to SINA Communicator H is also a worthy endeavour for public authorities, because the new telephony solution can be functionally integrated into existing SINA installations. “Today, it is already possible to communicate with SINA Workstation S and H via a secure IPsec connection up to the GEHEIM (SECRET) level using VoIP,” explains Leduc. “This function can also be integrated into SINA Communicator H, making it backwards compatible with the VoIP applications of SINA Workstation S and H. Central administration via SINA Management, which is usually already used by public authorities, also increases efficiency and facilitates migration. Overall, our goal was to give our customers as much added value as possible with the SINA Communicator H – and in my opinion, we have achieved our goal.”



Jan Leduc  
jan.leduc@secunet.com





## Business Continuity Management

# Nothing Works Anymore – So How Do We Keep Things Moving?

There is a power cut, an important service provider can no longer deliver, or pollutants are discovered in office premises ... the Covid-19 pandemic is not the first time an incident has paralysed the operations of a business or public authority from one moment to the next. In such emergencies, organisations that have invested in Business Continuity Management are at a distinct advantage. If the worst comes to the worst, the affected time-critical business processes can then enter controlled emergency operation, gaining important time for those responsible to cope with the incident.

Hamburg Airport, June 2018: A cable fire on a main power line causes a power cut in the morning. The reserve feed-in is also affected, as the normal and emergency power supplies run through a common shaft at the point of damage. The entire airport is emptied. After overnight repairs, operations can be resumed the following day.






Nordeutscher Rundfunk (NDR) public broadcaster, November 2018: During renovation work in a high-rise office building, a previously enclosed insulating material comes into contact with the air. Measurements in the affected offices reveal asbestos particles in the air. The management has the building completely closed for safety reasons. Alternative workplaces are provided for 300 employees within 18 hours. A decision regarding the replacement building will be announced in September 2019.

Everyone knows the third example! In spring 2020, the Covid-19 pandemic meant that countless office workstations around the world could no longer be used at short notice. A large number of mobile office workstations had to be set up at speed. Since then, interest in the topic of Business Continuity Management (BCM) has grown significantly.

 Fig. 1: Standard failure scenarios for business processes



 Fig. 2: Exemplary BCP overview for the emergency team

	time-critical business process HelpDesk	time-critical business process EPOS administration	time-critical business process token production	business process reporting
 Service provider failure	x (assumption of risk)	–	✓	no BCP needed
 Building failure	✓	✓	✓	
 IT failure	x	x	x	
 Personnel failure	x	x	x	
 Production facility failure	–	–	✓	

✓ = plan available      x = plan needed, but missing (plus a reason for this, if necessary)  
 – = not applicable/necessary

Those who have established BCM policies are better equipped for scenarios like these. First of all, a business impact analysis is used to determine which business processes need to continue even in an emergency. These are so-called ‘time-critical business processes’. Business continuity plans (BCP) are then drawn up for each process identified, specifying what needs to be done in the event of an emergency to ensure the process can continue. But how do companies and public authorities draw up targeted business continuity plans?

At this point, it is necessary to provide some definitions. BCM, or ‘crisis management’, is a system for organising and ensuring the business continuity of an institution at the business-process level. Depending on the approach, the data-centre level may be included (as is partly the case in German Federal Office for Information Security’s forthcoming 200-4 standard), or may be organised in an independent management system under the umbrella of IT service continuity management (ITSCM (ITIL)) or IT crisis management. In the following, only crisis scenarios for the business-process level are presented.

**From individual BCPs to a BCP with standardised failure scenarios**

The traditional approach in BCM is to establish one BCP per process. The focus and scope of each BCP are often defined individually, depending on capacities or departmental requirements. If an emergency occurs, outsiders are often involved who must then get to grips with a detailed document for the first time. It is not unusual for them to be faced with surprises. They have to spend time understanding the logic of each individual BCP – time that should be used more sensibly in an emergency.

