Günther Oettinger

Interview with the EU Commissioner for Digital Economy and Society

CLAAS

Safeguarding Agriculture 4.0: Interview with Thomas Böck, Member of the CLAAS Group's Board

Arne Schönbohm

The President of the German Federal Office for Information Security (BSI) on Cyber Security as a Requirement for Successful Digitalisation

The Importance of Cyber Security in the European Digital Single Market
International
04 The Importance of Cyber Security in the European Digital Single Market
10 SDW InterOp 2016 Test Results: Light and Shadow
11 Czech Republic: Border Control Systems Made Future-Proof

National
12 Arne Schönbohm on Cyber Security as a Requirement for Successful Digitalisation
15 ELSTER: Security for a Successful Model of E-Governance
18 Smart yet Secure: Safeguarding Agriculture 4.0
22 eIDAS: an Easy Upgrade to Trust
25 secunet Takes on the HJP Consulting eID Testing Business Unit
25 New secunet Showroom in Essen
26 Automated IT Baseline Protection
28 Three Questions for secunet Board Member Thomas Pleines

Technologies & Solutions
30 A Secure Authentication Procedure for SNMPv3
31 En Passant: ICS Attacks
32 SINA Apps: Tailor-Made Applications
33 Greater Speed for Secure Networks
33 SINA Workstation Now Also with a Virtualised Smartcard
33 Hardened Crypto Client with SECRET-level Approval
34 Ransomware: No Chance for Cyber Extortionists
35 Shorter Lines at Passport Control
35 Packed and Ready to Go

News in Brief
36 Actively Involved in Cyber Security
38 it-sa 2016 Achieves Double-Digit Growth
38 Close Cooperation with Industry Representatives

Dates
39 Upcoming Events
As 2016 draws to a close, cyber security is receiving more attention from the media and society than ever before. This development started in 2013 with the debate on the NSA scandal and continued with the discussion of the threat to critical infrastructures (which led to the German IT Security Act of 2015), before intensifying again this year. The sharp increase in cyber attacks, successful hacks of hospitals, the malware-induced failure of Deutsche Telekom network routers and reports of state-sponsored cyber espionage have transformed what was once a niche topic for IT experts into a cross-cutting social issue. Everyone is affected by it today – whether as a private user, a citizen of a nation or the EU, an employee, a traveller, a driver, an online shopper or even a user of utility services.

In November, the German Federal Office for Information Security (BSI) published its status report for 2016. In the report, its experts outlined a new quality of threat. An average 44,000 malware programs are filtered out of the German federal administration’s email traffic each month, for instance. In addition, the government’s networks are targeted by a variety of other attacks every day, including 20 highly specialised cyber attacks. In order to help public authorities and companies to counter such threats, we need a robust cyber security industry in Germany. This is why BSI President Arne Schönbohm uses his guest article to underline his support for the government’s Digital Agenda to make Germany ‘the world’s number one in encryption’.

The cyber security industry is also high on the European agenda. In an in-depth interview, EU Commissioner Günther Oettinger explains the motives behind the public-private partnership contract between the European Commission and the newly founded European Cyber Security Organisation (ECSO). We are delighted that we were able to help make this agreement a reality – representing just one example of how we took on a more international role this year.

As you can see, a particularly busy year for us is coming to an end. We would therefore like to thank all our clients and partners for their continued trust in our company. I hope you enjoy reading this issue of secuview and wish you a wonderful Christmas and a very happy new year!

Yours,

Dr Rainer Baumgart
The Importance of Cyber Security in the European Digital Single Market

After extensive preparations, the European digital single market finally began to take shape last year. So, too, has cyber security, as demonstrated by the contractual public-private partnership between the European Commission and the European Cyber Security Organisation (ECSO). What importance does EU Commissioner Günther Oettinger – one of the main architects of the digital single market – ascribe to the IT security industry?

The European single market has made the free trade of goods possible between EU member states for almost 24 years. Yet the success of the world’s largest economic area to date has, until now, had no equivalent in the digital services and telecommunications markets. In the ICT industry, the member states have been largely playing by their own rules. However, the fragmentation of the industry into individual markets represents a significant obstacle in Europe’s race to catch up with other economies that are already leaps and bounds ahead in digital technology – most notably the USA.

The sitting European Commission now plans to change this. In May 2015, it presented a strategy for a digital single market in Europe for which several measures had already been implemented. EU Commissioner Günther Oettinger is one of those responsible for the project.

Without IT security, there can be no digital growth. In order to promote this important sector, a cPPP (contractual Public Private Partnership) was concluded as part of the new cyber security strategy between the European Commission and the newly founded ECSO on 5 July 2016. This partnership
In interview:

Günther H. Oettinger has been the EU Commissioner for the Digital Economy and Society since 1 November 2014. He was appointed EU Commissioner for Energy on 10 February 2010 and was Vice President of the European Commission from 1 July to 31 October 2014. Previously, Oettinger was Prime Minister of Baden-Württemberg from 2005 to 2010 and has been a member of the state’s parliament since 1984. He is also a member of the Presidium and Executive Committee of German party CDU.

EU Commissioner Günther Oettinger on Cyber Security in Europe

How would you assess the current European – and German – IT security industry?

Oettinger: Let me start with the good news. The European cyber security industry has a lot of potential. Besides a range of established market players, we also have a large number of SMEs that are bringing new and creative cyber security solutions to the table. This sector is marked by intensive innovation, both in niche markets like cryptography as well as established markets with new business models, like anti-virus programs.

At the same time, the European cyber security market is highly fragmented geographically – which in some ways reflects its original proximity to the defence sector. Companies can therefore find it very difficult to expand beyond their national markets.

This is also the case in Germany. A big reason for this is the lack of trust in cross-border solutions. As a result, companies have to fight to achieve the economies of scale that would make them more competitive both in the single market and worldwide. Furthermore, this leads to a variety of mergers and acquisitions through non-European investors. A positive aspect of this trend is that it proves European cyber security companies are skilled at innovation. However, Europe is also running the risk of losing European knowledge and expertise, because its skilled workforce is emigrating.

As the global cyber security market is expected to be the fastest-growing segment in the ICT sector, this presents an enormous opportunity that we cannot miss. In my opinion, it is vital that we take action to

is the result of extensive planning by a dedicated steering committee. Gerd Müller of secunet’s international sales team has been there from the beginning. As a representative of Bundesverband IT-Sicherheit e.V. (TeleTrusT), he was a member of the committee and a major contributor both to

the founding of ECSO and the conclusion of the cPPP. Today, also on behalf of TeleTrust, he is Vice Chairman of ECSO. As a founding member of ECSO, secunet is also part of the public-private partnership.

is the result of extensive planning by a dedicated steering committee. Gerd Müller of secunet’s international sales team has been there from the beginning. As a representative of Bundesverband IT-Sicherheit e.V. (TeleTrusT), he was a member of the committee and a major contributor both to

the founding of ECSO and the conclusion of the cPPP. Today, also on behalf of TeleTrust, he is Vice Chairman of ECSO. As a founding member of ECSO, secunet is also part of the public-private partnership.
promote a more integrated market for cyber security products and services, which will help European companies to achieve growth and success while paving the way for European citizens and organisations to access practical and affordable solutions.

What is the importance of cyber security within the digital single market initiative?

