EURO SECURITY

The international trade magazine for security and management in the EMEA region

- **Perimeter Protection**
  Outlook for the year 2023 - technologies and focal points

- **PMRExpo 2022**
  New solutions for Communication solutions in the KRITIS area

- **Retail trade**
  EuroShop Düsseldorf - EHI Retail Institute: Metaverse in retail

ISSN 09481249 • 1-2023 • ZKZ 16724 Postvertriebsstück bezahlt • 80383 BAY Germany ©SEC Global • euro-security.de

Content

ADVERTORIAL

APPLICATION STORIES

BUILDING DESIGN

CYBER SECURITY

EVENT/REPORT

EXIBITIONS

MARKET OUTLOOK 2023

MARKET REPORT

Content

PERIMETER PROTECTION

PMREXPO

RETAIL SECTOR

ROUND TABLE

VIDEOTECHNOLOGY

—- www.eurosecglobal.de —

ISSN 09481249 SEC Global Ltd; P.O. BOX: 45276 AJMAN FREE ZONE; AJMAN, UAE; info@sec-global.org websites euro-security.de & eurosecglobal.de

Agency (Press & Advertisements)
Euro Security Fachmedien (ESF)

Postal address
Grabenfeldstrasse 25
83083 Riedering, Germany
Phone: +49 (0)8036 3035071 Websites
e-mail addresses
editorials@euro-security.de /
anzeigen@euro-security.de

Websites
eurosecglobal.de / euro-security.de /
euro-security.tv / ki-zeitschrift.org /
public-security.org / sicher-magazin.de/
sec-global.org /

Can trade fairs return to their former strength?

In 2022 - after the two Corona years - it became apparent that our society and economy had suffered from the effects of the pandemic. And this development did not simply pass the security industry by. In spring, companies tentatively opened their doors again and resumed normal business activities. It quickly became clear that the shortage of skilled workers and labour also had a decisive impact on our sector.

Nevertheless, the worldwide epidemic has also had a decisive impact on security companies: the degree of digitalisation has at least increased in corporate communication - in external communication and in internal dialogue. Video conferences via Zoom and other solutions are now integrated into the daily routine in the company, save costs and enable a more intensive exchange of opinions. And yet, all market players were happy when events such as trade fairs and conferences were also on the agenda with the opening. Everyone was happy to again cultivate business relationships and develop projects in personal exchange.

The trade fairs, which had been so successful in the past, at which the companies of the security industry exhibited, had not yet found their way back to their old strength, and the global context in which the German security companies had previously operated also suffered considerably. The trade fair events no longer reflected the international security industry and were fragmented. Let's hope that the coming year will bring more success. But the chances are good.

This is how the new year starts with Perimeter Protection 2023. Messe Nürnberg, as the organiser, is reporting a record number of exhibitors and is now naturally also hoping for corresponding visitor numbers. After all, the range on offer at the Nuremberg Exhibition Centre takes into account the top themes of those responsible for security in Germany. Thus, the focus is not only on mechanical and electronic property security. Intelligent, AI-based video technology or security services such as drone protection are also on the agenda. This is a response to the demand for better protection of critical infrastructures (CRITIS), but also for security solutions for the private sector. Other important trade fairs also take place in Nuremberg. What would the German security industry be without Feuertrutz or it-sa, which are key events for the industry?

Other fairs, such as SicherheitsExpo in Munich, have to prove themselves again this year. After a change of ownership and a slight market fatigue, new accents must be set this year to build on the successful pre-Corona period.

PMRExpo is also facing a new beginning this year. The trade fair, which was previously only held at the exhibition centre in Cologne under a different organisation, will in future also be planned and carried out by the management of KölnMesse. A look into the future is also interesting for this special trade fair. This trade fair, which is limited to control centres and communication, could receive a growth impulse by expanding the topics on the basis of the technologies presented here.

Control centres are the basis for a multitude of project solutions in the modern digital world. Thus, the topic of smart cities would certainly be an enrichment for the trade fair taking place in November. It remains to be seen what the hitherto authoritative association would think of such a thematic expansion. It would certainly be worth considering.

Hopefully, the year 2023 with all the different events will be purposeful for the security industry. Because the year 2024 should at least have another leading trade fair in store where innovations of the German and international security industry are shown and find their home. There is no question that the industry needs this.

Dr Claudia Mrozek

New products. Exceptional services. See access control in action at Intersec.

Are you coming to Intersec 2023 in Dubai? We hope we'll see you there! We'll be at the Dubai World Trade Center on January 17-19 to demonstrate the latest innovations in physical access control. You can find us in the German Pavilion, Booth SA-D18, Hall C.2. Need more time with us, or have specific issues to discuss? Schedule an appointment in advance to talk to one of our application experts.

We will be showcasing the products, services and solutions that define the future of access control for the Smart Building, Smart Office and Smart City. As buildings become increasingly networked and intelligent, they need to be able to think, learn and act autonomously for the benefit of their occupants and operators. That means access control solutions must also adapt—to become smarter, more responsive and more versatile. At the same time, solutions are needed that improve ease and convenience for tenants, workers and visitors while maintaining optimal security at all times. And, of course, you want solutions that look as good as they work.

That's where sesamsec comes in. We have innovative hardware, software, and cloud-based services for any access scenario, available as independent components or in one easy-to-implement package. You won't want to miss the opportunity to talk to us face-to-face at Intersec about your access control needs. Looking for innovative design and versatile applications? Need high-security access solutions? Curious about cloud-based access control systems? You can find it all here, at sesamsec. Plus, a Professional Services team who can help you get it all done—without breaking a sweat.

Innovations in access control

Stylish. Universal. Practical. Our access control hardware fits your environment and prepares you for the future. See the latest sesamsec products at our booth.

We offer a wide range of readers and access hardware, all manufactured to exacting specifications for reliability, durability, security and aesthetics. Readers are available in different color variants to harmonize with any environment and are available with or without keypads to meet different security requirements. And they support both classic card technologies and mobile credentials via smartphone or wearables for a versatile access system that is ready for the future.

Here’s what sets us apart.

- Modern, versatile design options: Our readers are distinguished by high-quality materials, modern aesthetics and exceptional versatility. With or without keypad, in bright silver or sophisticated charcoal, they look great anywhere—and are tough enough to stand up to the elements.
- Universal readers: sesamsec readers are compatible with up to 60 transponder technologies used worldwide, plus BLE and NFC for smartphone credential systems. That means they can be integrated into practically any system, anywhere, and support the technologies you and your clients are already using.
- Easy implementation: From physical mounting to software integration, our access control systems are built for fast, simple implementation. And with remote upgrade capabilities, it’s easy to update firmware or make configuration changes after they are installed.

PAC as a Service

The future lies in the cloud! You know about Software as a Service (SaaS). What about Physical Access Control (PAC) as a Service (PACaaS)? Our cloud-based PAC systems offer more flexibility, proven reliability and future-proof scalability. In a PACaaS system, all the necessary components for operating the access control solution are made available via the cloud. Cloud-based software gives you complete visibility and control of your access system and data from anywhere. No need to worry about servers, software or storage space: it’s all managed in the cloud, safely and securely. No large acquisition costs, either: just a simple monthly deployment fee, based on the exact services you need. PACaaS also offers advantage in terms of scalability. Get what you need now, and grow your solution for the future. You can choose your level of support, too, so you can customize your access solutions for your requirements and budget. PACaaS takes the hard work of designing, implementing and managing access control off your plate so you can focus on your core business, knowing your security is in good hands.

Professional services for installers and partners

Grow your business with the experts at sesamsec! With us, you are never on your own to support your customers. We offer easy entry into the world of cloud-based access control and help you meet customer requirements for security, availability and timeliness. Having a sesamsec expert at your side is a distinct competitive advantage for suppliers and installers of access solutions.

With our Professional Services offering, our installers and partners can draw on our expertise when implementing a cloud-based access control solution. sesamsec manages the complete implementation of the solution—from planning to installation and commissioning to monitoring. All of this is done in close coordination with our partners, so they can easily meet their customers’ requirements for a modern access control solution in terms of security, availability and updates.

We work with our business partners to help them deploy and scale access solutions, support their installations, and manage digital transformation for themselves and for their customers. Through smart cloud-based tools, expert advice and training, and ongoing support.

We can help you with:

- System planning
- Project management
- Customized interfaces
- Commissioning and monitoring
- Training and post-installation support

Talk to the access experts at Intersec.

We would love to have the opportunity to meet you in person at the fair. Stop by any time during exhibition hours or contact us to set up a personal appointment. We can’t wait to see you there! We’ll be at booth SA-D18 in Hall C.2, in the German Pavilion. Our experts will be there to answer questions, showcase our products, and talk about our service options.

Can’t wait? Or can’t make it to Dubai? We’re always here to help, wherever you are. We are happy to receive your call at any time to answer all your questions. The sesamsec team is standing by to help you solve your access challenges and prepare your organization for the future of access control.

76%
57%
x 1000

Everything from a single source

The practical event SITE SAFETY 2022 by KÖTTER SERVICES in Bremen as a first-time event in the context of security concepts for construction sites, shipyards and CRITIS areas with renowned partner companies.

KÖTTER Security held an 'Open Day' in Bremen on 6 October 2022 for Security & Services for construction sites, shipyards, and ISPS facilities. With over ten partners*, a variety of different topics were presented. The practical event for architects, planners and those responsible for security in the construction industry opened interesting perspectives for the areas of construction site security. Particularly through a total solution for secure 'sites', greater freedom in business processes results for customers.**

In the past, criminals have seen construction sites as self-service shops for their raids in all regions of the Federal Republic. Not only construction machinery and vehicles have been stolen from construction sites in Germany and disappear never to be seen again. Valuable building materials (wood, insulating materials), objects made of metal or with a high metal content (e.g., non-ferrous metal and copper, cables of all kinds and tools are also highly sought after by criminals. According to the police, the stolen goods are selected on 'order', quickly resold, or even used themselves. Construction machinery that is not taken abroad is also resold by fences.

The economic and organizational consequences are considerable: immense costs for replacement purchases, delays in the completion of construction, discussions with customers and insurance companies hinder the progress of construction and delay the completion of the objects.

