



“Our biggest challenge was time”

Mohamed Kiwan, CEO of EgyptTrust, on the implementation of a PKI solution for digital identities and signatures



Efficiency without dependence

The sovereign cloud for authorities and administration

Cryptography 2.0

Security against quantum computers



22 Cybersecurity legislation for industrial companies: The path out of the jungle of EU cyber regulation

National

- 4 The sovereign cloud for authorities and administration: Efficiency without dependence

International

- 8 Public Key Infrastructure: “Our biggest challenge was time”
- 10 Combating identity fraud at border control: Poor chances for morphs

Technologies & solutions

- 12 Security against quantum computers: Cryptography 2.0
- 15 Biometrics and artificial intelligence: Fairness, robustness and security for AI

Perspective

- 18 Connected and autonomous driving: “We need a public discussion on how much automotive cybersecurity is worth to us”

Guidelines & standards

- 22 Cybersecurity legislation for industrial companies: The path out of the jungle of EU cyber regulation
- 25 Information security management: The maturity model – ISMS taken a step further

News in brief

- 28 Healthcare: Service providers have a choice when it comes to TI access
- 29 Help with IT incidents: Cyber attack – now what?
- 30 Social Days: Taking responsibility together

Service

- 31 Dates – September to December 2023
- 31 Imprint

Interview with automotive cybersecurity expert Manuel Wurm: “We need a public discussion” **18**



Dear readers,

The exciting thing about the IT industry is that it is constantly renewing itself. We are currently facing a series of IT revolutions that will change all of our lives – for example, artificial intelligence (AI), the cloud transformation or autonomous driving. The exciting thing about secunet is that, as a cybersecurity company, we have the opportunity to play a part in all of these upheavals in one form or another.

This certainly applies to the cloud transformation, which has been noticeable in private and business everyday life for some time, but has so far stopped at the important area of public administration for security reasons. This is changing with the sovereign cloud offerings that are currently sprouting up in Germany. secunet is driving the change to a secure cloud and is investing to place its own very special offering in this market. Norbert Müller, who is responsible for secunet Cloud Solutions, explains what is so special about it in this secuvie.

Among the much-discussed changes that AI will bring are its applications in homeland security. These present not only great opportunities, but also challenges. Statistical biases in the data basis of AI models used for security purposes can have serious consequences, for example by the AI favouring or disadvantaging certain groups of people. In the current issue, we describe an approach that counteracts such a scenario.

On the road to autonomous driving, it is not only the vehicle itself that is changing. Already today, progressive networking means that we have to look at the entire, increasingly digital transport infrastructure from a cybersecurity perspective. Automotive cybersecurity expert Manuel Wurm talks about this paradigm shift in an interview.

Finally, cryptography is undergoing a profound change that, despite its far-reaching implications, is rarely discussed beyond the professional community. In response to the capabilities of future quantum computers, cryptography must reinvent itself – also to ensure the continued security of state secrets. This is another topic covered in the current issue.

With all this change, secunet will continue to stand for the best possible protection of digital infrastructures, data and applications. On this basis, we are prepared for every IT revolution.

I hope you enjoy reading this issue!



Axel Deininger



The sovereign cloud for authorities and administration


Efficiency without dependence

The digitisation of the administration will only be viable if it combines efficiency, sovereignty and security. This is especially true for cloud transformation, which is currently at the top of many German public authorities' agendas. Since the large hyperscalers' cloud offers often leave questions about transparency and data protection unanswered, there is a great need for cloud solutions "made in Germany". These are intended to combine security and digital sovereignty.

secunet is currently building an ecosystem of trustworthy solutions and services that enable cloud use even in security-sensitive areas and can also be combined with solutions from hyperscalers. In this interview, Norbert Müller, who is responsible for secunet Cloud Solutions, talks about the meaning and purpose of the sovereign cloud, the role of open source and the newly founded industry association ALASCA.

Mr Müller, why are public authorities striving for the cloud in the first place?

Norbert Müller: In private life and in the business world, digital processes are already part of everyday life and are predominantly based on applications that run in the cloud. Authorities and administrations have so far remained largely excluded for security reasons. But they also want the flexibility and efficiency that new cloud services bring. This will enable them to set up their IT in a more agile way and thus meet the great digitalisation pressure that is weighing on German authorities: Processes are to be accelerated, and citizens and companies also want more digital services. But the challenge remains that public authorities cannot compromise on security when it comes to cloudification. Personal and tax data are highly sensitive and must be completely protected. This applies all the more to classified information. Last but not least, there is the issue of digital sovereignty.

Norbert Müller,
Vice President Cloud
Solutions, secunet 



Why does the cloud for public authorities have to be not only secure but also sovereign? Is digital sovereignty perhaps a mere buzzword, as some observers think?

The value of digital sovereignty becomes clear when you imagine the opposite, namely digital dependency – for example, on certain providers that make it difficult to switch to another provider, or on the internationally dominant IT companies. The latter can become problematic, for example, when providers operate under US legislation with at least unclear influence on data security. For these and similar reasons, traditional cloud solutions, such as those offered by hyperscalers, often did not meet the requirements of authorities and security-sensitive companies. Sovereign cloud offerings, on the other hand, aim to change precisely this. Digital sovereignty therefore definitely makes a key difference for public authorities and administrations.

What are the key building blocks of a sovereign cloud?

First of all, the security level must of course be right as a basic prerequisite. Any cloud solution that comes into question for public authorities should work with highly secure encryption technology. It should be modular and include and combine different operating models – from “on premise” to “as a service”. For example, data requiring special protection can be located in one’s own IT infrastructure, while other applications are completely outsourced. The standardisation of resources in so-called containers and their orchestration in Kubernetes then ensure that all

parts of the cloud infrastructure interlock seamlessly. For German public authorities, it is also important that the infrastructure can be certified according to IT-Grundschutz and the Cloud Criteria Catalogue C5 of the German Federal Office for Information Security (BSI) as well as being approvable for classified information. Another important point is the use of open source building blocks.


The open source idea implies joint software development in a cross-provider community. What do the cloud customers get out of that?

The main issue here is transparency and verifiability. Proprietary software that is kept secret by the provider is like a black box for cloud customers. No one but the provider can judge whether it is really secure or not. No authority in security-sensitive areas can afford that. Open source software, on the other hand, is freely accessible and can be checked by anyone at any time. For this reason, by the way, we at secunet have been involved in open source technology for a long time and contribute to its further development – also beyond the cloud.

What is the core of the secunet cloud portfolio and when will it be available?

We will offer customers an independent cloud offering from a single source that is also very broadly positioned so that it can serve a wide variety of customer requirements in terms of technology stack as well as operating model. It is also designed to cover all security levels from GDPR-compliant to the high German secrecy level GEHEIM (SECRET).



In the cloud transformation, resources can be standardised in so-called containers. Using Kubernetes, these containers are then orchestrated across all parts of the cloud infrastructure. 

The portfolio will include a combination of German public and private cloud offerings in the areas of Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

The basis of the secunet cloud is already available today: We introduced our security-hardened cloud platform SecuStack in 2018. In 2022, we acquired the cloud-native specialist SysEleven, which brings special expertise in the orchestration of standardised containers using Kubernetes as well as its own infrastructure with data centres in Germany. The public cloud offering based on this has already proven itself with several hundred customers. The secunet cloud portfolio will now be expanded building block by building block over the next one to two years. The building blocks are modular and interoperable, which is why we call it an ecosystem. The next milestones we are aiming for are the very first approval of a cloud stack for classified information by the BSI, up to and including GEHEIM (SECRET), as well as a test certificate according to C5.

Can third-party offers also be integrated?