Oettinger: I am convinced that there can be no digital single market without trust and security. Cyber incidents in Europe cause enormous economic damage every day, which affects businesses large and small as well as the economy in general. This undermines the trust of citizens and companies in the digital society. A recent survey revealed that in 2015, at least 80% of European companies were the victims of one or more cyber security incidents – and the number of security incidents across all global sectors rose by 38%.

This is why cyber security is one of the pillars of our strategy for the digital single market. Europe must be ready to counter cyber threats that are becoming increasingly sophisticated and that recognise no borders. For this, we need top-quality, affordable and interoperable cyber security products and services. This is an enormous competitive opportunity for our cyber security industry in a fast-growing global market.

What concrete measures are planned for the near future?

Oettinger: In July this year, we gave the green light for a public-private partnership for cyber security in order to stimulate competition and innovation in the European cyber security industry. The EU has earmarked EUR 450 million for this partnership from its Horizon 2020 research and innovation programme – and cyber security market stakeholders that are represented by the European Cyber Security Organisation (ECSO) are expected to invest three times this amount. The partnership also includes representatives from national, regional and local public
I was delighted with the industry's support and commitment to the initiative and their representatives' hard work on an ambitious research and innovation agenda. During the preparatory phase, it was demonstrated that trust can be built and that a dialogue between the various stakeholders can boost this trust.

In addition, the Commission proposed a number of other measures to stimulate the European cyber security market in July of this year. Among other things, we plan to investigate the possibility of a European certification framework for ICT security products. Certification plays an important role in building trust and security in products and services. The lack of interoperable solutions (technical standards), procedures (procedural standards) and EU-wide certification mechanisms is one of the current deficiencies affecting the single market in the area of cyber security.

In the scope of national initiatives, we can see that high cyber security requirements are being determined for ICT components for conventional infrastructures, including certification requirements. These are important, but must not lead to the fragmentation of the single market and interoperability issues. Providers of cyber security solutions currently have to go through various certification procedures in order to offer their products and services in several member states, which is counterproductive.

In addition, we want to facilitate access to funding for smaller cyber security firms and hope to sound out different options for this as part of the EU Investment Offensive.

Last but not least, I'd like to remind you that we passed the first piece of European cyber security legislation – the Directive on the Security of Network...
Dr Luigi Rebuffi is the Secretary General of ECSO and the founder and CEO of the European Organisation for Security (EOS). After having graduated in nuclear engineering at the Politecnico di Milano, he worked on the development of high-power microwave systems for the next-generation thermonuclear fusion reactor (ITER). He continued his career at Thomson-CSF/Thales, becoming Director for European Affairs for the Group’s civilian activities in 2003.

He is a member of the Protection and Security Advisory Group on EU Security Research and President of the Steering Committee of the French ANR for security research.

In interview:

Dr Luigi Rebuffi is the Secretary General of ECSO and the founder and CEO of the European Organisation for Security (EOS). After having graduated in nuclear engineering at the Politecnico di Milano, he worked on the development of high-power microwave systems for the next-generation thermonuclear fusion reactor (ITER). He continued his career at Thomson-CSF/Thales, becoming Director for European Affairs for the Group’s civilian activities in 2003.

He is a member of the Protection and Security Advisory Group on EU Security Research and President of the Steering Committee of the French ANR for security research.

The cPPP contract was signed in summer 2016. What are ECSO’s next steps towards implementation?

**Dr Rebuffi:** Six working groups have already begun working to support the cPPP and the development of a European cyber security market through various industrial policy activities. In addition, we want to establish trust and a dialogue between the various stakeholders involved in cyber security in Europe – whose interests can sometimes vary widely. We therefore need to find common objectives, without degrading ambitions.

In the short term, we are providing the Commission and member states with suggestions for priorities for the 2018-2020 research programme Horizon 2020. These priorities are established taking into account the need to provide Europe with concrete solutions to evolving threats and protect the main European economic sectors (manufacturing, Industry 4.0, transport and logistics, etc.) against cyber threats and a loss of image.
How many members are currently involved in ECSO and where do they come from?

**Dr Rebuffi:** ECSO’s membership grows every week. We currently have 171 members. Before the organisation was founded, it would have been optimistic to have hoped for 150 members by the end of 2016. We are now well beyond that target. This demonstrates the enormous interest that the cPPP and ECSO have generated in Europe – and also shows that cyber security is considered to be one of the most important challenges for society and the economy today. Our current members come from 27 countries.

What would you like to have achieved with ECSO by 2020? Have you set yourself a personal goal for ECSO?

**Dr Rebuffi:** When we created the cPPP and ECSO, it soon became clear that time moves faster in the world of cyber security. Usually it takes one or two years to set up a cPPP, but we managed it in just four months, because the requirement was to complete it by summer. We initially based other objectives on ‘Brussels time’, but again our timetable has been dramatically shortened. We’ve therefore learned that in cyber security it’s almost impossible to define long-term objectives, as needs often arise earlier than expected and new goals come to the fore in just a few years. We need to be reactive and flexible.

Europe is still lagging behind on certain cyber security issues and our goal for 2020 is either to hold our position – which would be a success in itself, as markets are growing faster outside of Europe – or to improve our competitiveness and become global leaders in certain areas, e.g. securing the Internet of Things, cryptology and safeguarding Industry 4.0.

As a personal goal for ECSO, I would hope that by 2020 we’ll have established effective cooperation between all the main stakeholders in Europe. ECSO should be recognised, both in Europe and elsewhere, as one of the main focal points for cyber security.

“When we created the cPPP and ECSO, it soon became clear that time moves faster in the world of cyber security.”

In this context, by 2020, I would be pleased to see national public-private structures emerge that are dedicated to cyber security and promote the knowledge and activities we are currently driving forward at the European level both locally and regionally.

Finally, I would like to thank secunet for its active role in the process and Gerd Müller for his valuable work as a representative of TeleTrusT, both during the preparatory phase and now as a Vice Chairman of ECSO. I am sure that with our combined efforts, we will drive forward cyber security in Europe.
SDW InterOp 2016
Test Results: Light and Shadow

In May 2016, secunet conducted an interoperability test for electronic machine-readable travel documents (eMRTDs) at Security Document World in London. This was the fourteenth test since the first was conducted in Canberra, Australia, in 2003. Interoperability tests are important to ensure that travel documents and document verification systems are compatible worldwide.

The security standards for electronic travel documents have been updated again since the last test in 2013 and the latest updates were the focus of this year’s tests. These included the PACE-CAM security protocol, which is an extension of the PACE protocol defined by the International Civil Aviation Organisation (ICAO), adding a chip authentication function.

Seventeen document manufacturers and twelve providers of document verification systems took part in SDW InterOp 2016. In total, 27 sample documents were used to test the interoperability of the participating verification systems. Further tests were carried out by two independent test laboratories using secunet’s Golden Reader Tool (GRT). The overall results were positive: the sample documents passed 98% of the 8,502 test procedures. The quality of the documents can therefore be considered to be excellent.

However, the tests also revealed some shortcomings. For instance, they showed that there is room for improvement concerning passive authentication. This process helps to confirm the authenticity and integrity of the data held on a travel document’s RF chip. The test revealed that around 50% of the document verification systems failed to correctly perform passive authentication. A fake certificate used as part of the test was not recognised as a forgery in these cases. The manufacturers of document verification systems will therefore have to make some adjustments.