According to the Federal Criminal Police Office, the number of reported

thefts on construction sites was 22,773 (2021). And around ten percent are only solved.

In insurance terms, this means that construction companies and craftsmen on building sites basically hold until acceptance. So they are also responsible for any movable goods (construction machinery, vehicles and tools) on a construction site and must replace them if they are stolen. Based on current case law, this means that it remains a considerable risk for a crafts enterprise to store tools and materials on the construction site until acceptance is complete.

In addition to theft, incidents of vandalism have also increased in recent years. Arson and willful destruction of parts of shells and other parts of buildings are unfortunately not uncommon.

The bad guys usually come under cover of darkness and so lighting concepts and video cameras that can record or report events at night are particularly important. In combination with other security solutions, perpetrators can be approached, or alarms can be set off by a security service, thus driving away even those who have already trespassed on properties. Prevention and security concepts for 'sites' and especially construction sites have been in high demand for some time now in view of the crime rates. KÖTTER Security also offers construction site operators and property owners comprehensive security solutions with personnel and technical solutions. A characteristic feature of KÖTTER's services is the so-called precinct guard service, which checks the condition of construction site areas several times a night (on weekends or public holidays also during the day). This security service is primarily for prevention and intervention.

In addition, the Essen-based company offers technical safety concepts for the entire construction site cycle with selected partners: The customer thereby concludes a contract from a single source: all trades, including those of partner companies, are coordinated by KÖTTER during the entire construction phase. Construction fence banners around the construction site indicate that the site is monitored and protected. Uniform safety standards make an efficient solution possible on site nationwide, which are adapted according to the progress of construction.

Safety and occupational health

KÖTTER is aware of the importance of an effective operator model for planning, setting up or operating construction sites. A preparation of risk assessments and the definition of the required occupational safety specialist on site are part of the service concept. Not only do the numerous trades have to be coordinated, the aspects of occupational safety in Germany and health protection must also be guaranteed.

The legal requirements of customs and the employers' liability insurance associations are important framework conditions that must also be considered in safety concepts. The right work clothing, e.g., the obligation to wear a helmet on the construction site (mandatory personal protective equipment), or access to the construction site must be regulated in accordance with the law.

Access management

With the partner IQ-Pass, an integrated access control software ensures

documentation of various data and documents that are essential for construction site operators today. The company and personal registrations that legitimize access to the construction site are checked, as is the registration of workers with the relevant social security systems (building cooperative, health, and pension insurance). Of course, general legitimation checks (ID & A1 checks) can also be requested, and a minimum wage check (monthly minimum wage check) is included. This contributes to the fight against undeclared work on construction sites.

Attendances (entry and exit, entry, and exit) can be documented using a standardized evaluation platform. This data can be accessed via cloud-based access from anywhere in the world, which is important for globally active companies. Regarding asset management on the construction site

“We offer customers a solution"

Daniel von Grumbkow, Regional Manager and Authorized Officer and, from 1 January 2023, Managing Director of KÖTTER SE & Co. KG Security Hamburg, presents the service portfolio of the industry giant in a statement.

"SITE SAFETY 2022 was presented to the trade public for the first time in October. Due to the success of the event, we are planning this event at other locations in the Federal Republic next year. We chose Bremen for the first event because of its geographical location. Construction site safety is not just about classic building, civil engineering and new construction or reconstruction. Many shipyards and port areas are also located in the region. At the same time, every shipbuilding site represents a construction site and is also subject to similar or the same legal requirements as a conventional construction site. And these concepts that we offer here are just as interesting for the area of critical infrastructure (KTRITIS). Especially for port facilities in the International Ship and Port Facility Security Code (ISPS Code). That's why we chose Bremen as the location for our first practical day with our partners."

Services around security for construction sites

"KÖTTER SERVICE offers services for construction sites beyond the classic service. Normally, a developer looks

Mike Jürgens, Managing Director of KOOI Security Germany, presented the video solutions used by KÖTTER Security in Bremen. He particularly pointed out that due to a lack of personnel and tight budgets, video surveillance nevertheless guarantees the necessary level of security on guarded properties. He also rated the event very positively and is looking forward to the events in 2023 [Photo ©DCM2022].

for a security service provider who needs guarding personnel, in the second step he needs a service provider who provides video technology and in the third step still someone who offers customs-compliant visitor management systems.

KÖTTER Services offers this package from a single source. With this, the customer has already ticked off three topics. But this is not all. In addition, there are other services that customers need nowadays. KÖTTER offers everything from planning to implementation to sustainability audits."

- "In the planning phase - phase 1 - we support the client e.g., in the preparation of security concepts as well as hazard analyses, occupational safety and fire protection concepts."
- "In phase 2, in construction support, we are on site with the first guarding activities, implement the customs-compliant security management and ID system and install the first security technology, e.g., video management systems."
- "In the third phase, the construction phase itself, we are additionally on site for site. This scales from step to step: with fire guards, rescue, or company paramedics - also other units of the company rescue system and fire brigades. The hardware, perimeter protection and also access controls are further expanded or developed depending on the progress of construction."

"This means that security concepts and solutions are adapted to the construction progress and are scalable and thus individually designed for each customer.
The customer has a contact person who offers everything from one source as an 'all-round carefree pakkage', implements it and manages the trades. An operational contact saves a lot of planning time and last-but-not-least: the customer receives an invoice from us on which everything is settled."

area, a corresponding exit control can take place, which ensures that all machines and tools really remain on the construction site area.

Video management

Because every construction site has individual characteristics, different security measures are naturally required. Video surveillance has proven to be an obligatory solution for projects in recent years: With the KÖTTER Security Video Tower, the Essen-based company offers a video tower that can be extended up to eight meters.

This ensures a high level of protection against theft, vandalism, sabotage, and manipulation. Unauthorized persons (or vehicles) are detected fully automatically, recorded, and can be deterred from any criminal intentions via a live address. The Video Tower can also be used to document the progress of construction work, and, thanks to this mobile solution, the location of the Video Tower can be variably adjusted depending on the progress of construction work. But permanently installed video cameras can also be used, e.g., on large construction sites. **[www.koetter.de]**

*Topics & live demos on site: Construction site security, alarm activation and intervention; barrier systems, perimeter protection and video systems; construction containers, turnstiles and access control systems; customs-compliant access management; preventive and defensive fire protection; occupational safety and safety instructions; operational sanitation; digital construction documentation; planning, construction, maintenance and service; construction cleaning and final construction cleaning.

** Companies on site: KÖTTER Security; KÖTTER Cleaning; German Business Protection; TERAPON Consulting; CSS Computer Security Service; BAU.CAMERA; KOOI; IQ-Pass; Comp-Pro; ESB Solutions

PERIMETER PROTECTION

Video systems: Keeping an eye on perimeter protection

Cameras are the eyes of modern security systems. This makes them an indispensable part of perimeter protection. Especially when large areas or several locations need to be centrally monitored, video technology can bring its advantages to bear..

©MesseNürnberg

Video systems are perfect for making recordings during access control, as part of burglary protection or for motion detection, from which further measures can be derived. Ideally, they are individually tailored to the respective application and the objects to be protected. However, cameras often pay for themselves through their deterrent effect: visibly installed, they can prevent unauthorised intrusion or criminal acts.

Depending on the requirements, the selection ranges from cameras that only provide the pure video image to high-tech solutions with complex analysis options. The devices themselves can come up with intelligent features and provide information for perimeter protection with their sensors. If only the detection of movements is required, slimmed-down video systems or intelligent video cameras are sufficient. They only trigger in the event of an alarm - i.e. when a movement is detected.

Video surveillance as part of the IoT

If more effective solutions are required, it is advisable to network the video systems with the security IT and other site protection components. They are connected to servers via the Internet of Things and combine the electronic processing in the camera with other software applications. For example, if the system reports card use at an access point, the camera triggers and the image recognition software can identify the vehicle number. Software and interface standards as well as norms such as DIN EN 62676 "Video surveillance systems for security applications - Rules of application" facilitate the integration.However, the security-relevant use of cameras can go far beyond the detection of unauthorised persons or vehicles on the premises. Equipped with thermal imaging sensors, they can not only detect people in all lighting conditions, but also detect fires and smoke development at an early stage, for example.

Video codecs and digital recording devices offer further possibilities through their computing capacity and storage space. These include, for example, artificial intelligence. Algorithms make it possible to use given data or knowledge from the past to better recognise events and avert dangers.

Only a protected video system increases security

However, the use of video technology on the premises also has its pitfalls. Data protection and data security must be taken into account from the very beginning of the planning process to ensure legally compliant use. As far as data protection is concerned, marking the monitored area is often enough. In addition, there are company agreements and the protection of the privacy of employees or visitors, e.g. in changing rooms.
As with all networked systems, it is important not to make the security system a gateway for attackers. Video images, sound recordings or movement patterns can be exploited by criminals. For this reason alone, it is advisable to integrate the video surveillance system into the IT security infrastructure.

Planning video security technology

When planning video systems, the required image quality plays a major role. Aspects such as contrast, resolution, images per second and resistance to weather influences must be reconciled. If, in the worst case, the images cannot be used or are not analysed satisfactorily by the software, companies are saving in the wrong place. In the worst case, a video system that is too powerful can cause investment costs to skyrocket. Costs and required image quality should therefore always be the basis of the investment decision. Experienced advisors provide valuable services in planning - at the Perimeter Protection in Nuremberg, for example, the experts for video surveillance can be found.

Even after a system has been installed, it is necessary to continue to maintain the hardware and keep the software permanently up to date. This is the only way to maintain functionality and ensure cyber security. Lack of maintenance leads, for example, to frequent false alarms and thus calls into question the acceptance and purpose of the system. Therefore, careful instruction and training of security personnel and the definition of responsibilities as well as testing and maintenance schedules are important. If the resources are not available in the own company, there are qualified security providers who continuously keep the systems up to date.

So when investing in a video surveillance system, companies need to consider various trade-offs that vary from property to property. Once the right application has been selected, this often results in further advantages for the security of people and assets.