Our offering is designed as a hybrid cloud ecosystem that can securely incorporate solutions from partners and combine them into resilient multi-cloud offerings. Even solutions from hyperscalers can play a role, for example in less security-sensitive areas. This creates optimal freedom of choice for customers – but at a high level of security and with great transparency.

In what way does secunet's expertise in traditional IT security contribute to the cloud offering?

For more than 25 years, we have been securing digital infrastructures that require special protection, for example in ministries and security authorities. In the process, we have built up unique expertise in high-quality encryption technology, which now forms the basis for the secunet cloud.

In addition, our cloud offering incorporates established secunet solutions: for example, with our high-security solution SINA, which is the de facto standard for secure networks and workstations in German public authorities and public administration, we also enable customers to secure the access points to the cloud. This enables us to offer an entire IT infrastructure from a single source.



“In a few years, many IT security products that today are still based on hardware boxes will also be available ‘as a service.’”

Together with other European IT companies, secunet has founded ALASCA, a new association that aims to promote open source in the cloud context. What is this all about?

An innovative industry has emerged around the sovereign cloud in recent years that can offer society something crucial. Now is the time – with all the necessary competition – to exploit synergies, strengthen the open source community and thereby further advance technology development. In addition, the players in the new industry should sometimes speak with one voice so that knowledge about the sovereign cloud spreads. These are the goals of the new association. ALASCA stands for “Alliance for Sovereign Cloud Infrastructures”. secunet is one of the seven founding members. The association is open to other European companies that live the guiding principle of open source in the cloud environment as well as digital sovereignty.

What will the administrative IT landscape look like in five years’ time?

The cloud will then have become a self-evident, central component of public authority IT. IT managers will select very different cloud offerings according to the respective technology and security requirements and integrate them into the existing multi-cloud. The user experience will nevertheless be seamless. Furthermore, in a few years, many IT security products that today are still based on hardware boxes will also be available “as a service”. The cloud transformation is complete when it permeates all areas of government, business and society.



Norbert Müller
norbert.mueller@secunet.com

Norbert Müller is responsible for secunet Cloud Solutions. Previously, he was decisively involved in the successful expansion of secunet’s cooperation with public administration with regard to classic cyber security.

“Our biggest challenge was time”

In modern digital life, business processes are increasingly mapped electronically and confidential information is exchanged via open, internet-based platforms. The fact that such trust relationships work is often the result of a Public Key Infrastructure (PKI), which ensures the authenticity of digital identities in the background. In this interview, Mohamed Kiwan, CEO of EgyptTrust, explains why his company relies on a PKI solution from secunet and how the implementation went under time pressure.

Mr Kiwan, what services does your company provide and which are your main clients?

Mohamed Kiwan: EgyptTrust offers digital signatures and digital identities for all electronic services. We operate mainly in Egypt, because we are licensed from the Egyptian government for providing digital identities and digital signatures. Our clients are companies as well as all Egyptian citizens, meaning private individuals.

How did the cooperation with secunet come about?

Since we only had a limited amount of time for the project, we were looking for an experienced partner with a secure PKI solution that had already proven its worth. And that was why we chose secunet. And we have been working successfully with secunet for over one year now.

In which way do the PKI components from secunet help you to provide reliable and secure trust services? Are there any differences compared to PKI components from other vendors you have used before?

Compared to the PKI solutions we are operating with from other vendors, secunet PKI stands out for its simplicity of utilization for our engineers and users. In addition, the secunet solution distinguishes itself from the rest of the providers with its high performance – even when several processes are running at the same time, the PKI remains consistent and trustworthy.



 Mohamed Kiwan,
CEO EgyptTrust

For which application scenarios are the secunet PKI components currently used?

Our services, which are based on secunet products, can be found in applications that play a crucial role in everyday life in Egypt. For example, all companies as well as self-employed people such as lawyers and accountants must use electronic invoicing. This works with our digital signature services and the secunet PKI.

Another important application is customs clearance for shipments and goods coming to Egypt. All these goods coming to Egypt by ship, plane or other means must be declared. The documents required for this purpose must also be provided via digital services.

How went implementation and were you pleased with the way any challenges were resolved?

Our biggest challenge was time. We had to implement the systems quickly because we had a specific deadline from the Egyptian government. And we were able to meet this deadline. Only four months passed between our first meeting and the successful implementation.

“Our services, which are based on secunet products, can be found in applications that play a crucial role in everyday life in Egypt.”

Will there be further joint projects?

We are already planning another project with secunet and the registration authority in Egypt. Furthermore, we are in discussions about the possibilities of remote signing solutions, as we are keen to complete a platform for this purpose by the end of this year.



Gerd Schneider
gerd.schneider@secunet.com

HOW DOES A PKI WORK?

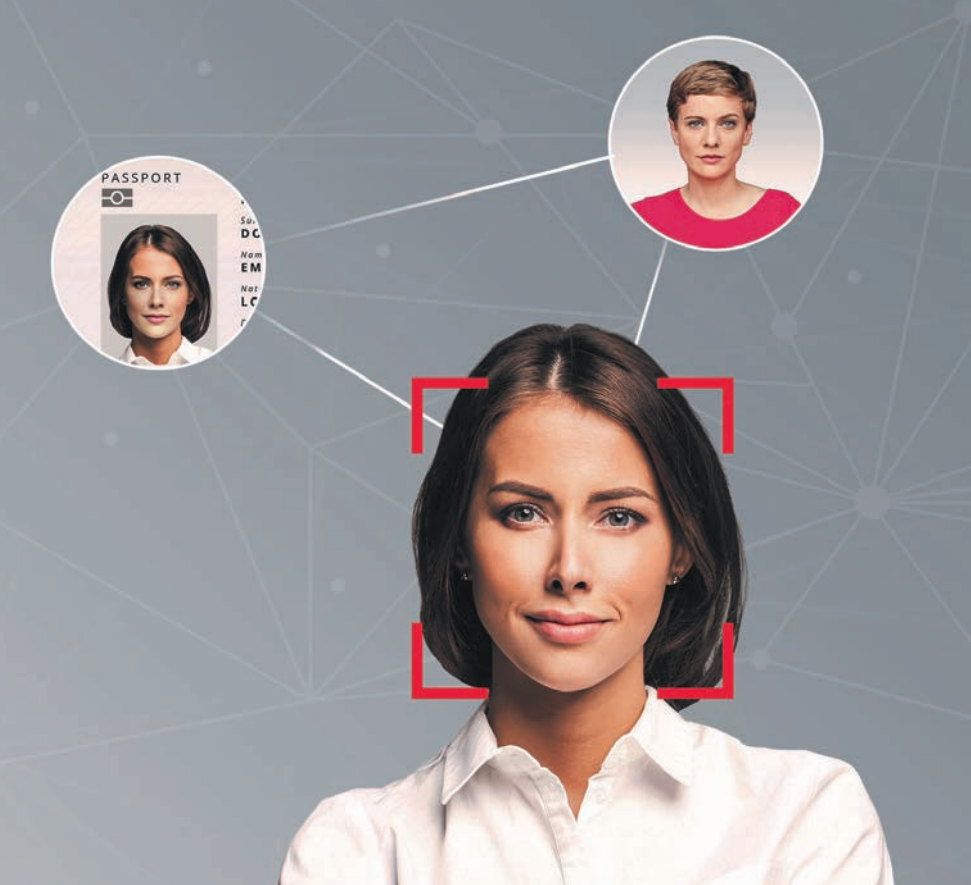
Digital certificates are used to authenticate persons and technical components and to sign and encrypt data and messages. A typical PKI consists of a number of elements that automatically issue, distribute and verify digital certificates. These include, for example, a so-called Certification Authority (CA), which signs the certificates, a Registration Authority (RA), which registers the users in the CA, and a directory service (DIR), which contains, among other things, a list of invalid public keys. Taken together, these and other elements ensure that the certificates in circulation are trustworthy at all times.