In addition, some BCPs are incomplete or not applicable to the case at hand. Let us take an example. In its detailed BCP, a department regulates how business is to be continued after (A) an office fire with (B) the subsequent failure of specialist software at the alternative location and (C) a lack of on-site support from the software manufacturer. A functioning BCP

is available for this escalating series of events. But what if it is not the software, but the hardware that is defective – and the replacement service provider is not only needed at the alternative location?

For these reasons, an alternative approach has been developed which works on the basis of standardised failure scenarios that are defined once and then apply to all business processes. The failure scenarios ‘service provider’, ‘building’, ‘IT’, ‘personnel’ and ‘production facilities’ have been established (Fig. 1).

This approach offers a number of advantages. Firstly, all parties can rely on an **equivalent level of coverage**; once a topic is delineated and defined as a standard failure scenario, it is applied to all business processes. The specifications with regard to focus and scope, for instance, are established centrally and are defined taking into account the entire institution.

Secondly, the BCP can be executed on a **modular basis**. Individual crises can be combined and, if necessary, can follow an escalation sequence.

Thirdly, the **comparability of the plans** is guaranteed, as there is only one document template for each failure scenario. For example, all BCPs for the ‘service provider failure’ scenario follow an identical structure. Dialogue between departments is encouraged and later crisis teams can quickly apply BCPs from different departments.

Fourthly, the **transparency of the implementation status** is guaranteed at all times; it is easy to check at any time for which failure scenarios the business process is currently equipped. This means that no area can be inadvertently left out. The obstacle of having to examine the plans’ content in detail for an audit is eliminated. Furthermore, if the crisis has occurred, the emergency team will be able to quickly identify – without any knowledge of its content – what a particular BCP is for. It also provides a transparent overview of areas in which action is needed, but where there is no BCP for a specific reason (see Figure 2).


**Basic principles for success**

The approach involving failure scenarios is based on a number of simple assumptions:

- All business processes are analysed **neutrally and uniformly**, regardless of the organisational structure. The same failure scenarios are always revisited.
- Failure scenarios are **cause-neutral**: Planning always starts with the fact that the time-critical business process must be compensated for on an ad hoc basis using a suitable continuity strategy. The cause is invisible and irrelevant. For example, in the 'service provider failure' scenario, it is not important if the service provider is currently unavailable due to a mechanical fire, a storm, insolvency or insufficient product quality.
- The basis for planning is the **worst-case approach**. This prevents the crisis response team from being surprised by escalations of reasons for failure that initially appear limited in scope. In the 'building failure' scenario, it is

assumed that the building in question, including its indirect surroundings, is no longer available. For planning purposes, a restricted impact zone (e.g. of one kilometre) should be assumed. A second building on the same site is therefore not a reliable alternative option. It should also be assumed that practically no working materials such as laptops or paper password lists are available after leaving a building – as may actually be the case in the event of incidents posing acute health risks. In the 'personnel failure' scenario, it is assumed that all participants in this business process, without exception, are no longer available. Any substitution arrangement within this group is useless. Nobody is available for further enquiries.

For all failure scenarios, a variety of different continuity strategies (including several variations) can be defined for the selection process. All developed continuity strategies are derived from the four abstract basic intentions in the table below.

 **Basic intentions of the continuity strategies**

Intention	Derivation from failure scenarios
<b>Diversification</b>	<p><b>&gt;&gt; productive operation continues with active partitioning</b></p> <p>Service providers: e.g. awarded 50:50 contract lots                      Buildings: e.g. two remote buildings are used simultaneously                      IT: e.g. active geo-redundancy with synchronisation                      Personnel: e.g. staff work at two locations</p>
<b>Replication</b>	<p><b>&gt;&gt; firmly prepared (use: immediately)</b></p> <p>Service provider: e.g. alternative service provider is waiting (contract)                      Building: e.g. alternative location is completely furnished                      IT: e.g. data centre container is ready for use                      Personnel: e.g. other staff are always fully trained</p>
<b>Standby</b>	<p><b>&gt;&gt; equally or rudimentarily prepared (use: longer / unknown lead time)</b></p> <p>Service providers: e.g. alternative service providers are known                      Buildings: e.g. empty building could be converted                      IT: e.g. stored hardware could be configured                      Personnel: e.g. similar staff could be trained</p>
<b>New procurement after the event</b>	<p><b>&gt;&gt; procurement / selection after the event</b></p> <p>Service providers: e.g. search for service providers and ask for a quote                      Buildings: e.g. rent a new building                      IT: e.g. buy hardware and install backups                      Personnel: e.g. hire staff service providers; train new staff</p>