More information:
Matthias Niesing
matthias.niesing@secunet.com
The Czech Border Police are enhancing their border control systems. By implementing a secunet Document Verifying Certification Authority (DVCA) as a new component in their background system for electronic identity documents (eIDs), the Czech authorities will be able to fully verify eIDs at all national border control points in the future. The project was successfully implemented in just three months, as the new component could be smoothly integrated into their existing infrastructure.

The solution is based on the secunet eID PKI Suite. The new DVCA module allows the customer to read data from eIDs that are protected by the EAC protocol. To do this, the module provides certificates via a secured channel to the various inspection systems within the overall system – including stationary and mobile inspection devices, as well as the EasyGO automated border control system. Some of these border control systems have been in use since 2006, when biometric documents were first introduced.

In technical terms, the DVCA solution consists of a server supplemented by two further instances: a back-up system at a different location, which is deployed if the primary system fails, and a test instance. Each instance has its own hardware security module (HSM) to ensure that security keys are stored securely.

Another part of the project is a so-called National Public Key Directory (N-PKD) module, which helps the Czech Border Police to handle all the data needed to comprehensively verify identity documents. By establishing a national counterpart to the ICAO PKD, the benefits of this central PKD can be exploited fully.

The project is still ongoing; a comprehensive registration and certification process for mobile document readers is currently being developed.

More information:
Petr Vyletal
petr.vyletal@secunet.com
Cyber Security: A Requirement for Successful Digitalisation

By Arne Schönbohm, President of the German Federal Office for Information Security (BSI)

Digitalisation has now touched virtually all areas of our lives. In public administration and the service sector, we already work with IT-based processes and are highly networked. Meanwhile, Industry 4.0 represents fundamental change in the manufacturing industry. Smart homes, mobile working, e-health and developments like driverless cars are further examples of advancing digitalisation, which presents many opportunities, as well as a number of risks. Cyber security has therefore become a major factor in the success of new technologies.

Digitalisation brings with it significant social and economic benefits. However, it also presents challenges, such as the prevention, detection and neutralisation of digital attacks, which are increasingly being launched by professional hackers. In spring 2016, for instance, the IT systems of companies, municipalities and critical infrastructures like hospitals were successfully attacked with ransomware. The perpetrators were therefore able to encrypt files in an attempt to extort those affected.

A BSI survey on German industry’s experience of ransomware revealed that one in three (32%) companies surveyed had been affected by ransomware. In some cases, the impact was considerable. While 70% of companies indicated that individual workstations were affected, one in five companies (22%) suffered major IT infrastructure failure and 11% lost important data.

Ransomware incidents have revealed just how vulnerable our digital society is. In fact, the attackers are often one step ahead of the defenders of IT systems; they can reach their target easily over the internet and use a number of different methods to disguise their point of attack. In addition, the complexity of today’s information technology of-
ders a large number of possible attack vectors. The attackers don’t simply exploit new and unknown vulnerabilities; they also benefit from the fact that users tend to drag their feet when it comes to installing updates and patches.

Ransomware is a negative example of the abuse of cryptographic methods by criminals. However, cryptography is and will, for the foreseeable future, remain key to the efficacy of many IT security mechanisms. The German government’s Digital Agenda outlines the goal of making Germany ‘the world’s number one in encryption’ to protect citizens, the economy and the government against spying and communication tampering. This goal is the focus of the BSI’s work. In general, current cryptographic mechanisms offer excellent security guarantees and it is very unlikely that the latest cryptographic systems can be broken. However, this could change with the development of the universal quantum computer. For this reason, the BSI is already thinking ahead to the post-quantum era and developing quantum computer-resistant public key processes.

Creating cyber security

Among other things, the BSI has spent years building and proving its expertise in protecting the German government’s networks by preventing, detecting and responding to sophisticated cyber attacks and IT security incidents. We also make this knowledge available to other entities such as regional authorities.

Thanks to the IT Security Act of 2015, the role of BSI as a centre for cyber security has been underlined for German industry, in particular. As expanding operational duties have led to increased authority and responsibilities, the BSI’s duty to do justice to these responsibilities has also grown. As a national

Arne Schönbohm became President of the German Federal Office for Information Security (BSI) in February 2016. Schönbohm studied international management in Dortmund, London and Taipei. Schönbohm held various positions at EADS before joining the Board of cyber security consulting firm BSS BuCET Shared Services AG in 2008.
cyber security authority, we have therefore adopted a distinctly cooperative approach to shaping the digitalisation of the state, economy and society.

In critical infrastructures, the BSI is cooperating with CRITIS operators as part of the CRITIS implementation plan (‘Umsetzungsplan KRITIS’, UP KRITIS). The main goal of the 400-strong UP KRITIS group is to maintain the unrestricted supply of essential services in the digital era. In order to provide authorities and critical infrastructures with on-site cyber defence, the BSI is currently forming mobile incident response teams (MIRT).

It is also driving bilateral cooperation with the business community through the Alliance for Cyber Security, which counts more than 2,000 institutions among its members. The Alliance promotes the intensive exchange of information on threats and security safeguards, including BSI reports on IT security incidents, as well as warnings of attacks and the development of practice-oriented recommendations by the BSI for relevant economic actors.

The developments triggered by digitalisation are sweeping and will fundamentally change Germany – meaning information security is vital to making digitalisation a success. The BSI will therefore continue to shape information security going forward in order to contribute to the successful digitalisation of the state, economy and society.

Report on the current state of IT security in Germany

The Federal Office for Information Security’s (BSI) 2016 report on the current state of IT security in Germany provides information on the type and extent of key IT threats and the resulting risks. The report is based on information analysed by the BSI relating to weaknesses and vulnerabilities in current information technology, as well as to attacks on IT systems and networks.

Download: https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html
ELSTER: Security for a Successful Model of E-Governance

Does Germany have any catching up to do in e-governance? Not when it comes to tax administration. ELSTER has digitalised Germany’s tax process from the bottom up and its scope is constantly being expanded. Over the last year, 20 million income tax declarations were processed electronically. One of the requirements for this success is high standards of information security. There has been a close cooperation with secunet since ELSTER was launched in 1999.

ELSTER is a joint e-government project involving the tax administrations of all German states and the federal government under the aegis of the Regional Tax Authority of Bavaria, based in Munich. The project aims to achieve the efficient, modern, media-independent and highly secure electronic transfer of tax information between citizens, tax consultants, employers, municipalities, associations, tax officials and other institutions.

All those involved stand to benefit. Digitalisation has simplified the tax process, which helps to reduce the workload of citizens, companies and tax administrations, while also minimising the costs of bureaucracy. As a centralised, nationwide infrastructure, ELSTER is available for use around the clock, 24/7.

ELSTER operates something called the ‘Zentrale Produktionsstätte (ZPS) ELSTER Kommunikation’ – or central production facilities – for the electronic transfer of different tax information via the internet. This includes all transport and communication programmes, as well as systems for data provision and data retention, authentication, authorisation management and encryption/decryption.

Certification according to ISO 27001
ZPS ELSTER Kommunikation processes and transfers citizens’ sensitive personal information, resulting in extremely high information security requirements. In particular, the confidentiality, integrity and non-repudiation of the transferred information must be guaranteed. In order to document its compliance
with this requirement, the Regional Tax Authority of Bavaria applied for certification according to the ISO 27001 standard based on the Federal Office for Information Security's (BSI) IT Baseline Protection in 2007. After doing so, it tasked its long-term partner secunet with establishing ELSTER’s eligibility for certification.