Since a PKI usually has a high degree of complexity, mainly use cases have prevailed in which the end users do not come into direct contact with the PKI and the solution runs automatically in the background. A good example of this is the encryption protocol TLS (Transport Layer Security), which is used in HTTPS-based web servers. Largely unnoticed by users, the browser uses the PKI for secure online banking and online shopping, for example.

In border control, a PKI verifies the authenticity of electronic identities. PKIs are also used in intelligent electricity meters, in networked cars or in the interaction of machines in the Internet of Things (IoT).

secunet eID PKI SUITE

secunet has bundled its know-how from more than 350 PKI projects in the secunet eID PKI Suite. The various software modules of the eID PKI Suite can be combined to form a high-performance overall system, but can just as easily be integrated individually into an existing system architecture. All relevant standards and protocols are supported. For areas of application with special security requirements, the eID PKI Suite is also available in a variant certified according to Common Criteria EAL4+.



 A morph (top left) can be created from the portrait of a real person (large in the picture) and another real person (top right) using image editing software. Morphs can be used for criminal purposes.

Combating identity fraud at border control

Poor chances for morphs

Biometrics and facial recognition have made border control more efficient and secure. However, so-called morphing attacks pose a challenge for officials and software systems alike. This involves fraudsters using ID photos that are composed – “morphed” – from the biometric passport photos of several people. Morphing methods are constantly evolving. The differential morphing attack detection from secunet does the same – and scored significantly better than all other methods in the FRVT-MORPH test of the US standards authority NIST when it came to recognising high-quality morphs

Morphing attacks are currently one of the greatest threats to border control. If the attackers succeed in combining two or more biometric passport photos into a convincing “morph” using image processing software and thus deceive biometric software or even border control officials, several people can use the same ID document to cross the border – namely all those whose images are involved in the morph. Security measures such as “live enrolment”, where passport pictures have to be taken on the spot and under the supervision of officials, or the training of border control officers counteract the criminal methods, but cannot completely eliminate the problem.

With algorithms against identity fraud

That is why the border control authorities also rely on intelligent software to put a stop to the fraudsters. The so-called morphing attack detection (MAD) refers to software algorithms that can detect facial morphs during automated border control. In doing so, they use different methods. secunet offers an algorithm that works according to the principle of differential MAD. In this process, a potentially morphed facial image is checked against a second image, which is usually captured live and is therefore trustworthy.

The reliability of MAD algorithms is determined within the framework of the independent and internationally recognised “Face Recognition Vendor Test (FRVT)-MORPH” of the US National Institute of Standards and Technology (NIST). Two values in particular are decisive: the Bona Fide Presentation Classification Error Rate (BPCER), also known as the false alarm rate, indicates how often the algorithm has falsely recognised genuine IDs as morphs. In contrast, the Attack Presentation Classification Error Rate (APCER), also called the morph miss rate, indicates how many morphs were not recognised. A low APCER therefore means that many morphs were successfully detected. The algorithms can be set to a low BPCER value, but then the APCER value usually increases. Therefore, it depends on good fine-tuning depending on the particular requirements.

Differential MAD with excellent results

In the FRVT-MORPH test of November 2022, the improved algorithm achieved its best result yet: With a BPCER of 0.01, only 9% to 36% of morphs (APCER) were not successfully detected across all datasets. With a BPCER of 0.02, the morph miss rate even drops to 4% to 22%.

The secunet algorithm scored particularly well in the category of high-quality morphs. Although such morphs are not particularly difficult for experienced attackers to produce, they are especially difficult to recognise. This category includes the “Printed and Scanned” data set, in which the morphs – as is usual with passport photos – were printed out and scanned in again, leaving

practically no traces of the manipulation in the image. With this data set, the secunet algorithm recognised 84% of the morphs even with a moderate BPCER of 0.01 and even 93% with a somewhat higher BPCER of 0.02. With these results, it beat all other of the more than 30 methods that took part in the test – and by a wide margin. The results are also interesting in comparison to human test subjects, who were found to recognise only 60% of morphs. This shows how much MAD can contribute to combating identity fraud at the border crossing.

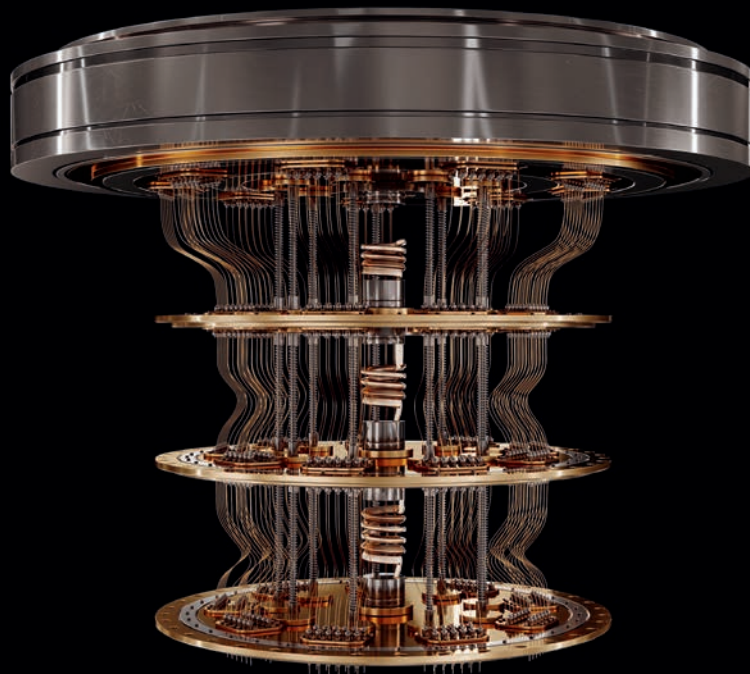
Nevertheless, morphing detection remains a challenge. The MAD algorithms must be continuously improved, expanded and retrained in the future to stay one step ahead of the fraudsters and further reduce error rates.



Michael Schwaiger
michael.schwaiger@secunet.com

The automated border control system secunet easygate, here an installation at Vienna Airport, has morphing attack detection.





Security against quantum computers

Cryptography 2.0

Future quantum computers pose a considerable threat to cryptographically protected data. This not only applies to everyday communication on the internet, but especially to highly sensitive data, including state secrets. New, quantum computer-resistant algorithms that have been developed in recent years promise a remedy. secunet has been dealing with this post-quantum cryptography (PQC) from an early stage. Today, several SINA components used by authorities and the German Armed Forces to handle classified information are already equipped with PQC. The German Federal Office for Information Security (BSI) has approved these devices for the high classification level GEHEIM (SECRET). This makes Germany a pioneer in Europe when it comes to PQC.

The security of digital infrastructures relies heavily on cryptographic algorithms and protocols. Common encryption methods such as the Diffie-Hellman key exchange used in many internet protocols such as Transport Layer Security (TLS) and Internet Key Exchange (IKE) assume that certain mathematical problems are practically unsolvable due to limited computing capacities. Digital signatures based on the RSA method, which are used e.g. for authentication in web browsers, are considered secure as long as there is no efficient algorithm for factorisation.

This could be relied on for decades. But when experts discussed the first concepts for quantum computers several years ago, it quickly became clear that the days of conventional cryptography are numbered. It will probably still take some time before the new type of computer can pose a threat to conventional algorithms. So far, quantum computers exist only as room-filling experimental setups in research labs,

and their performance is currently limited to solving simple computational tasks. But it is expected that in just a few years, advanced quantum computers will be clearly superior to classical computers in many areas. This includes solving mathematical problems that serve as the basis for conventional cryptography.