PERIMETER PROTECTION

Trade fair for perimeter protection, fencing technology and building security - Exhibition Centre - 90471 Nuremberg - Date & opening hours - 17 - 19 01.2023 - 09:00 - 17:00 (17 and 18 January), 09:00 - 16:00 (19 01) > Free admission ticket with codePPEUROS23LIT:
👉 https://lnkd.in/e7tTagfk

PERIMETER PROTECTION

Drones - Danger from the Air

Aerial drones for private and commercial use can now be found in every DIY store. With their wide accessibility and increasingly powerful cameras and sensors, unmanned aerial vehicles pose an increasing threat to perimeter protection.

Drohne - Gefahr aus der Luft // © unsplash

In recent years, drones have developed into electronic mass-produced goods for everyone. The technological development of the devices is progressing at an unimagined speed and can be compared to the leaps in development of mobile phones. Companies and authorities in the security industry have been making use of the flying eyes for some time now in order to maintain an overview when securing premises or events. They provide indispensable services in the surveillance of open spaces, industrial areas and critical infrastructure facilities. In the event of an alarm, drones provide video recordings within minutes and thus information for site protection.

But with prices from 50 euros upwards, everyone can now afford a drone - and so can criminals. They detect security gaps in the airspace, use the cameras to spy on company secrets, smuggle drugs over border fences or weapons and tools into prisons. They can also be used to tap data from company networks. Companies and organisations should therefore determine their individual drone risk, identify weaknesses in their security system and take precautions.

EU recognises security risks

Incidents involving drones are becoming more frequent - including an increasing number of critical situations.

In May 2022, for example, the Brandenburg police reported that a drone came dangerously close to a passenger aircraft and obstructed the approach to the capital's airport BER. A few months earlier, a quadrocopter missed a Boeing 737 with 189 passengers on board by only a few metres. Apart from the threat to air traffic, incidents in which residents feel spied on by flying cameras are now commonplace.

The EU has recognised the growing security risk and introduced a regulation in 2021 that puts the operation of drones on a legal footing. Drones weighing more than 250 grams must be registered and operators must comply with certain requirements. A remote ID acts as a digital ID and recognisable registration. However, the likelihood that criminals will use a registered drone is rather low.

The EU has recognised the growing safety risk and introduced a regulation in 2021 that puts the operation of drones on a legal footing. Drones weighing more than 250 grams must be registered and operators must comply with certain requirements. A remote ID acts as a digital ID and recognisable registration. However, the likelihood that criminals will use a registered drone is rather low.

A drone is essentially a flying computer. And just like them, they can also be used for cyberattacks, for example to tap data. Those who use drones for perimeter protection should also be aware that a vulnerable target is floating through the air with them.

It is also conceivable that malware could be smuggled in via the often poorly protected drone software. Drones in the service of one's own security department should therefore definitely be checked by the IT department and equipped with appropriate protective measures.

Passive defence as the only choice?

Defence measures are usually limited to structural or technical options to make flying over more difficult or to detect unauthorised drones. These include installations, but also detection devices. In the vicinity of prisons, for example, nets prevent intrusion into the airspace of the compound. Privacy screens, on the other hand, conceal sensitive areas on company premises.

Even birds of prey have been considered for drone defence: Police in the Netherlands tested the use of eagles to capture drones. After a test phase, however, the authorities found that the training and efficiency of the birds was more complicated and expensive than expected. The programme was therefore discontinued.

In the meantime, sophisticated systems are available to detect and repel drones. However, many of the solutions offered for active drone defence are not approved in Germany. For example, the use of jamming or spoofing is reserved for official and military security installations in Germany.

Passive defence measures with which companies can protect themselves range from radar and camera detection to RF-3D detection with high-frequency detectors. The industry will present these and other drone defence solutions at Perimeter Protection 2023 in Nuremberg.

The trade fair focuses on the security of open spaces and outdoor facilities and integrates the U.T.SEC platform, which focuses on the technical, legal and practical options for the use and defence of drones and other unmanned technologies.

Perimeter Protection in 2022

Several trends can currently be observed in perimeter security: On the one hand, the use of video technology has increased considerably and, on the other hand, the integration of additional, technical solutions is being intensified. Users are increasingly relying on the use of sensors and combinable technologies. For example, they are trying to incorporate preventive solutions such as thermal cameras or radar applications into solution concepts. In combination with lighting concepts and audio applications, deterrence against criminals is efficiently possible.

It is particularly important that the technologies used are open in their standardisation. The existing IP structures again result in new risk structures. In view of the fact that every endpoint of the network represents a potential weak point for cyber security, and because of the general threat potentials from cyber attacks, both physical and IT security must be considered holistically.

Security solutions for specific applications

Security in critical infrastructure environments (CRITIS) plays a special role in everyday life to underpin economic and social stability. Utility services in particular are the focus of protection concepts and the goal is to provide them securely and efficiently. With this. Perimeter security is a suitable technology for the protection of citizens, passengers, data and assets and prevents business interruptions of corresponding facilities.

Transport structures, such as seaports and airports, are also among the assets to be protected. Risks of terrorism and other threats and vulnerabilities are faced by many exposed facilities.

AI-controlled security systems

AI has made devices smarter. Based on data and system intelligence, faster and more effective decisions can be made than ever before.

Surveillance results from multiple security systems and thousands of cameras and sensors now converge on one platform.

By supporting the integration of any device, service or solution and bringing data together in a single area, organisations can achieve a different level of security.

Video technology is more important than ever

Video surveillance technology is part of a layered security strategy. Cameras complement security personnel and enable operators to effectively monitor and manage alarms in real time, while also collecting investigative and forensic data. Coordinated emergency responses are also possible. The combination of valuable video and security tools enables users to build more vital security programmes through intelligent data collection.

Feature-rich video viewing and policy-based distribution enhance emergency management, while containerised video management platforms serve as an intuitive platform that promotes a new level of situational awareness and enables rapid response. With many mission-critical facilities having to cut staff and also unable to draw on new security personnel, the demand for video technologies has skyrocketed."

The future

As with many other areas of physical security, perimeter systems are seeing more and more smart devices, integrated solutions and data-driven processes.

Ensuring cyber security has become imperative and system integrators are starting to offer this as part of their services. AI and video technology are more important than ever, providing operators with actionable insights and enabling them to respond faster and more efficiently.

Which technologies are shaping perimeter security?

According to the market research institute 'Markets and Markets', the market for perimeter security components will grow from 62 billion euros in 2020 to 98 billion euros in 2026. According to the forecast, the average growth rate is 7.9 percent.

Perimeter security is one of the growth areas in the security industry. As the importance of security solutions that are already effective at the perimeter of premises is growing, the demand for such solutions is very high. However, this is not only about securing open spaces and property or site boundaries of critical infrastructures (CRITIS), such as prisons, airports, or data centres, but also increasingly about applications in the private sector, such as logistics operations, industrial sites, or construction sites.

Perimeter security is designed to prevent people or equipment from entering a property directly at the outer perimeter or to trigger an alarm in the event of an intrusion attempt.

This type of security solution is important for a wide range of businesses and institutions. Security concepts around perimeter security include threat detection through sensors, each with its own detection method. Some technologies have gained in importance in recent years or are part of the basic equipment of a solution. We would like to introduce these in the following.

1. lidar sensors send laser pulses into the environment and calculate the distance of an object based on the time it takes for the pulses to travel back. One of the advantages of this technology over video technology is that it is independent of light and weather conditions. Since lidar is not only used in the security industry but is also used in the automotive sector in particular, the prices for lidar solutions have dropped considerably in recent years. As a result, lidar has become interesting for outdoor operation and is now used in many applications.
2. fibre optic sensors transmit laser light pulses via fibre optics and measure the light reflections that occur along the fibre. A disturbance of the fibre, caused for example by touching the fence, changes the amount of light reflected from that point. From an expert's point of view, fibre optics is a cost-effective solution for smaller sites with an above-average lifespan.
3. Wireless solutions and wireless communication between the sensor and the main system are becoming more and more important, especially for residential and small to medium sized commercial buildings.
4. Remote and monitoring functions are also in particularly high demand. Control via smartphone for remote control and monitoring is now state-of-the-art, especially from the private sector. This technology is also particularly important in-home automation.

5 Video surveillance is particularly

important at present. It has now become a mandatory technology for perimeter security. Increasing remote surveillance is important, not least because of the continuing shortage of employees. In the perimeter area, there is automatically a greater need for visual verification to reduce costs and the number of false alarms.

Other sensors are valuable in determining who is entering or attempting to enter a property. Video allows service providers or operators to determine more clearly what the situation is from a distance.

To maximise the effectiveness of video surveillance and assessment, the video management system must be able to link the location of the alarm to a camera or PTZ pre-set. This allows operators to respond more quickly, requires less training, and the pre-programming allows for optimised video quality and memory settings. Site-specific deterrence measures are also quicker to implement this way.

Sensors in combination

Of course, each detection technology has its advantages and disadvantages. Using a combination of these technologies (sensor fusion) makes detection of security breaches more effective. Intelligent, integrated solutions require an interplay of the technologies presented here to maximise their strength. For example, sensor fusion can analyse real-time data together with historical, location, environmental and classified information before an alarm is triggered. This avoids false alarms.

Efficiency

Factors for efficient video technology in the context of perimeter security

The perimeter is the first line of detection in security systems for buildings and premises. How efficient security solutions are determines the effectiveness of the entire security infrastructure and whether an unwanted incident can be prevented before it occurs. Modern solutions offer various options for protecting a site. These range from different types of video surveillance cameras to motion sensors, analysers, thermal cameras or even radar or LiDAR. The basis of all solutions among all these options is still the surveillance cameras to provide evidence in image and sound.

However, installing surveillance cameras outdoors brings some challenges.

Temperature is an important factor when operating cameras. Extremely low temperatures can have a negative impact on any surveillance camera. Cameras can freeze, erode, and form ice deposits on the lens that can cloud the view. In worse cases, the unit may not turn on at all.

Condensation is a major problem that limits visibility and damages electronics. In surveillance cameras, condensation can cloud the lenses and cause the electronic components to erode over time. If cameras are installed in a location where they are constantly exposed to air pressure fluctuations and rain, there is a risk that seals and components will crack, causing moisture to accumulate inside.