This required the development of an information security management system (ISMS), so secunet was made responsible for devising, implementing and operating the system, dubbed the ElsterISM. Certification was granted in 2008 and remains valid today subject to annual reviews and audits. The certification confirms that IT security is integral to the philosophy of the tax authority.

**Identifying, registering and authenticating users**

Alongside protecting data transfers, the authentication of users is another vital aspect of ELSTER’s security. Section 87a of the German tax code stipulates that an additional security procedure must be permitted alongside qualified electronic signatures to authenticate senders’ data and guarantee the integrity of the electronically transmitted datasets. ELSTER implemented this in cooperation with secunet based on a service developed in 2004 to issue certificates: ELSTER Trust Center. This service handles secure identification, registration and authentication for the ELSTER online portal.

Since 2012, users have been able to use their eID cards for authentication. In addition, secunet developed and implemented an authorisation management protocol for the administration of registered identities. Consequently, ELSTER meets all the cryptographic requirements of the BSI’s Technical Guidelines for the protection of confidentiality and integrity.

**Constant change, constant modernisation**

As ELSTER is being continually developed, its security technology needs are also in constant flux. secunet acts in an advisory capacity. This includes evaluating new technologies and implementing proof-of-concepts, as well as checking, devising and implementing organisational and technical concepts while ensuring compliance with all relevant security requirements.
A successful e-government application must strike a balance between security and user-friendliness. Together, ELSTER and secunet are showing that implementing an ambitious security architecture doesn’t mean sacrificing user comfort – and that this technology can also be implemented efficiently for operators.

More information:
Michael Gebauer
michael.gebauer@secunet.com

The Future of ELSTER

Mr Krebs, what security challenges is ELSTER currently facing?
For a few years now, we have witnessed a significant shift in the field of technology dubbed the ‘digital revo-lution’. New authentication methods are continually being developed and launched, and we want to – and must – validate these for possible use with ELSTER.

Our particular focus here is the use of ELSTER on mobile devices. Thanks to their prevalence today, modern technologies like mobile communications are taken as a given. In addition, they are vital to social inclusion; there are people who don’t have access to a computer, but do own a smartphone. This has also led to a change in ELSTER users’ requirements. We have to take this development on board and offer state-of-the-art technologies, while also meeting the highest possible security requirements.

What are the key criteria for future-proof authentication?
When we integrate new technologies, we must equip them from the start with components and interfaces that will allow us to integrate them into universal, multifunctional solutions later on. Likewise, new approaches to authentication must always be devised taking into account quality of use, for which the criteria are efficacy, efficiency and user satisfaction.

Privacy and personal data protection are basic requirements for every citizen to live a self-determined life. This is and remains the primary aim of authentication – to ensure that citizens are afforded effective protection against current and future attacks.

In interview:

Roland Krebs has run the Regional Tax Authority of Bavaria’s Information and Communication (16) unit since 2015. In 1996, he was a process manager for ELSTER. In this role, he was responsible for implementing the ELSTER process as part of the overarching KONSENS initiative at the national and regional levels. The cooperation between the government and the 16 German federal states is founded on the principle of ‘one for all’. This means that specialised fiscal procedures and the corresponding software are developed and implemented in all 16 federal states under the leadership of one.
Smart yet Secure: Safeguarding Agriculture 4.0

The networked agricultural economy has been a reality for some time. Agricultural machinery manufacturer CLAAS aims to drive this development forward and places significant importance on security.
The agricultural revolution that has long been discussed has finally become a reality; agricultural machines can now communicate digitally with each other, with an IT back end or with an IT system in the cloud. Sensors can now deliver data on the condition of the earth, seeds and crops. And in ‘precision farming’, the machines can even analyse subtle differences in the soil across a single field, allowing farmers to exploit this information through optimised management. The main motivation for this development is the prospect of significant gains in yield and efficiency.

The Westphalian town of Harsewinkel is home to CLAAS, one of the key drivers of networked agriculture. The global manufacturer of agricultural machinery currently employs 11,500 people and is the European leader in combine harvesters and the global leader in self-driving field choppers.

Mr Böck, CLAAS has a lot of investments lined up in digital agriculture. What are you planning specifically?

Böck: In July, we laid the foundations for a new electronics development centre in the town of Dissen in southern Lower Saxony. This is where our subsidiary CLAAS E-Systems – founded in 2014 – does its work. Today, more than 150 members of staff are developing control units, electronic architectures, terminals, camera systems, satellite-guided steering systems and more. It is our aim to become a technology leader and driver of digitalisation in the agricultural industry.

CLAAS plans to introduce new technologies in order to offer new networked added-value services for farmers. In particular, we want to connect process chains to support application scenarios like parallel driving or digital fleet management. In addition, technologies we’ve worked with for a long time – like telemetry – can be used in new application scenarios when combined with modern technology like mobile 4G or 5G data transfers. Another example is software updates over the air, which can offer farmers greater added value.

What role does security have to play here?

Böck: Our aim of achieving technology leadership necessarily implies the need to give as much attention as possible to the protection of networked systems. The involvement of different parties –

In interview:

Thomas Böck has been a member of the CLAAS Group’s Board since October 2014, where he is responsible for technology and systems. He has worked for the CLAAS Group since 2006 and has held a number of different management positions.
including manufacturers, clients and solution providers – is reason enough to make comprehensive security management a priority, as this enables us to protect machines against attacks via wireless interfaces and safeguard customer data in every situation.

To achieve this goal, CLAAS launched the Security@CLAAS project two years ago.

Please tell us a bit more about the project.

Böck: Security@CLAAS aims to offer complete protection against unauthorised manipulation for different use cases, while safeguarding confidential data. Its holistic approach takes into account the complete lifecycle of the machines (development, manufacture, after sales), the various use cases, and all possible users and systems.

Under the project, CLAAS’ specialist divisions will have access to cryptographic methods and security measures in the form of guidelines that can be applied generically to different scenarios. We are also defining and introducing procedural responsibilities in order to establish a universal security management concept.

With Security@CLAAS, cyber security has become a company-wide issue that is no longer the preserve of IT specialists; in fact, it is tackled head-on by all company divisions. This principle initially required a change in thinking across the company, but we managed to implement the transition successfully.

Following a selection procedure for an external partner to implement the project, CLAAS hired secunet. The key criteria underpinning this decision included secunet’s experience of working on comparable projects in the automotive industry. From the very beginning, secunet helped to design a security concept in close coordination with the CLAAS security team.

In the first stage of the project, secunet devised a security standard for CLAAS that forms the basis of each additional step towards the launch of a dedicated security management system.

More information:
Alexander Kruse
alexander.kruse@secunet.com

secunet in the automotive industry

secunet Security Networks AG has designed and implemented IT security solutions for almost 20 years. The automotive industry recognised this expertise early on and has integrated it into its own research and development since 2001. In 2007, secunet created a new company division dedicated exclusively to the needs of the automotive industry, making secunet an ideal partner when it comes to solutions for the modern, series-production vehicle. The company supports OEMs and suppliers in devising and implementing innovative security solutions – both within the on-board network and for connections with external services and systems. secunet also assists its clients by detecting critical security vulnerabilities through penetration tests, drafting specification sheets, and implementing and launching production-ready, back-end solutions.
OUR AIM
YOUR SUCCESS

CUSTOM SOLUTIONS
HMI PLATFORMS
EMBEDDED COMPUTING TECHNOLOGIES
National

eIDAS: an Easy Upgrade to Trust

The eIDAS Regulation is making digital business communications trusted and verifiable across the EU – while also being incredibly easy to implement thanks to trust service providers. What are the most important changes for businesses and public authorities compared to the German Digital Signature Act?