### Introduction to BCM with a series of questions

Anyone who wants to get an initial overview of the current status of BCM-relevant topics in their own company or public authority, should ask the following questions:

- Are there business processes that absolutely must continue and are therefore time-critical business processes?
- Can access to time-critical IT systems be restored in a few minutes?
- Is it documented which concrete working environment has to be provided for a time-critical business process (e.g. financial accounting) if this has to be rebuilt from the ground up on an ad hoc basis (number of workstations, networking, applications, switched telephone numbers, etc.)?
- Can time-critical service providers also be reached in the evening if necessary, and will they then provide support for as long as the crisis lasts?
- After a fire in the server room on a Sunday afternoon, who decides specifically who has to do what, when and how?

secunet has many years of experience in Business Continuity Management and supports companies and public authorities in developing goal-oriented business continuity plans. The effort demanded by this process is well worth it if valuable time can be gained in an emergency.



Christian Bergmann  
[christian.bergmann@secunet.com](mailto:christian.bergmann@secunet.com)

### Examples of concrete continuity strategies for the 'building failure' scenario

- **Conversion:** moving to rooms regularly used for other tasks (meeting rooms, canteen, offices of non-time-critical departments)
- **Work environment service providers:** reserved rooms, shared rooms (e.g. first come, first served)
- **Remote alternative location:** use of remote areas belonging to the organisation
- **Mutual agreement:** partners keep clearly defined building areas available for mutual use
- **Delivery of resources:** external contractor delivers (partially) finished environments (office containers, lightweight building construction)
- **Teleworking:** working from home office or mobile locations
- **Working time window:** optimum use of limited workstation capacity (off-peak times, weekends)
- **Robust operation:** permanent decentralised distribution of a business process to several locations

SINA Workstation S with optimised graphics performance

# Turbo for the Secure Home Office

The coronavirus, which is rampant worldwide, has changed our working world. At the same time, the requirements for technical equipment are changing. Since video conferences are now standard practice, graphics performance is particularly in demand in these times. secunet has reacted quickly to this and, together with its partner Cyberus Technology, has further developed the SINA Workstation S. Tor Lund-Larsen, CEO of Cyberus, explains together with Armin Wappenschmidt, head of the Network&Client Security department at secunet, how the secure client has been optimised and what advantages result for users.

**What are the concrete requirements of users today? And what advantages does the optimised SINA Workstation S offer them?**

**Wappenschmidt:** The demands are constantly increasing. Even with the high level of security offered by SINA Workstation S, users want to use it for all application scenarios in modern working life. This does not remain unanswered: We have always moved with the times and have adapted our solutions to the way users work. In the beginning, for example, SINA Workstation S was only available as a desktop, but today it is mobile and very flexible. Then came support for USB audio headsets and video cameras. Finally, graphics performance, which is required for video conferencing, among other things, played an increasingly important role. This has not only been the case since the Corona pandemic, but the crisis is currently driving this development strongly: presence meetings are cancelled, people work in the home office. We have responded quickly to this in recent months with technical improvements.

**Lund-Larsen:** The optimised SINA Workstation S offers several advantages for the user at the same time. Videos and other moving image applications such as video conferencing now run smoothly and in high quality without having to reduce the high security requirements of SINA S.

**How did you implement this technically?**

**Lund-Larsen:** The integration of the Cyberus virtualisation platform is a significant extension of the architecture of the SINA Workstation S. It required very close and intense development collaboration between secunet and Cyberus Technology.