Weather conditions are not the only enemy of surveillance cameras. If the cameras are in a maritime environment, the salt content in the air can cause the equipment to corrode over time. A similar problem arises if the camera is used in medical or industrial areas where strong chemicals are used.

By observing the IP rating (IP = Ingression Protection), protection from outdoor conditions is possible. The IP 66 rating protects against solids such as dust and liquids such as rainwater, providing a high level of protection. It is also important to pay attention to the correlation of the operating temperature with the temperature of the installation location. In general, the installation location has a great influence on how well a camera works. The quality of the surfaces on which cameras are mounted is also important. This is because they can easily transmit temperatures and thus also influence the operating temperature.

After growth in 2022,
things get a little jerky in 2023

In 2022, the majority of the 50 largest international security companies in the video surveillance and access control sector posted significant market growth. Despite these positive overall results, experts predict that the industry will struggle in the coming year.

According to the market report 'Security 50', the top 10 companies will be able to maintain their sales figures. Thus, the ten largest manufacturers in the video surveillance and access control sector (sales comparison to 2021: Hikvision Digital Technology,
Dahua Technology, ASSA ABLOY, Axis Communications, Motorola Solutions, Uniview Technologies, Tiandy Technologies, Allegion, Hanwha Techwin and Aiphone will not record any losses. Hikvision's market leadership becomes particularly clear when one realises that in 2021 the 10-billion-euro sales mark was exceeded. This represents a growth rate of 16.9 per cent compared to 8.7 billion euros in sales in 2020.

Hikvision sees itself in this prime position by pushing technological innovations, which are the key elements for business success. According to Frank Zhang, VP of Hikvision, the continuous development of products and market position supports the customer relationship and builds long-term trust.

Six companies were newly included in the 2022 Security 50: China's Dnake (intercom), Jovision (video) and EVETAR (lens), US-based Evolv, a screening provider, Australia's Ava Group with risk management solutions, and Korean video surveillance provider Webgate are now among the top companies. Fifteen companies in the top 50 come from China alone. And four in the top 10 alone: Hikvision, Dahua, Uniview and Tiandy.

Due to the COVID situation in China, Chinese companies had to absorb revenue declines in the first half of 2022 compared to 2021. US trade sanctions on Chinese companies and products have less impact. Taiwanese manufacturers such as Dynacolor, Hi Sharp and GeoVision are doing well and by focusing on niche solutions, the market position has been stabilised. The economic outlook is heavily dependent about OEM orders to Taiwan, which cannot yet be conclusively assessed.

Review 2021-2022: In biometrics, access control, video analytics and digital intelligence, companies all recorded significant growth this year.

This is due to increased demand for security and network video solutions and dynamic technological development. Thus, new, and more innovative products and solutions are in demand, replacing old technologies.

Forecast 2023: The security industry faces recessionary threats. The post-COVID era holds a multitude of problems:

1 For example, component and raw material shortages are causing problems in the supply chain. And pandemic-related closures have also led to losses. The supply chain crisis slowed growth in 2020 and 2021, but market leaders like Axis now see a return to double-digit growth. Diversification of supply chains by some manufacturers led to shifts in the market.

2 Strong inflation is affecting the prices of services, labour costs and raw materials. Thus, price increases for security products can also be expected in 2022 and 2023. At the same time, relationships with customers have changed and both payment and service models have changed. Customers are thus not overcharged but can continue to do business in a planned manner.

3 Of course, the conflict between Russia and Ukraine is also influencing the economic situation. In both countries, the economic activity of global security manufacturers and providers is currently at a standstill.

4 The impact of data protection regulations on video surveillance and AI-enabled technologies is interesting. Thus, the industry is challenged to respond to the regulations and take them into account in software developments.

According to the Top 50 report, 2023 could hold bleak growth prospects for physical security. in 2022, the security industry saw growth again. According to industry runner-up Dahua Technology, Asia Pacific, Africa, Latin America, and the Middle East will be 'relatively' optimistic, however, relatively weak growth will occur according to the Chinese manufacturer's forecast.

The global market for video surveillance hardware and software is expected to grow by 11.7 per cent in 2022. In 2023, it will grow by 6.4 per cent. In the longer term, there will be sustained and significant growth in the high single-digit percentage range.

Due to the economic problems already mentioned, fewer investments in safety technology will be realized. This makes relationships with existing customers more important, as replacement investments can be implemented here to reduce the costs of existing (security) management, among other things.

Trends continue to be dominated by artificial intelligence (AI), edge computing, cloud solutions and cyber security. From the market leader's point of view, visualization solutions will be increasingly used.

Especially multidimensional technologies such as radar, thermal imaging, X-ray fluoroscopy, temperature measurement, moisture measurement and gas leak detection will be given more space.

This will make safety solutions more efficient. In general, the role of sensors in security applications is becoming more and more important.

[The article is based on information on www.asmag.com]

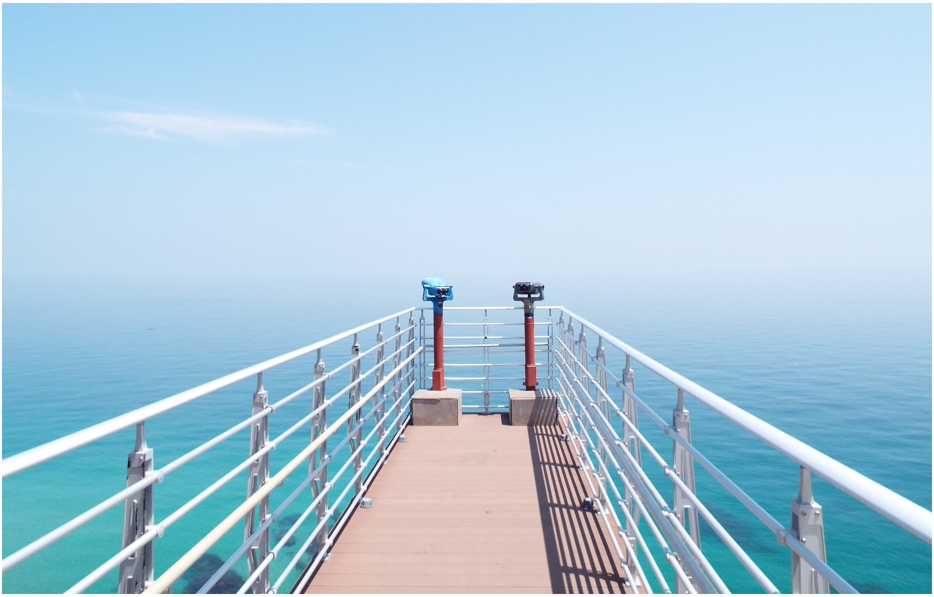
Business communication: Five trends for 2023

Strengthening resilience with digitalisation, automation and cloudification

From the Russian war of aggression against Ukraine to the supply chain crisis and deglobalisation: economic systems are currently under great pressure. Rising inflation and the prevailing shortage of skilled workers are further tightening the situation. To keep their business going against this backdrop, companies need to rethink their communication processes accordingly. Munich-based enterprise cloud service provider Retarus has identified five trends that companies should keep in mind for their business communications in 2023.

1 Cyber resilience as part of the business strategy

In uncertain times, companies must reckon with increasingly perfidious attacks on their communications infrastructure. Ransomware is still considered the main threat, while email is the most common gateway. As cyber-attacks have a direct impact on business success, cyber resilience must be a topic at board level. To en-



sure that central processes and infrastructures function even under extraordinary circumstances, business continuity concepts should include strategies for emergencies in addition to comprehensive mechanisms for advanced threat protection. For example, an email continuity solution outside the company's own infrastructure enables seamless communication via email even in emergency situations.

Geopolitical conflicts further increase the risk of cyberattacks from certain regions. With services such as Retarus Predelivery Logic https://tinyurl.com/3tyydk78, messages can be isolated based on their GeoIP as a precaution - whether for purely security reasons or due to internal compliance requirements.

2 Sustainable cloudification of business models

Digital business models are catching on. The cloud forms the basis for this. At the latest since the COVID 19 pandemic and the associated home office regulations, digital offerings and virtual collaboration have become established.

Cloud computing is now firmly established in IT departments. On the other hand, companies are facing considerable cost pressure. Budget managers are required to plan as cost-efficiently and sustainably as possible. Here, too, cloud services provide a remedy. They are flexible and scalable, so that the services can be adapted exactly to the current demand and over- or under-capacities can be avoided. As a result, innovative offers can be introduced to the market more quickly and costs can be better regulated.

Companies benefit from cloud service providers who relieve the burden on their own IT infrastructure with platform offers, managed services and innovative solutions. Companies are also optimally supported in introducing new business models, as a cloud service enables agile action and direct, fast communication to the market. The Retarus Enterprise Cloud (tinyurl.com/5hahp2z)3, for example, provides a wide range of services that companies can use for various application scenarios in different industries. The services meet all common industry standards. Standard interfaces enable seamless integration into on-premises, cloud and hybrid infrastructures.

3 Increased automations in the supply chain

The past year has shown how susceptible supply chains are to disruption. In addition, companies are currently feeling the skills shortage more than ever before. In 2023, companies will therefore need to make their supply chains more resilient and rely more on automation technologies. This will help them address the growing skills gap and increase productivity in the supply chain.

For example, automating the capture and processing of incoming business documents eliminates the time-consuming manual data entry of goods orders and purchase orders. Companies benefit from more efficient process communication, smooth cash flow and cost reductions of around 60 per cent compared to manual order processing. Professionals can focus on innovation again, ideally giving the company a competitive edge.

4 Optimized customer journey

Not least because of the pandemic, customers have increased demands on digital offers. They are now used to digital interactions and touchpoints. A positive customer experience is a basic prerequisite for business success. Only reliable, secure, and individually designed business communication makes it possible to offer a wide range of touchpoints with customers, thereby creating customer satisfaction and loyalty. Companies that do not invest in their customer communication lose customers to their competitors. With digital communication platforms, companies serve digital touchpoints such as multi-factor authentication, email order confirmations, transactional emails such as newsletters, weather alerts via SMS or status messages. Ideally, the services can be seamlessly integrated into business applications or digital platforms via standardized APIs and quickly and flexibly adapted to new requirements at any time.