Computing with qubits

Quantum computers are based on a completely different technology than conventional systems. Instead of being limited to binary arithmetic with zeros and ones, their fundamental information units, the qubits, can also work with gradations in between. This is because the qubits are based on quantum mechanical states and therefore do not have to assume exactly one of the values zero or one. Rather, the two values can overlap, with varying probabilities then applying to them. If numerous qubits are connected, logical operations can be carried out, which, however, are more similar to the processes in neuronal networks than to serial computing in classical computers. Quantum computers do not proceed step by step, but take many possible solution paths at the same time and may also find several solutions. In this case, algorithms have to limit the computing operations in a sensible way so that usable results emerge.

As soon as it was foreseeable that the new type of computer would threaten conventional cryptography, the search began for alternative crypto methods that are resistant to quantum computers. For it is not only because of the rapid development of the new technology that haste is required. The challenge is also that attackers can already record and store encrypted data today in order to decrypt it later, when sufficiently powerful quantum computers are available. This is a very serious scenario, because particularly sensitive data, for example with the classification SECRET, should often remain protected not only for years, but for decades. Thus, even before its development has reached the required level of maturity, quantum computers are already a significant threat to the information security of states and international organisations.

PQC in use

To counter this threat, the US National Institute of Standards and Technology (NIST) is currently conducting a process to standardise PQC and recently selected the first algorithms to be standardised by 2024. However, since possible attacks along the lines of “record now and decrypt later” require immediate preventive measures, secunet has decided, in consultation with the BSI, to implement PQC even before standardisation by NIST.



The SINA L3 Box H (left), the SINA Workstation H Client V (rear) and the SINA Communicator H (right) already work with PQC elements.



As an IT security partner of the Federal Republic of Germany, secunet produces technology that protects highly classified data up to the classification level GEHEIM (SECRET) and is used, among others, by the German Federal Armed Forces and federal ministries with special security requirements, such as the Federal Ministry of Defence. Since 2002, a total of around 30,000 SINA encryption devices approved for GEHEIM or SECRET have been delivered in Germany and other EU and NATO countries. In Germany, SINA represents the de facto standard for encryption at this high security level. secunet has already equipped three key products in this portfolio with PQC elements: the SINA Communicator H, which offers tap-proof voice communication as well as many other modern communication features, the highly secure VPN gateway SINA L3 Box H and the SINA Workstation H Client V, which delivers a unique combination of high-performance cryptography and high computing power.

The BSI has approved these three SINA components as the first encryption products with PQC in Germany for the GEHEIM (SECRET) level. In a European comparison, Germany is thus a pioneer in crypto devices that already work with PQC. And with the SINA Workstation H R RW14, the latest generation of hardened laptops designed for use under extreme conditions is already waiting in the wings to enter the PQC era.

Hybrid methods

In the three SINA components with PQC so far, the key exchange is implemented in a quantum-resistant manner. What does this mean? In order to guarantee the confidentiality of data during transmission against quantum computers, both the encryption algorithm and the key exchange procedure used to derive the key must be quantum resistant. Usually, the encryption algorithm is already quantum resistant if it is used with sufficiently large keys. Yet the conventional key exchange methods are potentially vulnerable to quantum computers. Since the PQC algorithms are still in the final stages of standardisation, the BSI recommends the use of so-called hybrid methods: By combining conventional cryptography

and PQC, an attacker would have to break each algorithm to break the hybrid solution. The three SINA products with PQC support a hybrid quantum-resistant key exchange with the BSI-recommended algorithm FrodoKEM. In the course of the next few years, secunet will implement all critical functionalities of the entire SINA portfolio for the GEHEIM / SECRET level, but also for lower classification levels such as VS-NUR FÜR DEN DIENSTGEBRAUCH (RESTRICTED), with PQC.

In this context, hybrid modes can serve not only as a temporary migration strategy towards PQC, but as a contribution to long-term security and agility with regard to encryption methods. In general, the use of PQC marks the beginning of a new cryptographic era, characterised not only by resistance to quantum computing, but also by increased cryptographic agility. In response to the threat, cryptography is thus reinventing itself – and gaining strength.



Leonie Bruckert
leonie.bruckert@secunet.com

Biometrics and artificial intelligence

Fairness, robustness and security for AI

Artificial intelligence (AI) holds great potential for applications in the field of homeland security. One example is the live analysis of facial images for security purposes, for example at airports. However, there is one major challenge: statistical distortions in the data basis can lead to biased results, which in the worst case can disadvantage or favour certain groups of people. secunet is researching solutions that counteract this dangerous and momentous effect and thus help to ensure that AI applications work fairly and are trustworthy.

In order to guarantee the security and fairness of AI applications, the EU is currently developing the so-called EU AI Act, which will divide AI applications into different risk categories and prescribe certain tests. In Germany, the Federal Office for Information Security (BSI) established a framework for testing criteria for AI applications early on with the AIC4 catalogue.

An important component of these tests is the question of whether and to what extent a trained AI model is subject to statistical distortions – a so-called bias. A bias arises, for example, from insufficiently balanced training data or from an overrepresentation of certain combinations of characteristics, which are then learned and generalised by the AI model. Thus, in the worst case, it can happen that certain groups of people or also individuals are disadvantaged or favoured in the application of the AI model. Especially in AI applications that work with images or videos of people, a bias would have serious consequences.

The problem is a deep-seated one: image-processing AI models with architectures like CNNs (Convolutional Neural Networks) are designed to identify patterns. Even if features such as age, gender or ethnicity are not explicitly labelled in the training data, an AI model can construct an indirect representation of such or similar characteristics based on the available image information. Such a so-called indirect bias is difficult to detect and even more difficult to correct.



These synthetic faces were assembled from a variety of possible features and then used as the basis for virtual images showing the faces in different situations. Such images are also used to check AI models for bias.



An analysis requires a very large, differentiated data set. To test all combinations of characteristics for bias in the conventional way, thousands of new images must be produced, which is simply not possible in relation to the time and cost required.

secuview has intensively studied the topic of bias in images and AI models with human reference and has developed a solution that not only detects bias in the data, but for the first time can also test the AI model for bias. With this solution, it is possible to further develop a model so that bias is eliminated. For this purpose, the training data is adjusted so that all features are fairly distributed and present and, as a consequence, a possible bias is mitigated in the model. Incidentally, this not only ensures fair and discrimination-free AI models, but also increases the security and robustness of the models. With additional functions such as the adjustment of environmental and surrounding factors, the limitations of the AI model can be determined and solutions can be developed.

The analysis and solution of the bias problem takes place in three steps:

- 1) The training and test data are analysed for bias in relation to characteristics such as age, gender and ethnicity. This allows problems to be identified at an early stage, which would later be reflected in the AI model.
- 2) secuview's solution performs a test of the AI model. In the process, it generates a large number of photorealistic artificial identities that differ in age, gender and ethnicity, for example. The original identities of the test data are exchanged with the artificial identities with the intention of testing the recognition performance of the AI model. In the process, arbitrary combinations of characteristics are generated; after all, the actual human diversity is also very large. There is no specification of a certain number of ethnicities, as this would lead to a new bias. The customised identities with fluid transitions in the characteristics thus represent the entire human diversity.
- 3) If a bias is detected, new identities can be created for the training data and the model can be re-trained. This process is repeated until no bias is detectable.

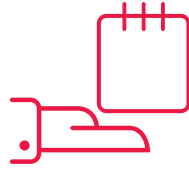




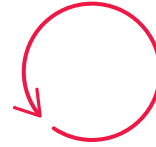
Initial situation:
Potential bias



Fairness
analysis



Generation of
artificial identities



Re-training
of the model



Result:
Fair model

The process is simple and quick. Once an AI model has gone through the process, there is proof that it is fair and free from discrimination. This creates confidence in the AI application – on the part of the public, but also on the part of the operators, because the latter can now assume with confidence that their model is fair.