The solution starts below the SINA software stack. The separation of the various guest systems, which is so important for the security of the SINA Workstation S, is now no longer ensured by the Linux kernel, but by the underlying virtualisation platform.

This also enables new functional extensions such as graphic virtualisation. Because the various guest systems of the workstation were previously unable to access a common graphics card for security reasons, the virtualised CPU, to put it simply, had to take over the graphics calculations. The new system architecture relieves the CPU of graphics performance. This makes the system more efficient, which can also have a positive effect on battery life.

The virtualisation platform is based on our open source “Hedron” micro-hypervisor, whose roots go back to the TU Dresden – in other words, technology “Made in Germany”, as is common for SINA.

**Wappenschmidt:** Cyberus has in-depth know-how on virtualisation, low-level hardware, CPU design and software test automation – a rather unique mix.

That is why Cyberus is the right partner for us. By the way, the Cyberus team played a major role in the discovery of the well-known “Meltdown” and “Spectre” security vulnerabilities in x86 processors in 2018 and 2019, thereby proving its experience especially in the CPU and low-level area. We plan to implement further projects together.

#### Were there any challenges in the development work that you had to solve?

**Lund-Larsen:** When the cooperation with secunet started, the initial focus was not on graphics performance – but on additional system security through virtualisation. The so-called “Trusted Compute Base” (TCB) was to be further reduced – i.e. the amount of code to be trusted. We had already made good progress in this respect when Armin called one day and

## In interview



**Armin Wappenschmidt**  
Head of Network & Client Security,  
secunet Security Networks AG



**Tor Lund-Larsen**  
CEO Cyberus Technology GmbH  
Photo: Tommy Sauer  
([info@tommysauerphotography.de](mailto:info@tommysauerphotography.de))



## Cyberus Technology

The Dresden-based company Cyberus Technology, founded in 2017, specialises in software for cyber security. In 2018, its employees discovered serious security gaps (“Meltdown” and “Spectre”) in micro-processors, which affected not only companies and public authorities, but also private computer users. Two other core areas of Cyberus Technology are virtualisation technology and test automation of software during its development. For more information, please visit [www.cyberus-technology.de](http://www.cyberus-technology.de).

brought up the issue of graphics performance, which had suddenly moved up the priority list due to the Corona pandemic. So we completely sealed off our project developers from all other tasks – and that for nearly a year and under pandemic conditions! We are pleased that we have now achieved our goal of offering secunet a unique graphics solution for the SINA Workstation S platform without losing sight of our original goal of reducing TCB and increasing system security.

### What improvements will be available when?

**Wappenschmidt:** The first version of the graphics-accelerated SINA Workstation S will appear as early as December 2020, focusing on the use of graphics hardware in a guest system. Due to the current situation, we wanted to quickly present users with a solution for this. A further release is planned for next summer, which will bring additional performance improvements and optimised coordination of all system resources. In this release, features such as support for multi-monitor scenarios and 4K monitor resolution, which have been available to our customers for some time, will also be available for the graphics-accelerated SINA Workstation S.

**Lund-Larsen:** We are looking forward to further intensifying the cooperation and we appreciate very much that secunet has placed so much trust in us so far. Although our company is small, we can offer highly specialised expertise which we are happy to use for secunet.



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



Even gaming is no problem with the graphics accelerated SINA Workstation S...  
 Photo: Tommy Sauer  
 ([info@tommysauerphotography.de](mailto:info@tommysauerphotography.de))