5 More complex data protection requirements

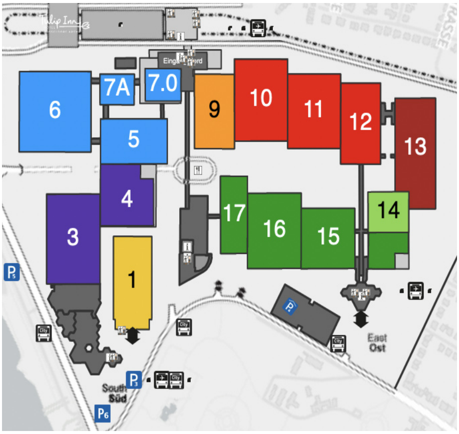
According to analyst firm Gartner, 75 per cent of the world's population will have their personal data protected by data protection regulations by 2024. Legal requirements are playing an increasingly important role, as regulatory requirements are constantly evolving internationally and becoming more complex.

Companies face heavy fines in the event of violations. When choosing an external service provider, it is therefore more important to ensure that the provider complies with all current data protection guidelines. Ideally, the service provider not only fulfils the GDPR requirements, but also industry-specific standards and individual compliance requirements.

All data should be processed in local, auditable data centers. Some providers already contractually guarantee this to their customers via service level agreements.

Retail Technology Stage in Hall 6 / I61

At the Retail Technology Stage, developments and trends in the field of retail technology will be presented on the basis of current use cases. Topics include mobile solutions, the latest developments in self-checkout and self-scanning, trends in analytics, RFID, IoT, smart stores and payment, as well as the latest security technology. Experience the dimension of retail technology not only in exchange with the exhibitors, who will present their latest solutions for seamless stores, customer centricity or the use of AI, but also take away incentives and inspiration from the presentations on the Retail Technology Stage. Visitors to EuroShop can attend the lectures at the Retail Technology Stage free of charge and without pre-registration and find out about the latest developments in compact presentations.



Event date & opening hours

Event date
26 February - 02 March 2023
Opening hours for visitors
daily: 10:00 - 18:00 hrs

Messe Düsseldorf GmbH
Messeplatz
40474 Düsseldorf, Germany
Tel: +49 211 4560-01
Fax: +49 211 4560-668
Web: www.messe-duesseldorf.de

Standards as trendsetters for the security industry

Standards by OSS in conversation with manufacturers and users

The non-profit organisation OSS-Association Open Security Association) establishes standardised protocols for the international security industry. Its members and affiliated companies develop components and codes for security-relevant hardware and software. As part of the first Media Talk, we asked Frederik Hamburg, Chairman of the OSS Association and Managing Director of ZUGANG GmbH, about his motivation and experiences with the adoption of standards in the security industry. We also spoke to Matthias Schmid, Manager in Business Development at ASSA ABLOY, about the advantages of using standards from a manufacturer's point of view. Another view from the manufacturer's perspective was given by Harmut Beckmann, Sales Manager at Uhlmann & Zacher, and finally Patrick Senneka, Senior Product Developer in the IT department of Fraport AG, showed us interesting perspectives on the use of standard access control from the user's point of view.

Frederik Hamburg, what is the motivation for you to stand up for standards in the security industry as chairman of the OSS Association?

The basic idea comes from the users and thus my motivation comes primarily from those who have many locks in use. Their concern was and is to break away from the proprietary systems of the manufacturers. Because in the meantime the demands on complex security systems have increased. The market is often confusing, and this is where the customers' desire arose for the different systems to be able to communicate with each other, completely independent of the manufacturers.

When was the OSS Association founded?

The OSS Association was founded in 2015. The idea from the beginning was to develop standards "from the industry for the industry". In addition, we wanted to go into further development whenever there are new requirements. The members of the OSS Association cover the entire spectrum of the security industry. Together, they can thus contribute to the further development of the standards. The aim is to connect the individual components so that, for example, the key card communicates with the software to read out authorisations for door locks and access control and time recording systems. This communication is based on standards by OSS to ensure compatibility with and independence from manufacturers of different brands.

Do the users have any influence on the further development?

Absolutely, the users are our first source when it comes to identifying the necessary further developments. The manufacturers and their customers enter into dialogue. Before the pandemic, we held user meetings to find out what customers wanted in direct contact. We are planning the next user meeting in 2023. Such user meetings serve to "listen to the customer" and to understand which components should be further developed and which should be added.

But we are also noticing more and more that the need for the use of standards is increasing - even if there are some manufacturers who do not yet want to acknowledge the advantages of standards. The use of standards also means opening up to other systems and taking the - admittedly small - risk that customers will (be able to) opt for other products because the proprietary nature is abandoned. But de facto the opposite is the case. With the use of standards by OSS, manufacturers become competitive and are always up to date in this respect as well, thanks to the constant further development of the standards always up to date in this respect. Individual components from different manufacturers can now communicate with each other. The end customer appreciates this flexibility, which can also lead to a reduction in costs, as the choice becomes greater and dependence on one manufacturer is eliminated.

ASSA ABLOY

As a manufacturer of security technology, ASSA ABLOY is the big player on the international market. In over 70 countries with more than 50,000 employees and an annual turnover of over 9 billion euros, the company is one of the leaders in the security industry. In the DACH region alone, 275 million euros were turned over by the ASSA ABLOY "Opening Solutions" unit in 2021, primarily in electronic access control, protective devices and locking systems. Mathias Schmid joined ASSA ABLOY Sicherheitstechnik GmbH in 2019 as Business Development Manager Access Control, where he is responsible for the further development of the solution portfolio in the field of electronic access control systems. We asked him about the development of standards from a manufacturer's perspective.

What was ASSA ABLOY's motivation as a manufacturer to promote the use of standards?

ASSA ABLOY has been using Standard Offline since 2015 and is one of the founding members of the OSS Association e.V. For our customers, end customers as well as system integrators, the expectation or requirement for us as a system and component provider was that the electronic fittings and cylinders could also interact with products from other providers. This was the starting signal for us to advance the topic of standards development together with the OSS Association

The Aperio product portfolio, which for more than 15 years has included both online integration via radio and offline integration via "Data on Card", supports OSS Standard Offline ex works. This enables our customers and partners to easily integrate Aperio components into their system and to communicate with other components as required. and communicate with other components as required. The customers are therefore opting for a product that convinces them.

At first, this does not seem favourable for the manufacturers. Because the times of proprietary systems are now a thing of the past and the supplier ties are dissolved to a certain extent.

So, what are the advantages of using standards from the manufacturer's point of view?

At first glance, supplier independence seems to be disadvantageous for manufacturers. But the opposite is the case. Because with the growing market requirements, everything that the customer is looking for and expects can be delivered. Because the integration of different components and products from different manufacturers made possible by the Standards by OSS often offers better solutions than a single supplier with a potentially limited portfolio can provide.
Therefore, the standards also open greater scope for us as manufacturers in the integration of other systems and we can create the optimum for the customer.

We see time and again how important it is for manufacturers to work together on joint development when new requirements arise, as is the practice of the OSS Association. And not only that: in tenders, system integrators can offer partial components from different manufacturers, because these have become compatible with others thanks to the manufacturer-independent standards.

The advantage for the tendering party is the "perfect solution" that meets his requirements and which he can easily expand with standard-compliant components in the further course. This promotes the accep-

tance of access control and locking systems and thus promotes market growth for the entire industry.

Where is the journey heading in the next few years?
Mobile access, i.e. access control via mobile devices, will certainly be an important topic in the next few years. access control via mobile devices. This is demanded by the industry, but acceptance and distribution in Germany is not yet widespread. Here, too, we will see whether a standard can be the driver for mobile access.

Fraport

From the customer's point of view, the use of standards offers many advantages. We asked Patrick Senneka, who has been at Fraport AG since 2012 and is responsible for the use and further development of the ESA (electronic locking system) product, about his experiences.

What is the motivation for you to use standards?

The OSS-SO standardisation makes it possible to integrate software and hardware components from different suppliers into the overall solution. In this way we ensure investment protection and at the same time do without proprietary systems. In total, we use about 75,000 airport ID cards and about 7500 offline readers at Frankfurt Airport. We can realise large installations with the use of Standard Offline and, for example, fall back on alternative OSS components in case of delivery problems or special requirements. This is a great advantage for us. The use of standards enables a high level of interoperability of products and flexibility in implementation.

An airport has special requirements in terms of security. How is this ensured using standards?

Imagine if each of the employees at Fraport had their own key for the different access authorisations. The employee leaves, loses the key, changes position and thus also the access authorisations. What an effort to handle this with mechanical keys and still guarantee security! The electronic locking systems and thus also the protocol of Standard Offline make it possible to issue temporary keys / authorisations that can be changed in the central system with one click. This ensures both security and optimised use of resources.

Mobile Access, it is predicted, will play an increasingly important role in access control in the coming years. What is the situation with mobile access at the airport?

Round table

This is a topic that is currently interesting for us, but less relevant. The laws that apply to The laws that apply to security areas require the permanent wearing of a visual feature, which cannot be realised with mobile devices at the moment.

What is your wish for 2023?

A user meeting to discuss new developments and to exchange ideas with other users would be important for the further development of the Standards by OSS.

Uhlmann & Zacher

Another manufacturer, or OEM (Original Equipment Manufacturer), is the family-run company Uhlmann & Zacher. The company has produced a total of more than 1,000,000 electronic clamping units. We asked Hartmut Beckmann, authorised signatory and sales manager at Uhlmann & Zacher, about his experiences with the use of standards in Germany and worldwide.

Mr Beckmann, how do you assess the situation in Germany regarding the use of standards?

In Germany there are still some manufacturers who prefer to use their own proprietary systems. They see the use of standards as a loss of their market power. However, there are companies on both the manufacturer and user side that have discovered the advantages of standards for themselves. When many locking systems for many people must meet very high security standards, the standards open new possibilities. security standards for many people, the standards open new possibilities. It would also be desirable for the standards by OSS to be used across countries, i.e., in an international context. international context. Here, for example, we have some partners in France who use OSS-SO.