Furthermore, the analysis of AI models is not only about bias. Other important aspects that are also reflected in the EU AI Act as well as in the BSI's AIC4 are robustness and security of recognition performance. For example, there is a risk that an AI application will fail to recognise relevant characteristics under certain weather conditions or lighting conditions, which would result in security risks. With secunet's research and development, various environmental factors can be tested to show the limits of an application's recognition performance and identify potential risks.

The risks of AI are debated a lot in the public, including in the context of its use for homeland security. A thorough and impartial examination and optimisation of the relevant AI models is the best way to respond to this discussion and to increase the acceptance of AI applications.



[Dominik Lawatsch](mailto:dominik.lawatsch@secunet.com)
dominik.lawatsch@secunet.com



Connected and autonomous driving

“We need a public discussion”

The automotive industry has to master several disruptions at the same time and faces a multitude of challenges in the process. One of them is cyber security. How do you secure systems that are part of a multifaceted,

interconnected infrastructure, have a life cycle of several decades and – unlike critical components in highly secure data centres – potentially find themselves in a hostile environment all the time?

Much can be solved technically, but a cross-manufacturer, public discussion is also necessary, finds automotive cybersecurity expert Manuel Wurm.

Mr Wurm, where do you currently see the greatest challenges on the path to secure mobility in the future?

The path to an electrified, automated and cooperative mobility of the future leads us from largely isolated, self-sufficient vehicles to an ecosystem of variously interwoven components: automated or autonomous vehicles, charging infrastructure, mobility service providers, manufacturers, fleet operators, telecommunication service providers and, last but not least, the end customers. Shared mobility, the principle of mobility that can be used jointly, is also reducing the importance of vehicles as possessions or even status symbols. Instead, the mobility of people or the transport of goods will be in the foreground in the future.

Besides all the advantages that such a future promises, there are some challenges to be overcome on the way there. The entire automotive industry, especially the manufacturers and their suppliers, are caught between time pressure and competitiveness on the one hand and new legal requirements such as UNECE R155/R156 on the other – and this on a playing field with partly new players. In order to maintain acceptance and trust in this new technology and in this new market in the long term, the necessary guidelines – with regard to security – must be discussed and defined publicly and transparently. What is the socially accepted (residual) risk for this new technology of connected and automated driving?

Furthermore, numerous reliability requirements must be met at the technical level in order to strengthen and maintain the trust of end customers and ultimately of society as a whole in the new technology. These include availability, because otherwise there is a risk of financial losses, functional safety, because otherwise there is a danger to life and limb, and security, including data protection, to protect against cyber attacks.

“What is the socially accepted (residual) risk for this new technology of connected and automated driving?”

With regard to cyber security, it is worth taking a closer look and possibly changing the perspective. Unfortunately, there is no consistent picture of the threat situation. Who are the possible attackers? What goals do they pursue and what capabilities and resources do they possess? From a cyber attacker’s point of view, connected vehicles with ADAS or AD functionality, i.e. with automated or autonomous driving functions, represent a highly attractive target. Thanks to their wireless interfaces, they are easily accessible from a distance; in addition, weaknesses in the back-end servers can enable attacks on the entire fleet; and finally, a lot of expensive and complex components, some of which are new

to the vehicle industry, are installed for automated driving – including a presumably long list of potential vulnerabilities.

You have published a specialist book specifically on the topic of automotive cybersecurity. What is the difference between classic cybersecurity and automotive cybersecurity?

Both areas have in common that they provide security for complex computer systems and networks. Up to now, it has largely been the case that IT technology could not simply be integrated into vehicles in the majority of cases. Limiting factors are often the lower resources of the embedded systems as well as stricter requirements of the automotive industry – for example, temperature resistance.

However, the (classic) distinction between IT security and automotive embedded security is becoming increasingly blurred in the automotive sector. Where vehicles used to be understood as isolated, autonomous systems, in the future they will communicate with other road users and traffic infrastructure components such as traffic lights. Where previously a network of dedicated control units carried out the various control and regulation functions, in future domain or zone control units with high-performance computers and software components from the “classic” IT or IoT sector will combine and take over the computing tasks of several control units. Thanks to the

broadband and comprehensively available radio connection, algorithms and functions, for example the calculation of the route, can also be transmitted from the vehicle to a cloud and calculated there. The Security Operation Centres, which at least all larger companies already operate to secure their IT infrastructure, will be extended to vehicles as new endpoints in the future.

An essential difference, which I also describe in my book, is the fact that vehicles are potentially in a hostile environment all the time: Attackers can eventually (legally) obtain vehicles and vehicle components and, to a certain extent, investigate and

¹ A regulation of the United Nations Economic Commission for Europe (UNECE)

attack them at will. In IT security, on the other hand, we lock up critical components in highly secure data centres and thus prevent at least the physical, local attacks. Manufacturers of mobile devices such as smartphones are confronted with the same problem.

Many players are active in connected mobility – OEMs, suppliers, infrastructure components, insurance companies, public authorities, to name but a few. How can all these different participants interact securely?

The creation of cooperative, intelligent transport systems and alternative mobility concepts requires a certain technological transformation, which in turn leads to changes in the supply chain or in the business relationships within the automotive sector. Instead of the established car manufacturers with hierarchical OEM-supplier relationships, complex technology-centred or business model-centred ecosystems consisting of various new players in the mobility sector will play an important or even dominant role in the future. New players include local public transport operators, mobility service providers with powerful digital platforms, some of which have enormous reach, and technology suppliers that provide, for example, high-resolution map material or LIDAR¹ components.

“Within the framework of transparent cooperation, in which all partners have the same knowledge and competences, the probability of unrecognised cyber risks is lower.”

How can we ensure that IT security does not fall by the wayside despite the wide variety of interests within these ecosystems?

Laws and regulations can help here, but in my opinion only define a minimum standard and set the guard rails, so to speak.

A sustainable way would be to build up knowledge, exchange it with each other and align the respective solution spaces through trusting cooperation, for example through joint development platforms and by creating common standards. Within the framework of transparent cooperation “at eye level”, in which all partners have the same knowledge and competences, the probability of

unrecognised cyber risks is lower. At least as far as technical cooperation in the context of a joint cybersecurity strategy is concerned, business relationships and hierarchies should play a subordinate role. Ultimately, only a well thought-out and structured application of technical cybersecurity building blocks can contribute to effective protection against cyber attacks.

Vehicles have a life cycle of several decades. What is the best way to deal with vague predictions about the future – for example, zero-day vulnerabilities or quantum computers?

The long life cycle of vehicles does indeed present us with great challenges. Around 15 years – compared to the average useful life of smartphones or PCs, that’s an extremely long time, and it feels like only major household appliances come close to that.

To directly address your two examples: Against zero-day exploits, one probably cannot completely protect oneself with finite means, but only prepare and build up a defence. Against future attacks based on quantum computing, we can already protect ourselves today or at least prepare for them: Post-quantum cryptography, i.e. cryptographic algorithms that presumably cannot be decrypted in a short time even by quantum computers, should already be considered in product development today.

However, the industry will have to adapt technologically and organisationally to longer-term support periods by maintaining the necessary personnel, equipment, tools and knowledge over the entire period. Resources

should be reserved as part of product development and a certain flexibility should be planned for to allow for the future replacement of hardware, updating of software and, in particular, the adaptation of crypto-algorithms. Furthermore, so-called “degraded functionality” should be considered already in the development phase. This means that, for example, the secure execution of certain functions can no longer be guaranteed at some point and must therefore be prevented or restricted. In order to cope with all these tasks, sophisticated processes as well as personnel and technical capacities are required – both at the manufacturers’ and at the suppliers’.