## Central administration of the SINA Workstation S

# Ready for the Mass Roll-out

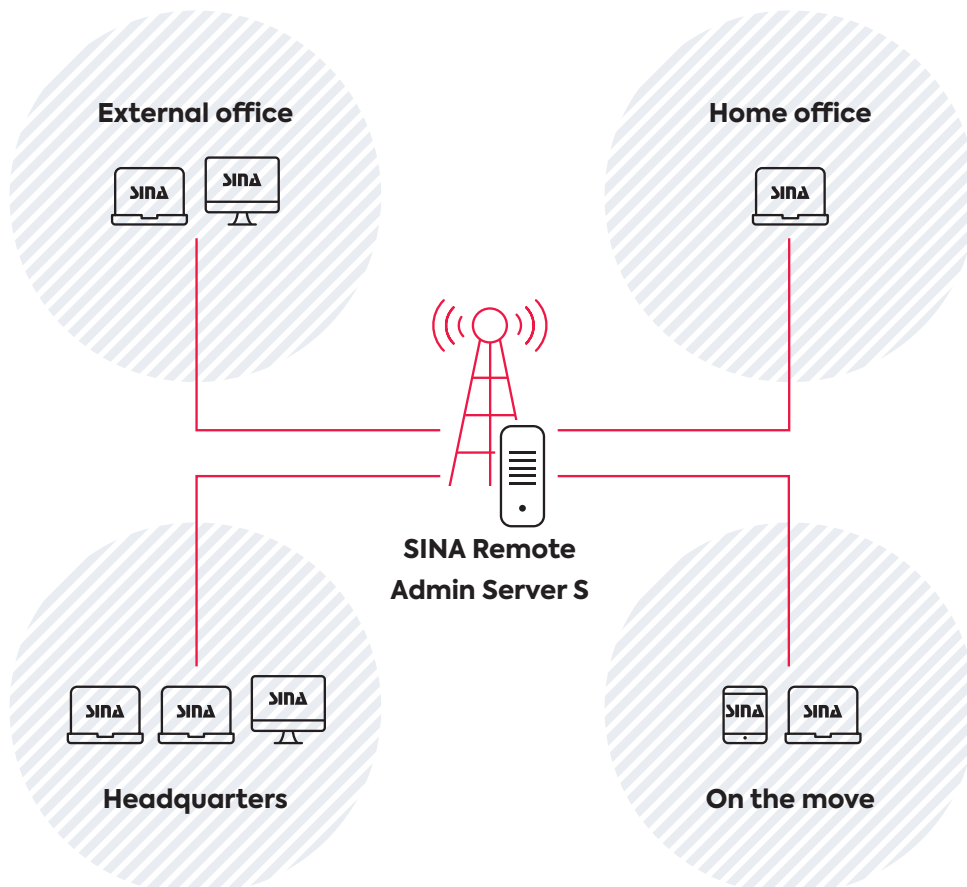
Especially at the moment, when social distancing is important and the preference is for working from home, many authorities and companies are equipping their employees with SINA

Workstation S devices. The SINA Workstation S offers a secure yet convenient alternative to the conventional workplace PC – with great mobility too, since users can access their organisation's IT network securely from wherever they are, including their homes.

When managing large-scale installations with lots of SINA Workstation S devices, those in charge of IT are supported by the SINA Remote Admin Server S, which secunet is continually optimising.

The more complex the IT infrastructure, the more crucial the administration work becomes. This applies to secure SINA infrastructures as well. The challenges are especially significant for administrators and IT support staff if they do not have physical access to infrastructure components, and if employees are increasingly working from home and are only connected to their authority or corporate network via the Internet.

In the age of the coronavirus pandemic, the amount of time spent working from home can be up to 100 per cent – over an extended period of time or, in any event, over a period of time that is difficult to plan for. Service times for the components can only be adhered to via remote access, therefore. Regular changes such as software updates and configuration improvements are normally straightforward to carry out using this approach. However, when security updates are installed, or breakdowns remedied, remotely, there can certainly be an element of risk attached.



A good example of this is a software update that needs to be implemented across all devices. Everyone knows from experience what this involves: the prompt to restart the machine always appears at the worst possible moment and is therefore readily postponed for as long as possible. So, what can the administrator do if some users do not carry out the required restart, even after receiving multiple requests to do so?

The solution to this issue is the SINA Remote Admin Server S (SINA RAS) remote maintenance software. This enables the administrator to first of all gain an overview of which SINA Workstation S devices accessible via the network operate with which version of software. If required, the administrator can then force a centrally controlled software update. In addition, the inventory function gives the administrator an overview of a number of other parameters.