Help is now at hand in the form of EU Regulation 910/2014 (Electronic Identity and Signature – eIDAS), which entered into force in the summer. Alongside electronically identifying your communication partner, it is now possible to make binding, certifiable agreements using new trust services. These services, which are briefly introduced below, are designed to be used alone or as a package. Thanks to uniform regulation across the EU, eIDAS will significantly boost the trustworthiness of the digital internal market.

Remote signatures
Has Germany not had a solution like this – the electronic signature – and even the Digital Signature Act for some time? It is true that this national law enables us to use mathematical procedures and sophisticated technologies to confer binding legal force on electronic documents. However, instead of a solution, users only had access to a technology with which they could independently create their
own, trusted communications. For many users this was overwhelming, as this technology is often not very straight-forward. The eIDAS Regulation provides the foundations for a solution-oriented service for trusted communications, whereby trust service providers take care of the technical side of things and thus unburden users. Now, trusted digital communications will be simple and easy to implement for the first time.

A seal for organisations
Even before eIDAS, mass signature procedures offered proof of authenticity in output management and led to measurable cost savings and a rationalisation effect. Consequently, recipients could verify bank statements, certificates, documents, official references and invoices using electronic signatures. Until now, a signature of this kind was assigned to a natural person, such as a system operator. However, in the case of bank statements, for instance, assignment to an individual sometimes leads to questions, as assignment to a banking institution is expected instead. Under eIDAS, electronic seals can be assigned to the issuer, in this case the banking institution. Meanwhile, organisations can use an eIDAS seal in their own name to make a certificate verifiable using the electronic seal. The probative value of a seal like this is enhanced using a ‘qualified seal under eIDAS’.

When it comes to mass signature procedures, secunet recommends switching to qualified seals in order to avoid headaches for recipients. However, previous mass signature procedures are still secure, so it is possible to make the switch when your respective signature certificates expire.

Remote seal
It is also possible to use a combination of the remote signature and remote seal. A remote seal is ideal for organisations that do not wish to operate their own mass seal procedure, but want to retrieve the seal...
from their applications as needed. With this solution, the document does not have to leave the organisation to create a seal. Instead, it is sufficient to exchange a cryptographic checksum, which prevents any conclusions from being drawn regarding the document’s content. This kind of data protection concept by design minimises the data volumes to be transferred by a factor of up to 1,000, thus saving additional costs while guaranteeing enhanced performance.

**Time stamp**
As was the case after the Digital Signature Act, qualified time stamps can also be integrated into electronic business processes as trust anchors for the legal time under eIDAS. Qualified time stamps can serve as proof that a deadline has been observed, for instance. They are already proven for this application and are therefore also available under eIDAS.

**Delivery services**
In Germany, delivery services such as e-Postbrief and De-Mail are well-established under the technical guidelines of the German Federal Office for Information Security (BSI). These delivery services are also recognised under eIDAS, whereby their current offerings are supplemented by a time stamp.

**Archiving services**
When an electronic business process is concluded and all electronic documents have been exchanged, there may – depending on the transaction – be a requirement to store such documents over the long term. Besides guaranteeing the readability of various data formats, the cryptographic processes used must be adapted to the then current requirements. In Germany, these are described in another of the BSI’s technical guidelines: TR-ESOR. In the future, there will also be service providers that offer archiving services under eIDAS.

**Summary**
Essentially, eIDAS makes it possible for users to easily create trusted, verifiable electronic business processes across the EU for the first time. Meanwhile, the complexity of the underlying processes is handled by qualified trust service providers. When creating a seal, the organisation must either operate a seal machine or use a remote seal provided by a trust service provider.

secunet offers consulting and numerous other services related to eIDAS – whether customers wish to use trust services or offer their own.

**More information:**
Roland Krüger
roland.krueger@secunet.com
secunet Takes on the HJP Consulting eID Testing Business Unit

Secunet is expanding its core competencies in the Homeland Security division. To do so, the company is acquiring a business unit from HJP Consulting, based in Borchen, North Rhine-Westphalia. With this partial transfer of operations, secunet will be taking on experts in electronic identity documents (eID). The staff from this unit of HJP Consulting will provide extensive expertise in the safeguarding and review of eIDs, allowing them to supplement the activities of the Homeland Security division.

Furthermore, secunet will be adding GlobalTester to its range of test software. This product is used to comprehensively review the compliance of chip cards and, in particular, eIDs, as well as the corresponding readers. This means that two globally recognised test suites for eIDs will be bundled at secunet in the form of the secunet Golden Reader Tool and GlobalTester.

New secunet Showroom in Essen

Visitors to secunet’s head office in Essen will soon be able to form an even better picture of the company’s wide range of services. The new showroom contains examples of current hardware components. The application scenarios for each piece will be explained with presentations by secunet employees. In addition, a fully functional eGate will allow visitors to thoroughly test automated border control technology. In the future, the presentation will be rounded out by a selection of historical encryption devices.
Automated IT Baseline Protection

Modern-day police work would be inconceivable without high-powered information technology, which is why the German Federal Police has one of the largest IT infrastructures of all German police forces. The security authorities are now meeting their obligations to IT baseline protection with an automated solution that significantly reduces the associated administration while boosting security.

Pursuant to the German Federal Cabinet’s 2007 ‘implementation plan to guarantee the federal administration’s IT security’ (‘Umsetzungsplan Bund’, UP Bund), the German Federal Police must establish a so-called IT security concept based on IT baseline protection for each administrative procedure, taking into account the requirements of the German Federal Office for Information Security (BSI). On one hand this is logical, as security authorities naturally have to have high information security requirements. On the other hand, the German Federal Police operates a highly complex IT infrastructure boasting around 250 administrative procedures at various locations. It soon became clear that the development and maintenance of the necessary security concepts could not be achieved in the traditional manner and using existing resources.

As a result, the German Federal Police opted for a new approach – a solution that would enable it to complete a largely tool-supported implementation audit of security measures and create relevant IT security concepts. In secunet, it found a partner that is well-suited to co-developing a concept like this thanks to its years of project experience in IT baseline protection. Since the project development phase started in 2014, secunet has been responsible for technical consulting, guaranteeing BSI conformity and quality assurance. Another partner, Hewlett Packard Enterprise, has provided assistance with system design and integration.

In order to make automated implementation auditing possible, the security requirements for IT infrastructure needed to be highly standardised. This means that security measures are no longer separated for each administrative procedure. Instead, they have been uniformly been standardised, implemented, audited and documented for the German Federal Police’s entire information network. This will result in a secure core IT system comprising mainly standardised components that can be used for a variety of administrative procedures.
Another key aspect of automation is modularisation, whereby security modules (SiM) are used instead of the usual IT baseline protection ‘components’. Just like these components, the SiM model the target objects of the IT network – including systems, applications, and network and infrastructure elements – and allocate the designated security measures to them as necessary. However, the measures cited in the IT baseline protection catalogue will also be supplemented with other measures based on manufacturers’ and other best-practice recommendations, thus fulfilling even higher protection requirements. In addition, the SiM are much more detailed than the baseline protection components and also outline the respective implementation audits for each measure. The result is a tool-supported basic security check for implementing the security measures.