What is the advantage of Standards by OSS from your point of view?

Uhlmann & Zacher does not sell to end customers, that is the strategy of our company. Through OSS-SO we have the opportunity to gain new integration partners without these partners having to develop a proprietary solution.

How do you see the future of Mobile Standard?

Mobile devices are equipped with Bluetooth, for example. Here, a standard ensures the communication capability of different end devices. There are various manufacturers in the mobile sector, some of them new and growing, others established. In this sector, the standard ensures that the technology remains future-proof, even if a company disappears from the market again.

And what about Germany as a whole? What is the situation with mobile use, i.e. mobile access in Germany?

In Germany, the acceptance of mobile access control is - in contrast to other countries - still somewhat hesitant. in contrast to other countries - is still somewhat hesitant.

However, we are currently working on a project to establish our own mobile access platform. We are looking forward to the next steps and the further development.

Looking to the future, what would you like to see?

We would be happy if large companies - independent of competitive thinking - would cooperate and participate in the further development of the standards. From our point of view, distribution would be much easier if as many larger projects (and companies) as possible would rely on the Standard by OSS.

The interviews were conducted by Martina Müller, pr-ide GbR, on behalf of the OSS-Association. www.oss-association.com

©pixabay.com

Cybersecurity Trends 2023

by Todd Moore, VP Encryption Products bei Thales

As 2022 draws to a close, it's time to look ahead to what the industry can expect in 2023. From Thales' perspective, the following six trends can be observed.

Market outlook

1. Mass layoffs in the tech industry will trigger a major security breach

Mass layoffs at tech companies - many of which are virtual - will undoubtedly lead to major security breaches, whether from disgruntled employees or downsized IT teams not taking the right steps to remove access rights. One way or another, we will see a major security breach in 2023 due to poorly managed user accounts.

2. Data sovereignty in MultiCloud environments.

A year ago, sovereignty meant that data did not leave the boundaries of the organisation. Today, some companies understand sovereignty as the ability to control the location of their data. They periodically move the location of their data to another place to protect it from outside access.

This trend will continue and data transfer will become a top priority for global companies. To achieve this, companies need to ensure they have cloud-agnostic technologies in place so they can easily move a workload in the cloud to another location. DevOps approaches can also help by writing cloud-neutral code so that workloads can be launched anywhere.

3. The recession will accelerate enterprise consolidation strategies.

Enterprises will move away from standalone solutions and return to data consolidation. With the recession, huge increases in the cost of living and looming skills shortages, simplification and efficiency will be top priorities in 2023. Automation will play some part in simplification, but businesses need to work with the right partners to ensure assets and data are properly secured.

By combining robust encryption, policy-based access controls, centralised administration and enterprise-wide key management, organisations can consolidate while ensuring their valuable assets are protected and regulatory compliance is met.

4 Connected cars will be the next big target for hackers

The connected car market continues to grow and is becoming a bigger and bigger target for ransomware groups. Connected cars operate with millions of pieces of computer code that, if not properly secured, can be easily hacked. Installing malware in a vehicle's operating system could have serious consequences - whether disabling brakes on a busy road, locking users out until a ransom is paid, or stealing corporate data. Additional attention must also be paid to electric vehicles. Their pace of development could bring additional security risks. Security by design is critical and it is essential that car manufacturers build in robust cybersecurity standards from the outset.

5. The metaverse will open a new frontier for hackers and extortionists.

As the Metaverse and other virtual platforms become more popular, virtual services and resources are becoming more important - users are beginning to value these assets as much as physical ones.

Children in particular are early adopters of these platforms and often use their parents' bank details to buy virtual currencies, making them a vulnerable target and a potential gateway for attacks.

These platforms have very quickly entered the mainstream, so ownership of these virtual assets must be subject to strict control and should be met with the same level of security and control as other platforms.

6. The business of cybercrime: extortionate ransomware will increase

Attacks on critical infrastructure will continue to occur in 2023. The tactics of these threat actors will likely remain unchanged. The reality is that cybercriminals operate like a business. If they continue to be successful with their attacks, they will see no need to stop.

While the way cybercriminals gain access is not changing, the approach to ransomware is. Double and even triple ransomware attacks against critical infrastructure will spread rapidly as they offer attackers the prospect of larger ransom sums and multiple payment options. The revenue thus generated is then reinvested in their own infrastructure

Trends 2023

What are the predictions and trends for the IT services industry in 2023?

Expert opinion by Colin Blumenthal, vice president of IT services at Sharp Europe.

Today's organisation increasingly relies on IT services and the outsourcing of certain responsibilities to support and drive growth. The last twelve months have not been easy for companies of all sizes, and in particular for SMEs. External factors have put their finances under pressure, stretching their resources to the limit. Issues of efficiency, security and value creation have become paramount. In the digital age, and in order to make the most of limited resources and staff, we need to put even more emphasis on strategy and collaboration. In this context, we will try to anticipate what 2023 and the months and years to come hold for the IT services industry in terms of new trends.

1 **Migration to the Cloud:** The migration of SME activities, services and processes to the public cloud, a trend that we have seen growing in recent years, shows no signs of slowing down. According to a recent study[1], the use of the public cloud by European SMEs has increased by 5% between 2020 and 2021. Moreover, 41% of organisations in the EU rely on such services in some way, for example to host their email systems and store files electronically. This trend is expected to continue and grow steadily. Many of our customers have migrated to the Microsoft 365 public cloud - by far the most dominant player in the SME market today.

2 **Teleworking is on the rise:** The continued migration of workloads, processes and data to the cloud and to in-house infrastructures has allowed companies to offer a more hybrid environment to their employees.

This model will continue to be popular, as it offers more flexibility and control to employees - not only in the workplace, but also in the way. SMEs need first-class IT environments to support a new generation that is more adept with new

technologies, and more demanding than before. This will be critical to recruiting and retaining the best talent. By getting the right infrastructure in place, organisations create a real value proposition, especially for the younger generation entering the market.

3 **Security at all costs:** With the amount of information hosted in the public cloud reaching unprecedented levels, organisations need to think about data protection. This ranges from the most obvious software (against viruses, malware and the like) to the implementation of rigorous backup policies, as public cloud providers do not always do this themselves (this is the responsibility of companies).

Data security awareness and the need for ongoing support will therefore be a key trend in the coming year.

As costs come under increased scrutiny, companies will be looking to save money in all areas. And security is one of those areas where spending cuts could be considered. However, such a choice would be ill-advised, regardless of the organisation. All it takes is one serious data leak or hack to put a company out of business and into bankruptcy. Some statistics show that 60% of companies would go out of business within six months of a serious cyber attack.

As with the benefits of security, IT service providers need to do a better job of highlighting the value of their products to their customers. Only by adopting a more sophisticated approach can they fully demonstrate their importance. This is likely to be a major trend in the future.

4 **Data automation:** In 2023, data management, like the capabilities provided by Microsoft Power BI, is expected to be-

come even more important. This business intelligence platform provides business users with non-technical profiles with the tools to aggregate, analyse, visualise and share data. Until recently, this technology has been reserved for medium and large companies, but we are beginning to see smaller companies take full advantage of it. Whether working with IT service provider partners, or on their own, smaller organisations are now producing valuable information.

Process automation will also remain a strong trend in 2023. We are currently seeing a push towards process automation - not just to streamline laborious tasks, but to make workflows more efficient. Indeed, given the financial pressures facing organisations of all sizes, automation can help reduce ongoing costs.

5 **Voice over IP:** IP telephony is expected to be a big hit in 2023. This is because the Integrated Services Digital Network (ISDN) and the Public Switched Telephone Network (PTSN) no longer meet the needs of users in an increasingly digital world. As a result, ISDN will be decommissioned in 2025, allowing IT service providers to offer unified and IP-based communication solutions to their customers.

Organisations that put off thinking about their migration to IP telephony may well find themselves short of not only the resources but also the skilled personnel to carry out the task. We are already well into discussions with many organisations seeking to make such a transition. However, for many others, there is still a lot of work to be done in terms of raising awareness of the benefits and the need to proceed with such a migration as quickly as possible.

Tech-Trends 2023

7 Trends for the New Year

Security: Cloud Native Application Protection Platform (CNAPP) and quantum cryptography on the rise - Network: Full-Stack Observability (FSO) and Internet of Things (IoT) boost business efficiency and resilience - Sustainability & Artificial Intelligence with tangible impact

In 2023, the economic climate will continue to be characterised by the need to reduce costs and increase efficiency. The future view of many companies is therefore directed towards innovative technologies that can help here. Liz Centoni, Chief Strategy Officer and GM of Applications at Cisco, therefore outlines the seven technology trends for 2023 from the areas of security, increasing efficiency in the network, sustainability and AI. According to Gartner, 60% of companies worldwide will define zero trust as the basis of their security architecture by 2025 - and 80% of companies worldwide will implement a strategy that allows web applications, cloud services and private apps to run on a uniform platform. AI and sustainability will also become increasingly important.

IT Security

1) Application and API security

As modern cloud-native environments become more of a business driver, protecting them is critical. In 2023, developers will be given more tools to manage and secure distributed application architectures.

There will also be a further evolution towards tools that allow developers, SREs and security experts to work together seamlessly. The whole thing will then bear the sonorous acronym CNAPP - Cloud Native Application Protection Platform.

2) Advance of quantum cryptography

The transmission of key data poses a fundamental security risk. Quantum Key Distribution (QKD) technology will prove particularly effective as it avoids distributing keys over an insecure channel.

In 2023, a new macro trend is on the horizon with the introduction of QKD in data centres, IoT, autonomous systems and 6G.

Efficiency

3) Increase business efficiency with full-stack observability (FSO).

Too much data with too little context - this is the challenge many companies are currently facing with their monitoring. Many of the collected data volumes do not bring any real added value to the company's management.

This is about to change. The full-stack observability approach optimises business processes and will become increasingly prevalent in 2023.

4) Internet of Things (IoT) makes supply chains more resilient

Businesses and logistics service providers will increasingly use the Internet of Things to bring complete visibility to their supply chains in 2023. IoT and other technologies will not only play a greater role in improving the resilience, efficiency and sustainability of supply chains, but also improve cybersecurity and IT/OT network management. Enterprises and logistics providers will reconfigure their supply chains based on predictive and prescriptive models, including smart contracts and distributed ledgers.