**A software update** can contain important security patches and should generally therefore be run at the earliest opportunity – particularly where it is necessary for maintaining the approval given by the German Federal Office for Information Security (BSI). Even where the update is not urgently required for ongoing operations, it is nonetheless generally beneficial to users. In addition, having the same software in place on all devices makes looking after the system administration easier.

#### Convenient maintenance

The main task of SINA RAS is to facilitate configurations of SINA clients during operation. Updates of SINA apps, changes to access permissions or the installation of new network profiles – administrators can implement these types of tasks centrally using the tool, irrespective of where the clients happen to be located.

SINA RAS was given the go-ahead in the mid-2010s, when several German federal ministries fully equipped themselves with SINA Workstation S devices. It was at that point that the question first arose of how the secure client, which had originally been designed as a specialist solution, could be rolled out and administrated on a large scale. The answer lay in automation and remote maintenance.

Initially, SINA RAS began as a pure installation script for the roll-out of SINA Workstation S devices. Within a short space of time it then developed into a flexible tool for carrying out remote maintenance of SINA S components. Since then, it has been continuously enhanced and adapted to new versions of the SINA Workstation S.

Via the CLI (Command Line Interface), the RAS commands can be integrated in an automation workflow that responds to the precise requirements of the organisation. Since SINA RAS uses a scripting language (Groovy), the individual functions can be adjusted in a highly granular way for automation within the organisation's own procedures. New scripts can even be created and used.



### Future-proof infrastructure

SINA RAS was developed with the objective of facilitating the administration of a large number of SINA Workstation S devices without requiring the deployment of additional personnel. A further objective was to offer power users workable automation interfaces. The functional scope of SINA RAS is changing with the growing demands of users. The next release, for instance, will include support with administrating ongoing virtualised guest systems, thanks to the RAS Maintenance Mode.

Some technical optimisation may be unseen by the users, however it makes the system more robust and reliable. This category includes some of the measures currently in plan that will, in future, reduce the test burden on developers and thereby accelerate the release flow for the implementation of specific requirements. For users this means that, in future, necessary features can be made available faster and in a more agile way as a product version – which can be a decisive factor, especially when it comes to the operation of complex infrastructures.



In future, the SINA Remote Admin Server S will provide a graphical user interface.



Improved test automation is the prerequisite for faster enhancements and future redesigns. In one of the next steps, the internal interface to the SINA Workstation S is optimised in order to make the device administration even clearer and the operational processes more task-oriented. To do this, in future the administrator will be given access to a flexible, high-level API and a graphical user interface (GUI) that sits on top of it. With the high-level API, an abstraction layer is introduced that offers more straightforward access to control of SINA RAS – either manually through the administrator or automatically as part of the customer processes. The GUI will soon enable more intuitive, faster operation and make it easier for users who only look after a small number of SINA Workstations, or who want to enhance them, to get started with remote administration.

The SINA Workstations are clearly shown in the GUI and can be filtered or sorted by means of their parameters, so that the necessary administrative interventions can be carried out more easily. Administrators who have limited experience of Linux-based systems or whose work is generally less Shell-based will, in future, benefit from the user-friendly interface in the same way as users whose main domain is Windows administration, or those only partly involved in looking after SINA Workstations.

In future, the SINA RAS should be amalgamated with other SINA administration tools in one SINA Management Centre (SMC). These optimisation measures will make central administration of SINA even more functional and convenient. The SINA Remote Admin Server already provides users with the necessary tool to administrate SINA S components easily and reliably, however.



Andreas Rach  
andreas.rach@secunet.com

The **RAS Maintenance Mode** is an enhancement that utilises the flexible functionality of SINA RAS in order to carry out changes to virtual SINA Workstation guests – even remotely, without intervention by the user.