This automated implementation audit is conducted using the Symantec Control Compliance Suite (CCS), which collects and evaluates relevant information from the systems and applications based on the requirements of the SiM. As these technical checks can only be conducted for a selection of the measures, they are supplemented by web-based multiple choice surveys that are completed autonomously by the competent staff (e.g. system administrators). Compared to conventional implementation auditing methods, which involve interviews and inspecting the system configuration, this yields considerable savings in time, costs and resources. At the same time, a detailed audit can provide a significant boost to security.

The central administration of all information regarding target objects and security measures, as well as the automated creation of security concepts, is achieved using a new software product from secunet: the security management database (SMDB). On one hand, this imports information from the CCS on the target objects and the implementation status of the security measures. On the other hand, it makes it possible to enter and maintain all other data on the administrative procedures via a userfriendly web interface – including allocation of the target objects to the respective IT network, network plans, communication links, and risk analyses.

The pilot phase of the new solution has already begun. Each component is being gradually integrated into the system before the solution goes operational next year. The initial results look positive: during an administrative procedures audit based on ISO 27001 (according to IT baseline protection), the auditor noted significantly improved security levels and gave positive feedback on the concept of automated baseline protection.

More information:
Mario Tönse
mario.toense@secunet.com
Three Questions for secunet Board Member Thomas Pleines

The cyber threat continues to build every day. According to the latest report from the German Federal Office for Information Security (BSI), around 380,000 new malware programs are detected on a daily basis. As a result, there is considerable demand for the knowledge of cyber security experts. Can you describe secunet’s ideal IT security specialist?

Pleines: Aside from the skills that all IT security experts need to have, it is important to have a global view of IT security in which the customer network and functionality are granted the same high importance. Security without the necessary user awareness and acceptance simply doesn’t lead to the desired results. As we at secunet focus solely on information security, our employees have worked on thousands of customer projects over the years that have helped us to build an in-depth knowledge of security processes. Thanks to this experience, our specialists have a very good feel for what our customers need. When it comes to actually implementing a project, this means that the customer is guaranteed the best possible security with optimum functionality.
BITKOM e.V. has complained for several years now about the current shortage of IT specialists. Is this also an issue for secunet?

Pleines: Of course, employee acquisition has not got any easier in recent years. Nowadays, IT security specialists are not just sought after in the IT industry. Thanks to networking, e.g. through the Internet of Things, IT security knowledge has become essential for all manner of products that communicate digitally – from the car to the oft-cited refrigerator.

However, despite the stiff competition, secunet has still managed to continually recruit new staff. We believe this is thanks to a mixture of characteristics that make secunet a truly unique company. First, secunet has nine offices throughout Germany. This means we offer our employees the opportunity to live and work in the place they have built their lives. It also means that we can take into account people’s changing circumstances. In addition, close cooperation with universities, institutes and professors helps the company to introduce students to the company early on in their careers. We reserve a large number of vacancies for them, whether internships, student jobs, or jobs for bachelor, master or PhD students. This allows the next generation of IT experts to get a profound, early insight into their potential future careers. At the same time, this commitment is an excellent opportunity for us to recruit young employees for the company, who then already know our culture and the way we work. We also offer incentives and excellent growth prospects within the company; management positions are often filled by existing staff, for instance.

How does secunet differ from other companies?

Pleines: I think our overall package is key. Of course, secunet offers the usual industry benefits like flexible working hours, a pension, various health services and regular training. However, we also score points thanks to our unusual, often unique projects. We regularly carry out pioneering work in IT security and are continually set new, bigger challenges. It is very satisfying to overcome these challenges together and this spurs us on to develop new and improved services.

Then there is the active communication we encourage between employees, which fosters a very special company culture. Our excellent working environment is a decisive factor for people when deciding to work for us. Quite simply, our staff feel happy here – and this is confirmed in regular employee surveys. We also boast a below-average staff turnover for the industry. I feel this is an excellent indication that our employees are very satisfied. Ultimately, it is the sum of our parts – great and small – that makes secunet such an attractive employer.
A Secure Authentication Procedure for SNMPv3

The Simple Network Management Protocol is used in global IT infrastructures to control and monitor systems and active network components. Since the first two versions of SNMP were deemed to be relatively insecure – hence the playful interpretation of the acronym as ‘Security is Not My Problem’ – the third version, SNMPv3, was introduced with a whole host of new security mechanisms. As a result, the user-based security model (USM) for SNMPv3 makes it possible to cryptographically authenticate and encrypt messages based on the symmetric keys of (technical or human) users. On behalf of the German Federal Office for Information Security (BSI), secunet devised a new authentication procedure for the USM that was officially adopted as RFC 7860 in April 2016 and thus became a new industry standard.

In the original USM specification (RFC 3414) from 2002, so-called hash-based message authentication codes (HMAC) with 96-bit lengths were used for authentication based on the MD5 and SHA-1 hash functions. Today, these two hash functions are defunct technology. In the context of HMAC, their poor collision resistance, especially regarding the use of digital signatures, is no longer relevant. However, 15 years after the introduction of SHA-2 hash functions, they also no longer offer the highest level of security. In addition, longer MACs are recommended today to guarantee security against brute force attacks in the future.

In order to make SNMPv3 more future-proof, the BSI tasked secunet with specifying new HMAC authentication procedures for the USM based on the currently recommended SHA-2 hash functions and bit lengths between 128 and 384, and submit it to the internet engineering task force (IETF) for standardisation. In accordance with the standardisation processes of the IETF, secunet’s experts and the BSI devised a new internet draft in coordination with the competent working group. As it turns out, there was considerable interest from IETF and software manufacturers in modernising the authentication procedure, meaning the initiative was welcomed and supported by all. Of course, this contributed significantly to the successful conclusion of the project.

More information:
Johannes Merkle
johannes.merkle@secunet.com
En Passant: ICS Attacks

Time and again, minor details often reveal critical system vulnerabilities. Most recently, this was proven during a secunet pen test for industrial control system (ICS) devices that are responsible for a client’s building automation system. In this case, the ‘minor detail’ made it possible to take over the generator control system.

During the pen test, our experts analysed a Windows-based web portal that enabled the control of several ICS systems. This took place in a separate network and the firewall ensured that only the IP address of the web portal was accessible.

Initially, the pen test seemed to show that the portal developers had done a good job and almost no relevant vulnerabilities could be found. Access to the ICS devices was governed by a role-based authentication system, whereby standard users could only read values – not change them – and could not bypass defined switching zones.

The pen test breakthrough came when a bug was found in the web portal’s remote desktop server, which was used to maintain the operating system. The bug had not been adequately patched and therefore allowed logins as a standard user. A first scan through the firewall revealed that you could achieve FTP access (not used by the web portal) on the ICS devices, which made it possible to download the current device control files. Within these files, it was then possible to identify the unencrypted password for further ICS devices, which gradually opened up access to all ICS systems. Attackers would also have been able to upload their own control files to the devices.

As a result of the analysis, the web portal patch concept was updated and the building automation network concept was modified. In addition, the web portal and ICS device networks were separated with an additional firewall. Now only connections used by the web portal can be utilised within the LAN for ICS control. This means it is no longer possible to modify the device control files by taking control of the web portal.