¹“Light Detection and Ranging”, a method for optical distance and speed measurement

“How do other industries deal with such challenges and are their experiences transferable to the automotive industry?”

Because here again several different parties are affected, from the manufacturer to the end customer, the guard rails for long-term security support should ideally be discussed and decided jointly and publicly – and not be solved individually by individual companies. We should ask ourselves the following questions: What are the possible consequences of successful cyber attacks on vehicles and on their digital infrastructure? At the very least, everyone should know the magnitude of the possible consequences. What is the socially accepted risk from cyber attacks on vehicle manufacturers and mobility service providers? Will the remaining (residual) risk be borne by insurance companies? How much is security worth (to us)? And how much is the customer willing to pay for it? How long should manufacturers guarantee the security of their products and provide updates? When or under what conditions can costly maintenance and updates be terminated prematurely (end-of-service vs. end-of-life)? How do we deal with security vulnerabilities that cannot be fixed in the short term – shutting down vehicles and mobility services or continuing to operate with limited functionality?

For the automotive industry, these requirements are a novelty because necessary processes have yet to be established. Experienced and cross-industry service providers like secunet can provide valuable assistance here, in my opinion. How do other industries deal with such challenges and are their experiences transferable to the automotive industry?

We also have a shortage of skilled workers in Germany. Do you see growing interest in the topic of IT security as part of your lecturing activities?

In recent years, we have fortunately been able to observe that more and more degree programmes with a security focus have emerged, and that security as a topic cluster is more frequently permeating various subject areas: from computer science to electrical engineering and mechatronics to business informatics and technology management.

In order to arouse curiosity for the topic of security, simple demonstrations, “live hacks”, often help to show students how low-threshold access to “hacking” can be. Thanks to the availability of inexpensive hardware and software, one is now technically able to carry out a wide range of attacks on vehicles with a budget of less than 100 euros. Instructions, how-to videos and software are mostly freely available and easy to find.

Manuel Wurm

Manuel Wurm works in the automotive industry as a research and development engineer. He has been a lecturer at the DHBW Ravensburg since 2012 and also at the Vorarlberg University of Applied Sciences in Dornbirn (Austria) since 2019. His book “Automotive Cybersecurity: Security-Bausteine für Automotive Embedded Systeme” (Automotive Cybersecurity: Security Building Blocks for Automotive Embedded Systems) was published in German language by Springer Vieweg in 2022 and is available e.g. in online bookshops.

© Dieter Seibel, Wangen





Cybersecurity legislation for industrial companies

The path out of the jungle of EU cyber regulation

Cyber Resilience Act, NIS-2 and the CER Directive: The cybersecurity legal situation for industrial companies in Europe is diverse and confusing. But the implementation of the various regulatory requirements can help to successfully defend against cyber attacks. This is urgently necessary, because the number of cyber attacks is increasing. According to the techconsult study “Attack Detection in Critical Infrastructure Companies” from the beginning of 2023, 79% of companies estimate the current threat situation as growing to strongly growing. But who are affected by the regulations? What obligations arise from them? And what deadlines must industrial companies meet? Here is an overview of the most important cyber security laws in Europe.

1. Directive on Security of Network and Information Systems (NIS-2 Directive)

The NIS-2 Directive is an important part of the EU digital strategy “Shaping Europe’s Digital Future” and the advancement of the first NIS Directive already issued in 2016. The aim is to ensure a high level of cyber security at European level and thus strengthen the single market. The directive entered into force on 16 January 2023. The EU member states must transpose the provisions into national legislation by 17 October 2024.

Affected economic sectors are divided into two categories: essential – i.e. sectors with high criticality – and important – other critical sectors. The former includes, for example, energy, transportation and traffic, financial markets, the health sector, digital infrastructure and public administration. Other critical sectors include postal and courier services, manufacturing, chemicals, and the production of medical devices, electronic equipment, machinery and means of transport. Exactly which companies

within the defined sectors are affected is determined by the respective national legislation.

For industrial companies, NIS-2 brings new rules and thus new tasks. Companies must register and report cyber security incidents to the responsible authorities in a multi-stage process according to clearly defined guidelines.

Companies must also implement active risk management and adhere to standards for network and system security, incident handling, crisis management, secure supply chains and asset management. Protection mechanisms and technologies used must be state of the art. A certification obligation to demonstrate compliance can be additionally demanded and introduced by the nation states.

In Germany, it is planned to transpose NIS-2 into national law through the NIS-2 Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG). This is again an article law, which adapts many existing laws in accordance with the directive. Critical infrastructure operators in Germany have already built a solid foundation as a result of the IT Security Act. For example, companies that have implemented an Information Security Management System (ISMS) and the necessary trustworthy cybersecurity technology are well positioned and only have to expect minor adjustments.

2. EU Cyber Resilience Act – cyber security for connected products

The EU Cyber Resilience Act (CRA) is a draft law with the aim of protecting end consumers and companies from products that do not take cyber security sufficiently into account. To this end, the Act aims to define requirements for products with digital elements in terms of development, design and production, thus ensuring cyber security throughout the life cycle – including, for example, the provision of software updates. The security level of networked end products is to be increased in order to prevent cybercrime. The law is expected to come into force in 2023. After that, those affected will have twelve to 24 months to implement the new requirements.

Many manufacturers of hardware and software products are affected by the regulations. The requirements are differentiated depending on the potential impact. Stricter regulations are expected for products that affect larger economic areas, such as IoT and mobile devices or operating systems. For example, cyber security is to be taken into account as early as the production process or configuration (“security by design and default”) – starting with the planning of a product and continuing into the operating phase and several years after the product is sold (up to five years). In addition, manufacturers must keep detailed documentation. The provision of software updates or patches and the active



communication of security vulnerabilities and their elimination is another essential component of regulation. Furthermore, clear and comprehensible operating instructions must be made available for affected products.

3. Directive on the Resilience of Critical Entities

The EU Directive on the Resilience of Critical Entities (CER Directive) aims to strengthen the physical resilience of critical entities and thus to counter hybrid threats in particular. The CER Directive replaces the old Directive 2008/114/EC and broadens its scope. These new rules oblige EU member states to identify critical facilities and strengthen their resilience. The CER Directive entered into force on 16 January 2023. EU member states must transpose the provisions into national legislation by 17 October 2024.

Affected economic sectors are divided into the categories “essential” and “important” according to the Directive. A total of eleven sectors are included in the scope, some of which overlap with the NIS-2 Directive: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration, space, and production, processing and distribution of food.

Companies must implement both organisational and technical security measures. These include a functioning risk management system to prevent business interruptions. A business continuity management system (BCMS) can be a suitable measure here. In addition, companies should be able to react adequately to security incidents and define an incident management plan accordingly. Security incidents should be reported to the responsible supervisory authorities. These can carry out their own inspections and audits and demand the implementation of appropriate measures.

Step by step to more security – this is what companies can do now

Industrial companies can prepare for the regulations in five steps:

- 1) Check who is affected (product manufacturers, operators, integrators)
- 2) Check requirements
- 3) Prepare reporting processes or adapt existing implementations for this purpose
- 4) Establish security concepts, information security management (e.g. based on ISO/IEC 27001 or IEC 62443) including business continuity management
- 5) Implement risk management in the defined area of application

Whether CRA, NIS-2 or the CER Directive: If companies do not comply with the regulations, the EU states can impose fines. In the case of the CRA, for example, these fines amount to up to 15 million euros or 2.5 percent of annual turnover. This makes a structured and holistic (cyber) security strategy all the more important. In addition to technical measures such as securing networks and devices, this also includes looking at securing company processes and raising awareness of the issue among employees.