# New ENISA Threat Landscape Report Available

In October 2020, the European Union Agency for Cybersecurity (ENISA) has published the 8th annual ENISA Threat Landscape (ETL) 2020 report, identifying and evaluating the top cyber threats for the period January 2019–April 2020. This year’s publication is divided into 22 different reports, available in pdf form and ebook form. The combined report lists the major change from the 2018 threat landscape as the COVID-19-led transformation of the digital environment. During the pandemic, cyber criminals have been seen advancing their capabilities, adapting quickly and targeting relevant victim groups more effectively.

The ENISA Threat Landscape (ETL) 2020 report is available for download on ENISA’s website: [www.enisa.europa.eu](http://www.enisa.europa.eu)



## Sterntaler Bonn: “Social Sponsoring” for Children

For many children, a loving home in which they are cared for and their development is encouraged is a matter of course. For many, however, it is not. The Sterntaler Bonn e.V. association addresses this problem. It offers needy children in Bonn more education, support and participation: Homework supervision in family centres, healthy meals, projects to prevent violence, promotion of psychomotor skills, language and music development – with these and similar offers, the association helps children to make a better start in life. It has found an apt term for its activities: “social sponsoring”.

This year’s secunet Christmas donation goes to Sterntaler Bonn. “We are convinced that every child deserves appropriate support,” says Bill Mockridge, patron of Sterntaler. Arndt Hilse, chairman of the association, adds: “For many of our measures, we are dependent on funds in addition to the commitment of our members. We are therefore very pleased about the support”.


Contact possibility:

Sterntaler Bonn e.V., Sudetenstr. 24, 53119 Bonn

Arndt Hilse, Chairman

Email: [vorsitzender@sterntaler-bonn.de](mailto:vorsitzender@sterntaler-bonn.de)



 Arndt Hilse (left) and Bill Mockridge, Sterntaler Bonn e.V.

# Dates – January to June 2021

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

2–3 February 2021

17. Deutscher IT-Sicherheitskongress | digital

13–15 April 2021

DMEA | Berlin, Germany

27–28 April 2021

ID@Borders Conference | Brussels, Belgium

3–5 May 2021

Omnisecure | Berlin, Germany

5–6 May 2021

LEA-DER | Prague, Czech Republic

17 May 2021

RSA Conference | digital

18–19 May 2021

Berlin Security Conference | Berlin, Germany

19–20 May 2021

AFCEA | Bonn, Germany

25–28 May 2021

ICAO TRIP Symposium and Exhibition | Montréal, Canada

29 June – 1 July 2021

Passenger Terminal Expo | Amsterdam, Netherlands

Do you have any questions or would you like to book an appointment with us? Please send an email to [events@secunet.com](mailto:events@secunet.com).

## Imprint

### Publisher

secunet Security Networks AG  
Kurfürstenstraße 58, 45138 Essen, Germany  
[www.secunet.com](http://www.secunet.com)

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

Marc Pedack, [marc.pedack@secunet.com](mailto:marc.pedack@secunet.com)

### Design and Setting

sam waikiki GbR, [www.samwaikiki.de](http://www.samwaikiki.de)

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

### Copyright

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

### Photo credits

Title, p. 9, 10: ECSO  
p. 2 (top), 14, 16, 19, 21: Adobe Stock  
p. 2 (bottom), 8, 27, 33 istock  
p. 3, 13, 22, 23, 29 (left), 31: secunet  
p. 5: BMG/Akthar  
p. 12: alamy  
p. 18: ESA – S. Corvaja  
p. 29 (right), 30: Tommy Sauer  
p. 34: Sterntaler Bonn e.V.

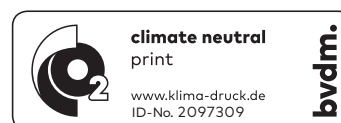
For reasons of legibility, in many cases the male form is chosen in the text. The information refers nonetheless to members of both genders.

## Subscribe to secuvie

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

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

There you can also change your preference or unsubscribe.







**Utilities  
companies stay  
plugged in.**

**secunet security infrastructure  
keeps cyber attackers at bay.**

When it comes to the security of utility suppliers, secunet is ready to help. As IT security partner to the German federal government, we advise operators of critical infrastructures on security policies and implement superior security measures.

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

**secunet**