5) Optimisation of multi-cloud resources.

2023 is the year when companies will face cloud management challenges. They will be optimising their cloud resources in large numbers - including to address or prevent major performance issues with their multi-cloud infrastructure. Machine learning and deep analytics will be increasingly used. We will also see innovations that create a more inclusive and sustainable future for all.

Sustainability & AI

6) Sustainable data centres

Net Zero remains the 2023 action target to move data centres towards a more sustainable future. Major advances in Power over Ethernet (PoE) are contributing to this. Networks and APIs are evolving in the management of data centre platforms to monitor, track and change energy consumption. IT vendors and equipment partners will be transparent in reusing hardware (circular economy).

7) Responsible AI

In 2023, individuals and organisations will continue to use artificial intelligence to achieve unethical and socially destructive goals. Industry, governments, academia and NGOs will therefore work together to develop a framework for the ethical and responsible use of AI to limit the potential harm. This framework will be based on principles such as transparency, fairness, accountability, privacy, security and reliability, and will set the first landmarks on the road to "Responsible AI".

Author: Liz Centoni, CSO / GM of Applications bei Cisco

How digitalization and sustainability will shape the construction industry of the future.

Seven Trends

that will transform the construction industry.

More sustainable and digital: The construction and real estate industry is on the verge of substantial changes. But what will the future of construction and building operations look like? Siemens Smart Infrastructure has identified seven trends that show where the journey is headed.

1 Digital building design with BIM fit for the future

Digital design using Building Information Modeling (BIM) gives building owners much more control over their project.

Many modern buildings are already being built twice – first on the computer, and then in the physical world. The magic word that has pushed open the door to the future of building design is Building Information Modeling (BIM), a type of computer-aided design (CAD) for buildings.
Digital design using BIM gives building owners much more control over their project. Thanks to BIM, they can do a virtual walk-through of their building during the design stage. This is made possible by a detailed virtual model of the building, a digital twin, based on the BIM data.

The virtual model allows building owners to assess implementation variants in 3D and provide feedback. They can also take financial factors into account because the costs of each design measure are stored in the digital twin. As a result, it is easy to see how a particular change will affect the price.

Based on feedback from the owner and other stakeholders, the designers make adjustments to the project, which can then be reviewed again. These iteration cycles are short and cost-efficient because algorithms take a lot of the work out of the hands of the designers. If, for example, the room size is reduced when designing a hospital, an algorithm automatically adjusts the walls in the virtual model based on predefined criteria. The same applies to other details, such as the number and position of fire detectors. This makes planning more reliable and efficient. The digital twin allows for transparent design across disciplines. This helps avoid errors, optimally coordinate disciplines, and provide up-to-date cost information at all times. This trend will become more pronounced, making building design not only more transparent, but also more efficient and cost-effective.

2 Collaboration in the digital twin

Establishing transparency: In a digital building twin, data from all stakeholders involved in construction are shared.

For digital design to deliver on its benefits, the stakeholders involved in construction must share their data. Only then can transparency be established across the entire design and construction process.

In modern software development these processes are modeled on platforms such as Github or Gitlab which allow multiple programmers to collaborate on a project. The software manages all inputs, and all changes are visible to everyone.
However, the construction industry is not there yet. Many stakeholders still work with disconnected two-dimensional plans or move the BIM data to other systems, leading to major adjustment losses. The desired transparency over the entire design process is currently still a pipe dream.
In addition, it remains to be seen how this new approach can be used to offset expenses if stakeholders design their disciplines in collaboration with others. New approaches are needed. For example, the building owner who benefits from the digital twin during operational optimization could compensate the designers who created it for this added value.

3 Digital project management as a basis

When the digital building twin is in place, the next question is in which steps the physical building will be constructed. Today, the project planners determine the sequence. It is based on experience, is usually imprecise, and is difficult to adjust if delays occur in a substep.

Digitalization promises dramatic improvements for project management. For example, the U.S. company Alice Technologies is working on completely automating this process. The computer learns the ideal sequence of project steps and uses BIM data to create project plans on its own. They can be updated instantaneously if delays occur somewhere. This ensures that the best possible sequence is selected. According to the company, this solution can already save an average of 11 percent of costs and 17 percent of time during construction.

In the future, computer-aided project management is likely to become even more refined. This, in turn, could change the way contracts are awarded for construction projects: In this way, even small project steps, like installing room devices such as thermostats, could be put out to tender via an app as work packages at a predefined price – similar to the way Uber offers trips to its drivers. This would also give small local installers an opportunity to participate in construction projects. In addition, quality assurance could be performed through reviews and feedback in such an app.

4 Building while conserving resources

The construction of buildings is resource-intensive and anything but climate-friendly: Each year, approximately 4.4 billion tons of cement are produced, releasing roughly as much CO2 as 700 coal-fired power stations.

In order to reduce the environmental footprint of buildings and infrastructures, it is crucial to use building materials sustainably. First, more building materials need to be recycled. To some extent, this is already being done today. For example, an existing concrete shell is no longer demolished and rebuilt, but incorporated into the design of the new building or reused as fill material. Secondly, more climate-friendly alternative building materials such as wood should be used more widely.

New technologies can also make construction more resource-efficient. For example, 3D printing promises not only more efficient processes, but also a massive reduction in the environmental footprint, because additive manufacturing can be used to print new shapes that use less construction material without compromising stability.

5 Robots on the construction site

Another trend that can already be seen today is the use of robots: Drilling robots from Schindler or Hilti, for example, are already in use, independently drilling holes in concrete according to data specifications.

In addition, robots are already being used to manufacture complex structures from alternative building materials. Increased cost pressure will lead to more industrial construction. Using new digital manufacturing methods, components will be produced individually and on demand. Since more elements will be integrated into prefabricated products – electrical components, for example – the construction site of the future will increasingly focus on assembling prefabricated elements.

6 Data-based building operation

Heating, cooling, and domestic hot water require the most energy during the building's operational phase. A smart building of the future will have sensors and intelligent controls to make the operation of building equipment as efficient as possible. It will also take the behavior and needs of the building occupants into account:

There is, for instance, no need for heating in unoccupied spaces. The smart building incorporates weather forecasts and the availability of renewable energy – for example from the PV system on the roof – into its behavior.

The data collected in the smart building can be analyzed by algorithms to optimize building management: When deviations occur, facility management is informed so that they can decide what to do. The data will be available in a standardized form, and there will be applications that process the data and offer added value, such as energy savings. These applications can be available in a virtual marketplace, and customers will be able to select those that best serve their purposes.

7 Electric vehicles as power storage

Charge and discharge: In the future, electric cars can serve as energy storage units, optimizing the use of renewable energy.

In smart buildings, energy storage will have a larger role than it does today. Electric vehicles will play an important part: During the day, when they are parked at work, they receive for instance solar power and are charged. The stored power can then be used at home in the evening. Smart systems ensure that the battery still has enough of a charge to drive back to work the next day. If the calendar shows a meeting further away, the discharge of power from the vehicle's batteries will be stopped earlier so that the destination can be reached easily.

Connecting consumer and power generation data makes it possible to optimize the use of renewable energy

and will play an important role in ensuring a sustainable energy supply. This type of energy optimization will result in new business models. For example, excess power could be sold to a neighbor. However, such solutions currently face high bureaucratic and political hurdles.

Looking ahead

Although technologies and materials for a more sustainable and intelligent construction and real estate industry already exist, the road into the future of construction is rife with obstacles.

Today, many companies see no incentive to actively drive change. Regulatory requirements and historically evolved structures partially impede progress. And as long as the cost pressure is not high enough, the automation of the construction industry will not move forward. In the long run, however, this will not be a viable approach. Progress and digitalization will prevail, as examples from the printing, photography and music industry have clearly shown.

The good news: There are many ways to modernize the construction industry. Software developers, startups and advanced technologies can and will revolutionize many things – this is just the beginning.

The author:
By Michael Kiy, Director Innovation Management, Siemens Smart Infrastructure. Michael Kiy studied physics and completed his doctorate at ETH Zurich. He then worked as a Senior Engineer at the Centre Suisse d'Electronique et de Microtechnique (CSEM), as a Project Manager at Alcan Packaging, Associate Director of Engineering at Vistaprint / Cimpress and as Director of Engineering at Heptagon OY / AMS AG. Since 2018, he has been Director of Innovation at Siemens Smart Infrastructure. Since 2019, Michael Kiy has also been a member of the Expert Board of Electrosuisse and a member of the organising committee of the Swiss Building Technology Congress and the Smart Home Forum.

2023 with new cyber threats and challenges

Seven security experts have explained for us what companies will have to prepare for in terms of IT security in the coming year.

For example, the use of Wiperware malware could increasingly take place across countries next year, while hybrid human-machine attacks will automatically identify vulnerabilities that are then evaluated by a human expert. Ransomware-as-a-service on the darknet will also increase, for example to specifically sabotage competitors or politically exploit cyberattacks. Next year, mobile edge computing via 5G will also go live for the first time, which will require the use of modern security concepts such as ZTNA (zero-trust network access concept).

Fleming Shi, CTO, Barracuda Networks

"Wiperware will increasingly take place across countries and ransomware gangs will become smaller and more skilled."

"Russia's attack on Ukraine has once again made it clear to us that modern digital warfare is also taking place on our own doorstep, so to speak. The increased use of so-called Wiperware was particularly striking. A wiper is destructive malware that targets files, backups or the boot sectors of the operating system. We saw attacks against Ukrainian organisations and critical infrastructure.

The frequency has increased dramatically, as shown by WhisperGate, Caddy Wiper or HermeticWiper, which have made headlines since the outbreak of the war. In contrast to the monetary motives and decryption potential of ransomware, Wiperware is usually used by nation-state attackers with the aim of damaging and destroying an adversary's systems to such an extent that recovery is impossible. Moreover, Wiperware originating in Russia is likely to spread to other countries in the future, as geopolitical tensions are by no means abating, as is hacktivism by non-state attackers looking for further measures to exploit their victims. To ensure business continuity despite an attack, companies need to focus on whole-system recovery so that not only the data, but the entire IT infrastructure is functional again. For example, quickly restoring the virtual version of an attacked physical system can greatly improve a company's resilience against Wiperware or other destructive malware attacks.