Alexander Schlensog
alexander.schlensog@secunet.com



Steffen Heyde
steffen.heyde@secunet.com

Information security management

The maturity model: ISMS taken a step further

Gunter Pilger, author of this article, is an IT security representative (TÜV), Baseline Protection (IT-Grundschatz) practitioner and data protection representative (TÜV) at secunet and specialises in information security.

Currently, the horizon of information security ends for most authorities and companies after an information security management system (ISMS) has been introduced. Although many actively live an ISMS, be it through regular (internal) audits, the derivation of measures and the implementation of these measures, in many cases there is no systematic process that comprehensibly maps measures and presents the current state of the ISMS in aggregated form. This is where the so-called maturity model comes in. It also helps to meet the requirements of ISO/IEC 27001 (specifically: ISO/IEC 27004) and the German Federal Office for Information Security's IT Baseline Protection (BSI IT-Grundschatz).

The aim of introducing and later applying a maturity model is to determine and increase the quality and performance of the ISMS (cf. fig. 1). With the help of the maturity model, regular evaluations can be used to check which (sub-) processes are not yet optimally controlled. There is a need for action in areas where the determined maturity level is low.

Maturity models can help prioritise the further development and improvement of an ISMS. The application of a maturity model is intended to provide a comprehensive view of the efficiency of the information security process. For this purpose, the ISMS is analysed over a longer period of time in order to measure the efficiency of the ISMS process, to review it at regular intervals and to take corrective measures for improvement if necessary.

Successful implementation of a maturity model

It is advisable to first apply the maturity model to a limited information network and then gradually roll it out into the organisation, thereby expanding the scope.

Before the maturity model process is started, it must be ensured that security objectives are defined in detail. This is of great importance because it is the only way to ensure that key performance indicators (KPIs) can be derived and in turn aligned with the

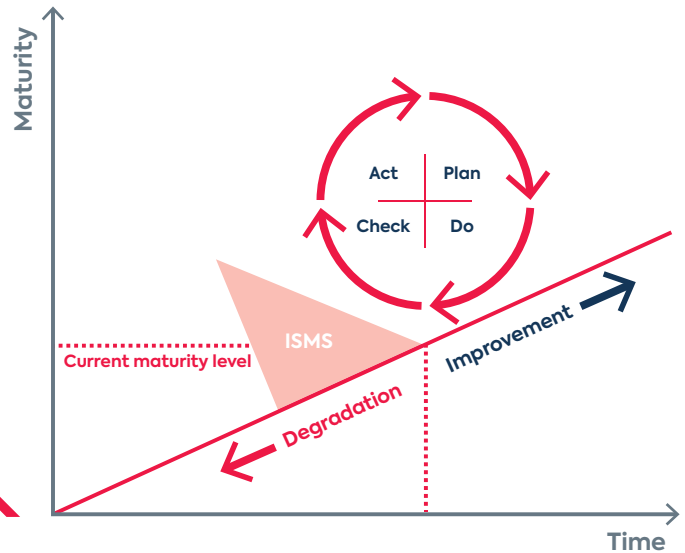


Figure 1: Maturity level and continuous improvement

ISMS

An ISMS provides the framework for ensuring the information security of an organisation through defined rules and methods. secunet supports companies in setting up an ISMS in accordance with the IT Baseline Protection (IT-Grundschutz) of the German Federal Office for Information Security (BSI) and ISO 27001.

Maturity model

A maturity model is used to evaluate and improve ISMS processes. It also helps to monitor development trends.

Benefit of a maturity model

A maturity model can be used to optimise and systematically control processes.

security objectives at the end. This presupposes that the goals are defined in a comprehensible and measurable way and that, in addition to the clear link to the target objects, a connection or cause-effect relationship can also be established, similar to a balanced scorecard. One example: If the training rate is high, it is assumed that security gaps will be detected and remedied more quickly. This leads to higher customer satisfaction and a better reputation. With a defined strategic goal of “higher reputation”, a causality between cause and effect would thus be established.

Contents of a maturity model

Once the implementation procedure has been defined, the next step is to determine the maturity levels (cf. fig. 2). Here, for example, it is also specified at which maturity level the introduction of key figures should be aimed for.

It is advisable to work out suitable KPIs for the organisation in several workshops and to derive them on the basis of the defined topic areas. All stakeholders should be involved in the definition of the KPIs from the beginning, so that they can identify with the KPIs. KPIs can be presented in a KPI profile with details on how they are to be determined and evaluated.

Figure 2: Procedure for implementation



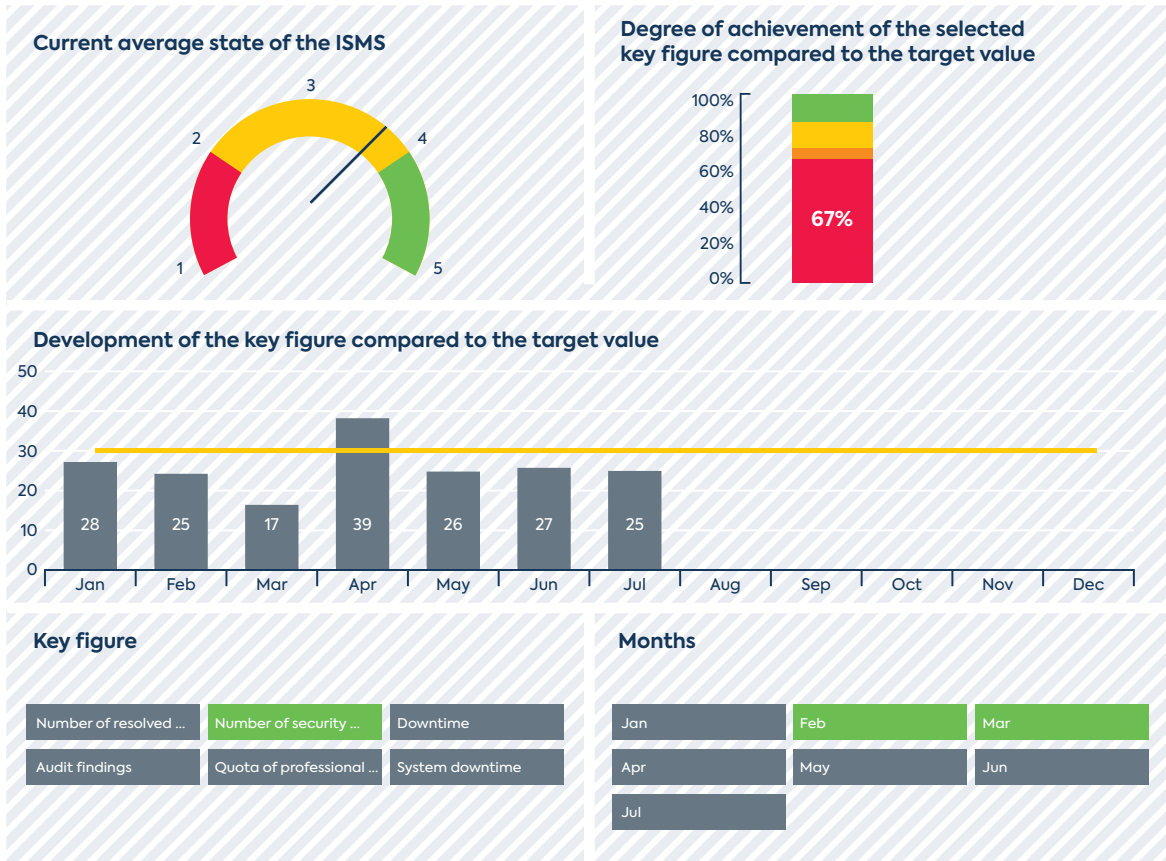


 Figure 3: Dynamic dashboard

The declared goal is to capture and determine KPIs as efficiently as possible. This is realised by deriving them as automatically as possible from existing systems and databases. The identified KPIs and their value should also flow back into the overarching risk management process for continuous improvement. On this basis, the processes required for maturity measurement with KPIs and the company or authority should also be subject to continuous improvement.