In general, digitalisation leads to the progressive networking of formerly separated systems, which in turn creates security risks. Pen tests help to reveal these vulnerabilities and show how they can be eliminated – a goal that was also achieved in the above case.

More information:
Dirk Reimers
dirk.reimers@secunet.com
SINA Apps: Tailor-Made Applications

Our private and professional lives would be unthinkable without apps. They offer us flexibility and make work and communication easier – and new ones are being released with increasing regularity. The concept of SINA Apps will now allow users to benefit from these features when working with VS-NfD (restricted) documents. SINA Apps can be developed quickly and flexibly for the SINA Workstation in order to meet the unique needs of one or more customers. As they are launched as separate workplaces (or ‘sessions’) in the SINA environment, the apps ensure that classified documents are separated and secure at all times. This also means that SINA Workstation can now be easily adapted to future needs.

Some of the apps that are already available include the SINA App Hotspot, which makes it possible to establish secure connections with your company’s intranet via public hotspots like those in hotels and at conferences. Another example is the SINA App Private Browser, which allows users to freely and securely surf the web without needing to worry about malware gaining access to the entire system. Meanwhile, a SINA Messenger app with P2P encryption and a SINA VoIP app for video and audio telephony are now in the pipeline.

In cooperation with IGEL Technology GmbH, secunet is developing an app that makes the IGEL Universal Desktop Converter thin client software (UDC) available for the SINA Workstation. This app for remote access to virtualised desktops will complement the SINA thin client function and offer additional benefits like support for VMware Horizon, RDP, Citrix and numerous other protocols, as well as extended features for protocols already available for SINA.

Secunet explicitly encourages its customers to share their app wish list; in many cases, the corresponding apps can be made a reality. In the future, the company also plans to allow customers to develop their own SINA Apps via a dedicated framework.

More information:
David Hajok
david.hajok@secunet.com
Greater Speed for Secure Networks

The SINA L3 Box S is an IP-based VPN gateway and a core component in highly secure networks. Thanks to the SINA L3 Box’s various performance characteristics, national and international IT networks of all sizes can be secured without a high cost or time investment. As cryptographic network access points, SINA L3 Boxes are located upstream from server segments. In the S product range with official BSI (German Federal Office for Information Security) approvals (national up to VS-NfD (restricted) and international up to NATO RESTRICTED and RESTREINT UE), the SINA L3 Box S 5G is currently the most powerful model. It connects public authorities and company networks quickly and securely over the internet. With the current software version, the data throughput of the 5G model is up to 5 Gbit/s. The SINA L3 Box is equipped with a range of high-powered network interfaces (6 x 10/100/1000 Cu and 4 x 10000 Mbit XFP) and is therefore destined for use in complex central network nodes.

SINA Workstation Now Also with a Virtualised Smartcard

ecunet has now developed the virtual smartcard as a user-friendly alternative to using a service card with the SINA Workstation. It is used in precisely the same way as a physical smartcard, offers the same content and features as the original, and eliminates the need to plug in a customer token like a service card for guest applications. Allocation and administration can both be handled centrally. It is also easier to use, boosting user acceptance, while the solution maintains the same high level of security. The virtual smartcard is available for use with the SINA Workstation 3.3.6 and is currently going through the approval process for VS-NfD (restricted) applications by the German Federal Office for Information Security.

Hardened Crypto Client with SECRET-level Approval

A crypto client for extreme application scenarios like the armed forces, the new SINA Workstation H R RW11 features a wide range of product improvements compared to the previous SINA Workstation H R RK9 model. The workstation is equipped with a modern Intel® CoreTM i7-3610QE CPU – and with 32 GB of RAM, it offers significantly enhanced performance, especially when running parallel sessions. Another technical highlight is the 15.6" full HD screen. Thanks to its aluminium housing, the device weighs just 6 kg compared to its 8 kg predecessor. In addition, the SINA Workstation H R RW11 boasts a much slimmer design and is sure to impress with a considerably reduced unit height of 54 mm (compared to 79.2 mm in the previous model). The new hardened notebook will be available from summer 2017.
No Chance for Cyber Extortionists

Ransomware (also known as crypto trojans or blackmail trojans) has been on everyone’s lips since the Locky trojan wreaked havoc in February 2016. With this type of malware, attackers encrypt important files on the victim’s computer – and promise to decrypt them upon payment of ‘ransom money’. However, the Federal Office for Information Security (BSI) recommends not giving in to such attempts at blackmail; in many cases your files will never be decrypted.

Today’s ransomware often boasts multilevel design. First, a download component (dropper) is placed on the affected computer – as an email attachment, via security loopholes or active browser content, through cloud storage services or through external storage devices (e.g. USB sticks). Once the dropper is executed, the actual ransomware is downloaded and activated.

But how can you protect yourself against attacks like this when even anti-virus software and firewalls can’t help? One option would be to reduce your online communications to a limited number of trusted pages and to disable active content in your browser. However, these days this isn’t practical, as active content is mandatory for certain applications and it’s rarely feasible to limit internet access. Furthermore, even restrictive configurations like this would not help to protect your system, as droppers can access computers by email or through data storage devices and download the malicious code.

Possible solutions include secunet safe surfer, which is based on the BSI’s remote-controlled browser system (ReCoBS) and ‘browser in the box’ concepts. The software separates trusted internal networks and workstation systems from the internet and only transmits online content as image and audio files. This prevents your browser from downloading malware – and therefore droppers – to your workstation computer.

But what happens if a dropper makes it onto your computer by email, download or an external storage device? In this case, safe surfer ensures that it cannot download malware by separating internet access from the workstation system, thus protecting the user PC from the crypto trojan.

More information:
Jan Leduc
jan.leduc@secunet.com
Shorter Lines at Passport Control

At Frankfurt am Main Airport, the passports of third-country travellers will soon be checked more quickly. Thanks to the secunet easykiosk, airline passengers will be able to complete document checks and have biometric data collected autonomously for identity checks. When they then go to the border control desk, the officer will already have access to all the data collected at the easykiosk, which will speed up passport control considerably.

secunet developed the easykiosk as part of the European Union’s Smart Borders project. The solution contains a passport reader, a fingerprint scanner, a facial recognition camera, an iris scanner and a touchscreen. It also features an intuitive, multilingual user interface to guide passengers through the process. The German Federal Police is set to launch a secunet easykiosk pilot project at Frankfurt Airport at the end of 2016.

More information:
Thomas Schäfer
thomas.schaefer@secunet.com

Packed and Ready to Go

Public authorities often face the challenge of recording the identities of large numbers of people in the field, such as when identifying the attendees of major events, registering refugees at preliminary reception centres, recording visa applications outside of embassies and consulates, and registering voters in developing countries. secunet has now developed a suitcase solution especially for these scenarios, containing everything public authorities need when out in the field – robustly packaged, lightweight and ready for use in just a few minutes.

The solution is based on the SINA Workstation S, which is responsible for the encrypted transmission of personal data. It also includes a fingerprint scanner, a passport reader, a signature pad and a facial recognition camera with an extendable tripod. Boasting incredible flexibility and years of proven applications, secunet biomiddle is responsible for seamlessly integrating the individual components.