KPIs only reflect reality if they are under continuous observation and control and are recorded qualitatively or quantitatively to see how measures have actually had an impact.

An overall result is also determined from the values of the KPIs, which can be used to assess whether there has been an improvement or degradation of the overall maturity model.

Presentation of the key performance indicators (KPIs)

It is advisable to present individual KPIs in a dashboard (cf. fig. 3) so that they remain clear and comprehensible for control purposes, as well as to give the organisational management a rough overview of the current status of the ISMS in a monthly report.

The KPIs are presented in different types of diagrams for the management report in order to quickly obtain a meaningful overview. Both individual KPIs and the observation periods as an aggregation of the KPIs over a certain period of time can be selected for presentation.

Conclusion

A maturity model is being explicitly demanded more and more often, and the benefits for companies as well as public authorities are increasing. The employees are engaged with processes, they therefore become comprehensible and tangible, and KPIs measure and control the processes. The KPIs can thus be used for process optimisation, as in a balanced scorecard, and at the same time serve the continuous improvement process, which is checked by auditors both in BSI Baseline Protection and, for example, within the framework of ISO/IEC 27001. secunet has already successfully introduced several maturity models for customers and can thus provide qualified support to both authorities and companies as required.

 [Gunter Pilger](mailto:gunter.pilger@secunet.com)
gunter.pilger@secunet.com

Healthcare

Service providers have a choice when it comes to TI access

The secunet konnektor provides a secure connection of doctors' surgeries, hospitals and other medical service providers to the telematics infrastructure (TI), the data highway of the German healthcare system. The connectors contain smart cards (gSMC-K) with certificates that expire after five years according to the security specifications in the TI. After that, a new connector must be used that is equipped with a gSMC-K with current key material. The first connectors from secunet for online productive operation were produced at the end of November 2018. Thus, their certificates expire by the end of 2023.

In addition to the option of a connector exchange, secunet now offers service providers a software update to extend the runtime of secunet connectors. From August 2023, this will enable an extension until 31 December 2025 for all secunet connectors that contain certificates issued before 1 January 2021 – regardless of whether the connector is set up with ECC or RSA keys. For service providers, nothing changes in the setup or daily routine; they receive the update from their contract partner.

“With the runtime extension, we are offering users of the secunet konnektor another quick and uncomplicated alternative in addition to the replacement of the hardware, and we are giving them time to make a well-considered decision as to which path into the TI is the best for their requirements profile in the future,” says Markus Linnemann, Vice President Division eHealth, secunet.

In addition to the on-site connector, the first “TI as a Service” offerings based on centrally operated single-box and data centre connectors are already available today. With the TI gateway and the high-speed connector, secunet is preparing the next evolutionary stage of “TI as a Service” offerings in parallel. “TI 2.0 focuses on new models that do not require local physical access points,” says Linnemann. “With the high-speed connector, secunet offers the technical basis for this.”

Thus, service providers will soon be able to choose their favourite TI connection – single-box connector, high-speed connector or TI as a Service – depending on their individual requirements.

The secunet high-speed connector, which is currently in the approval process, will offer decisive advantages for hospitals and “TI as a Service” providers before the end of 2023. It can be operated centrally and serves the requirements of large IT networks and healthcare facilities. Especially for “TI as a Service” providers, it is multi-client capable. The solution ensures maximum performance, an easily scalable load and a high level of resilience of the TI access.



Medical practices and other medical service providers require access to the telematics infrastructure (TI).

On the way to TI 2.0, the freedom of choice for service providers is increasing. It is worthwhile to look at the options, as individual needs can be better taken into account in the future.

The secunet eHealth Newsletter provides up-to-date information on TI access and other topics relating to the digitisation of the German healthcare system. It is currently available in German language only. Click here to subscribe:

<https://www.secunet.com/anmeldung-ehealth-newsletter>

Help with IT incidents

Cyber attack – now what?

secunet is the first IT security service provider in Germany to be listed by the German Federal Office for Information Security (BSI) for the scope “incident handling” and is also the first registered IT security service provider of the Cyber Security Network (CSN) – a voluntary association of qualified experts for IT incident handling. The certified cyber security service providers are meant to help companies respond quickly to security incidents and successfully defend against them.

The secunet test centre has already been serving the areas of conformity with technical guidelines, information security management systems (ISMS) and penetration tests for many years, thus providing support in averting threats. The new area now expands this portfolio by adding various services as part of a step-by-step approach to handling security incidents, which are carried out by a team of BSI-certified incident experts.

Specifically, these are:

- Analysis of complex IT security incidents, especially on site
- Rapid containment of the extent of damage caused by a major IT security incident
- Determination of the causes of complex attacks
- Recovery of various affected systems after an IT security incident

“Companies are often overwhelmed with the management of IT security incidents. Particularly in complex cases requiring strong technical expertise and experience in incident analysis and handling and demanding personnel capacities, the IT department quickly reaches its breaking point. In this case, a certified IT security service provider can help,” explains Holger Funke, Director Business Development, who is responsible for managing the test centre.



Holger Funke
holger.funke@secunet.com

secunet is the first BSI-certified company for incident handling.





Social Days

Taking responsibility together

secunet is Germany's leading cybersecurity company and stands for the best possible protection of digital infrastructures, data and applications. But what else does secunet stand for? What values does secunet represent as a company? What makes secunet special? Who better to answer these questions than the drivers of the company's success: the secunet employees. Together they have formulated the company values. In this context, one of the key statements is: We take responsibility together. And we do so actively. To ensure that this statement – even apart from business – does not remain a theoretical declaration of intent, secunet is committed in the form of the newly established Social Days. secunet supports social projects in the area of children's and youth work financially and with the commitment of its employees. It all started at the major locations in Berlin, Dresden, Essen and Munich. More than 100 employees took part in gardening, the embellishment of outdoor areas, visits to museums or upcycling activities with primary school classes. "A great day that was not



only fun for the children. Besides the social commitment, we were able to get to know new colleagues, work successfully as a team and do something good together. We will definitely be back for the next Social Day," was the summary of one participant. "A big thank you goes to all secunet employees who took part this year and actively live our values together as a team. We look forward to the next Social Days," says Axel Deininger, CEO of secunet.

Dates – September to December 2023

20 – 21 September 2023
PITS Public IT Security |
Berlin, Germany

25 – 26 September 2023
AUTOMA+ | Zurich, Switzerland

10 – 12 October 2023
it-sa | Nuremberg, Germany

10 – 12 October 2023
JAPCC | Essen, Germany

11 – 12 October 2023
LEA DER | Prague, Czech Republic

18 – 20 October 2023
Intergraf | Bilbao, Spain

14 – 16 November 2023
Space Tech Expo |
Bremen, Germany

14 – 17 November 2023
Milipol | Paris, France

29 – 30 November 2023
Berlin Security Conference |
Berlin, Germany

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

Imprint

Publisher

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

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

Marc Pedack, marc.pedack@secunet.com

Design and Setting

sam waikiki GbR, www.samwaikiki.de

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

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. 3, 5, 8, 10, 11, 13, 16, 17, 26, 27, 30: secunet
p. 2 (top), 6, 22, 23, 28: Getty Images
p. 2 (bottom), 18, 29: Adobe Stock
p. 12: iStock
p. 21: Dieter Seibel, Wangen



As private as required, as public as needed.

secunet - cloud solutions thought through.

Being a long-term IT security partner of the Federal Republic of Germany, we design sovereign cloud solutions already today according to your needs - on-premise, public or also combined as a flexible hybrid cloud.

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

secunet