More information:
Frank Steffens
frank.steffens@secunet.com
Actively Involved in Cyber Security

No other technology has evolved as rapidly or on as many levels as cyber security. This is why it is discussed in numerous national and international associations across different industries. It is also the subject of ongoing standardisation processes. As a major stakeholder in the German and European cyber security industry, secunet is actively involved in a number of associations, committees and working groups. These include Bitkom e.V., TeleTrusT Deutschland e.V., and the Alliance for Cyber Security. The company was also a founding member of the European Cyber Security Organisation (ECSO) – and you can read more about this in this issue of secuview. In many cases, secunet’s involvement takes place at a personal level, as illustrated by some examples on this double page.

Automotive: Harry Knechtel and Martin Brunner are Involved in Expert Committees

Secunet’s Head of Production Automotive, Harry Knechtel, has already been a member of the German Commission for Electrical, Electronic & Information Technologies’ (DKE) 901.0.115 working group for three years. The working group addresses information security issues for electric mobility. An application rule is currently in the pipeline that will determine what security requirements there are for smart charging that are not already stipulated in the existing ISO 15118 standard. Knechtel also helped to elaborate this ISO standard. In addition, secunet’s Principal for Embedded Security, Martin Brunner, is helping to develop a new international cyber security standard for the automotive industry, for which he is involved in a number of different national and international committees.
Christine Skropke Joins the Board of Directors of AFCEA International

Christine Skropke, secunet’s Head of Marketing, PR & Internal Communications, was appointed to the Board of Directors of AFCEA International (Armed Forces Communications and Electronics Association) for two years in June 2016. She had previously been Associate Director of the non-profit organisation since June 2015. The AFCEA is an association that offers a platform for the military, public authorities and global industry to discuss security topics like cyber security, C4ISR and homeland security.

The association has more than 31,000 members worldwide and secunet currently occupies one of six spots for Europeans on the 50-strong Board of Directors. In addition, Christine Skropke is the first European woman to join the supervisory body.

Find out more at www.afcea.org.

TeleTrusT Board Re-Elected – Dr Baumgart Confirmed as Deputy

At the annual general meeting of the Bundesverband IT-Sicherheit e.V. (TeleTrusT) in Berlin on 25 November 2016, Professor Norbert Pohlmann, Dr Rainer Baumgart, Ammar Alkassar and lawyer Karsten U. Bartels were re-elected to the Board.

Professor Pohlmann was appointed Association Chair, while Dr Baumgart was appointed Deputy Chair. Dr Baumgart has been a member of the TeleTrusT Board since 2008 and has been the association’s deputy chair since 2011.

The general assembly also voted to approve the TeleTrusT Board’s previous composition and distribution of roles for another term. Consequently, the association embodies continuity in an otherwise dynamically evolving industry.

Matthias Keßler Heads Up a DIN Working Group

Matthias Keßler, a team leader for Security Management Consulting at secunet, has led the 1 NA 043-01-27-01 working group of the NA043 DIN Standards Committee on Information Technology and Applications (NIA) since 29 August 2016. The committee meets every six months and currently has 60 members. It works to establish requirements, services and principles for IT security management systems. These include the DIN ISO/IEC 270001 guideline, which governs information security management systems (ISMS). Matthias Keßler also contributed to the recently published German translation of the DIN ISO/IEC 27002:2016-11 standard. He was appointed to his new role by the other members of the working group, succeeding Armin Wappenschmidt, who also works at secunet and was head of the committee for eight years.
it-sa 2016 Achieves Double-Digit Growth

When it-sa 2016 drew to a close, it had broken all previous records. This year, 490 exhibitors from 19 countries and more than 10,000 visitors from Germany and abroad used Europe’s biggest IT security exhibition as a platform for dialogue. it-sa recorded double-digit growth in the total number of exhibitors and attendees, as well as the amount of reserved exhibition space. In particular, this year’s exhibition saw a notable uptick in visitors from overseas, helping to underline it-sa’s role as a major IT security information platform.

secunet also attended the exhibition, where it presented a wide range of products and IT security solutions for e-government, public authorities, critical infrastructures and Industry 4.0 alongside its partners.

Close Cooperation with Industry Representatives

Nowadays, no industry is safe from hacker attacks aiming to facilitate espionage or sabotage. Many potential threats and defensive strategies are similar no matter what industry you are in. However, there are also industry-specific issues and requirements that secunet regularly discusses with clients at dedicated events, which provide a forum for lively exchanges between IT security experts and industry representatives.

On 19 September 2016, for instance, CRITIS operators attended the 3rd Critical Infrastructures Information Security Symposium in Frankfurt am Main, where they learned about security in the era of full connectivity. At the Safety & Security Meets the Digital Medical World symposium on 27 October, experts from secunet and S.I.E. – a leading provider of embedded computing and HMI solutions – spoke with representatives from the health sector about 360° solutions for their industry. Finally, ‘Let the water flow! When hackers are in control’, an IT security workshop dedicated to the water management industry, took place in Essen on 3 November, while the pros and cons of connected vehicles were discussed at the IT Security on Board workshop in Munich on 25 November.
January to June

16 – 18 Jan 2017  »  OMNISECURE 2017 / Berlin, Germany
7 – 9 Feb 2017  »  E-world Energy & Water 2017 / Essen, Germany
13 – 17 Feb 2017  »  RSA Conference / San Francisco, USA
17 – 19 Feb 2017  »  Munich Security Conference / Munich, Germany
19 – 23 Feb 2017  »  IDEX / Abu Dhabi, UAE
21 – 22 Feb 2017  »  European Police Congress / Berlin, Germany
27 Feb – 2 March 2017  »  Mobile World Congress / Barcelona, Spain
14 – 16 March 2017  »  Passenger Terminal Expo / Amsterdam, Netherlands
20 – 24 March 2017  »  CeBIT / Hanover, Germany
4 – 7 April 2017  »  LAAD Defence and Security / Rio de Janeiro, Brazil
7 April 2017  »  IT Security on Board: Automotive Workshop / Munich, Germany
24 – 26 April 2017  »  NITEC / Ottawa, Canada
26 – 27 April 2017  »  AFCEA exhibition / Bonn-Bad Godesberg, Germany
26 – 28 April 2017  »  id4Africa / Windhoek, Namibia
4 May 2017  »  secunet Annual General Meeting / Essen, Germany
16 – 18 May 2017  »  BSI Congress / Bonn-Bad Godesberg, Germany
23 May 2017  »  SINA User Day / Bonn, Germany
30 May 2017  »  SINA User Day / Berlin, Germany
20 – 21 June 2017  »  Future Congress: State and Administration / Berlin, Germany

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

Subscribe to secuview
Would you like to receive secuview on a regular basis, free of charge?
There you can also change your preference or unsubscribe.

Imprint

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

Press Law Representative: Christine Skropke, christine.skropke@secunet.com
Chief Editor, Head of Design and Content: Marc Pedack,
marc.pedack@secunet.com
Design: Agentur für dynamisches Marketing, www.knoerrich-marketing.de

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.

secuview 2/2016  39
A secure workplace.
If it’s got SINA.

SINA Workstation turns every workplace into a secure workplace – no matter where it’s located. The reasons behind it? The sophisticated system platform? Yes. Our secure smartcard technology? Of course. Plus: thanks to completely encrypted data systems and IPsec-protected communication, your data security won’t become a balancing act between being allowed to do, having to do and being able to do. It just works – always. It’s hardly surprising, that SINA has received top-tier approvals by BSI, EU and NATO. What does this mean for you? You can relax, for your workplaces are secure. Thanks to SINA.

IT security „Made in Germany“. www.secunet.com/sina