In 2022, the major ransomware gangs - LockBit, Conti and Lapus$ - were behind attention-seeking attacks that regularly put them in the headlines. In 2023, with the booming Ransomware-as-a-Service business model and the recent build leak of LockBit 3.0, a new generation of smaller and smarter gangs will steal their thunder. And businesses will face ransomware attacks with new tactics more often. Those who are not prepared for this will find themselves in the headlines and risk damaging business and reputation."

Jörg von der Heydt, Regional Director DACH, Bitdefender.

"Hybrid man-machine attacks are targeting businesses of all sizes."

"The race between hackers and IT security teams continues in 2023. New tools and faster hardware with often growing government-backed budgets put attackers in an ever-stronger position. A continuously increasing number of vulnerabilities and the lack of resources or insufficient tools to patch them in a timely manner support this trend.

A particular danger is the timely availability of quantum computing, which will disruptively change encryption and password security. A rethink is already necessary.
Hybrid man-machine attacks are equally important: Automated tools identify vulnerabilities in the infrastructure to be attacked - experts then evaluate these in terms of attack potential. Cyber defence should also proceed in this way. However, they often lack budget, time, skills, and competent personnel.
If companies - regardless of size and sector - do not want to fall victim to such an intelligent attack, they must also rely on hybrid defence. "Fight Fire with Fire" also applies here: Companies must either form (or train) teams themselves - or supplement them with external Managed Detection and Response (MDR). It is important to understand the potential damage. Many recent conversations show that this awareness is often lacking, and IT security is too often still seen merely as a cost factor with invisible benefits."

Lothar Hänsler, COO, Radar Cyber Security

"Threat situation remains tense in 2023, KRITIS operators still challenged."

"As long as Russia is at war, the threat situation must be taken particularly seriously. KRITIS operators, for example in the energy and financial sectors, are particularly challenged here. In the public administration, DDoS attacks are likely to increase in the future (such as the recent attack against the website access of the EU Parliament).

One of the greatest threats to companies and public authorities continues to be the constantly changing threat situation around ransomware and emails containing dangerous malware, or even the combination of both forms. Newer types of ransomware do not necessarily focus on data encryption at all, but on exfiltration. The attackers then exert pressure by threatening to release the data. They use increasingly sophisticated methods to get email attachments opened or specific websites visited. In the worst case, they manage to intercept credentials and login information, which are used for further compromise.

Email security therefore remains one of the central topics for companies and authorities. To cover the essential "open flanks", a three-part package of measures is needed:
technology (reputation check of websites, sandboxing, malware protection, continuous monitoring, analysis of events), **personnel** (sensitisation measures, training) and **processes** (regular prompt remediation of vulnerabilities, emergency plans and exercises). Therefore, we need to consistently make systems more cyber-resilient. Zero-trust networks must be considered as well as securing remote access. The use of endpoint detection and response (EDR) is urgently recommended - and OT security must not be forgotten either. The holistic and consolidated security view is be-

coming increasingly important in the context of risk management."

Robert Rudolph, Product Marketing Consultant, ForeNova

"Heterogeneous attacks dictate behaviour-based and proactive defences."

"The year 2023 will continue to transform the world of cyber threats. Trends that have been visible recently will continue to intensify. Small and medium-sized enterprises, such as the manufacturing sector, will be in the spotlight. On the one hand, because of their valuable sensitive know-how and potentially sufficient capital to service high ransom demands, on the other hand, because of too traditional IT security consisting of firewalls and AV. The current crisis situations are reflected in targeted attacks on allies in conflicts and their critical infrastructure. At the same time, cyber criminals are becoming more professional. Ransomware-as-a-service on the darknet is leading to more covetousness among those who want to sabotage the competition or exploit cyberattacks politically.

Attackers are becoming more and more targeted. They screen victims extensively in advance and unerringly exploit gaps they have identified. They all too often find a way into corporate networks via security gaps and social engineering. Especially since almost all corporate communication, for example between people, devices, and switches, now takes place in the network. An increasing number of "clients" - such as IoT devices in the healthcare sector - are then a target for cyberattacks. IT managers must therefore supplement classic signature-based defence approaches with security technologies that effectively detect anomalous activities in the network and on endpoints. In addition to behavioural analysis, the next trend is proactive protection: functions such as ransomware honeypots can specifically trigger and actively combat attackers' actions before the cybercriminal carries out his master plan. Those who want to defend against this should seek the help of external cybersecurity experts."

Ari Albertini, Co-CEO, FTAPI

"Linking sustainability with the opportunities of digitalisation."

"The digitisation and automation of processes, as well as the move from on-premise systems to a secure, European cloud, will be as much on the minds of companies, public authorities and organisations in 2023 as the topic of sustainability.

These three topics are closely interlinked: Ideally, a digital, automated process is paperless and - if implemented correctly - leads to significant time savings for employees. However, the issue of sustainability is about more

than just going paperless. Companies must learn to make better and more efficient use of the resources at their disposal. Automated existing processes free up valuable time for employees to use creatively, for example, to tackle future-proof strategies or implement innovative ways of working.

Companies will also centralise their competences more, but at the same time increasingly refrain from operating data centres in their own companies. Most managers now know full well that it is more effective to store data in a secure, European cloud.

Sustainability is more than a trend - it has become a fundamental issue for society. Linking it with the opportunities of digitalisation will be one of the key challenges next year."

Arne Jacobsen, Director of Sales EMEA, Aqua Security

"Securing software high on CISOs' priority list in 2023."

"There are more and more attacks on the software supply chain, increasing by 300 per cent from 2020 to 2021 alone. In the meantime, the intensified threat situation is also preoccupying politicians: the White House recently published a corresponding 'executive order', and in a current directive of the EU Parliament, securing the supply chain is even one of the four central requirements.

In my opinion, these efforts are a big step in the right direction to make software more secure. Even if there is still a transitional phase until the directive is ratified in all EU countries, as was the case with the GDPR, one should already prepare oneself now. Securing software will therefore be at the top of the CISOs' priority list in 2023. Specifically, they will have to invest above all in solutions for analysing the composition of software, securing the tool chain and in "Software Bills of Materials" (SBOM for short). During this, the spread of DevSecOps - after years of discussion - will also increase strongly.
As of now, SBOM will be at the centre of industry-wide efforts - accelerated by the policy directives. This means that companies that use software - which is true for almost everyone these days - should now make sure that their software suppliers implement the guidelines, use tools to secure their entire development process and can guarantee the origin and security of all software components via a complete SBOM. Software vendors, on the other hand, must now invest in solutions that secure the entire process in order to detect and fix errors in their solutions as early as possible."

Jan Willeke, Area Director Central Europe Cradlepoint

"Mobile edge computing over 5G networks goes live in 2023 and requires modern security concepts like ZTNA."

"5G networks - whether private, public or hybrid - in combination with mobile edge computing: this will be one of the market-defining topics in 2023. In the past two or three years, technology companies, edge device manufacturers, application providers, research institutes as well as end customers have invested a lot of resources in the development of application scenarios and functioning eco systems. Now we are reaching the point where these developments go into productive implementation and create added value.

Secure access from the network edge to applications and other resources plays an important role in productive operation. The Zero Trust Network Access concept, or ZTNA for short, provides an intelligent, easy-to-use, and reliable approach. Companies can use it to reduce the risk of so-called lateral movements of malware in the network because users are directly connected to applications instead of the network.

Zero Trust Network Access is fast becoming a standard in networking that wireless WANs need to adhere to as well."

Bildnachweis:Checkpoint Systems GmbH

EAS in the retail sector

Why theft prevention is the best strategy for retailers. Why electronic article surveillance is becoming increasingly important and timely. And how to implement an EAS system most economically.

According to the EHI Retail Institute, the entire German retail sector lost about 4.1 billion euros due to inventory discrepancies in 2021. The share of losses due to theft from customers, employees, suppliers, and service staff was around 79 percent, which corresponds to approximately 3.23 billion euros. This figure alone is sufficient reason to act, but what makes the situation even more urgent is the large number of unreported cases: less than two percent of thefts are reported. In purely mathematical terms, it can therefore be assumed that more than 19.8 million shopliftings with a value of 106 euros each go undetected every year.

Prevention is better than reaction

What can be deduced from these figures? One possible insight from this could be that it is above all important for retailers to take preventive measures and rely less on law enforcement and crime detection. But watch out: One measure that used to be extremely popular and is still frequently used today should be reconsidered - locking away or putting away expensive goods and goods with a high risk of theft. "When customers cannot see and experience merchandise, impulse buying is precluded, and many cross-selling opportunities are lost.

Calculating this lost revenue is difficult, but we have been able to determine that in the opposite case - i.e., when goods are openly displayed - sales increase," explains Hans-Jürgen Nausch of Checkpoint Systems, a vertically integrated provider of RF/RFID solutions for retailers. "Moreover, brick-and-mortar retail thus forfeits one of its greatest advantages over online retail - the haptic experience." In other words, the ideal theft prevention solution must not only prevent theft, but also encourage an open display of merchandise - otherwise retailers are effectively hurting themselves.

The secure 3

With regard to these item security requirements, three solutions in particular have proven their worth: EAS, camera surveillance and security staff.

Security staff has some advantages, including a very high deterrent effect, but also some weak points. For one, there is the cost factor. According to the Global Retail Theft Barometer studies, security guards account for the largest share of many retailers' loss prevention budgets worldwide. For another, the quality of surveillance is difficult to verify, because while in the past many companies had security guards on their own payroll, this is becoming increasingly rare. And with contract surveillance, it is difficult to guarantee the standard of security guards and measure their effectiveness.

While CCTV can also be considered a preventive measure if the cameras are placed very conspicuously and thus have a deterrent effect, its main contribution is to visually clarify afterwards what happened, how and when. It also provides retailers with clues to the identity of those involved. So, it is primarily more of an after-the-fact law enforcement measure.

The third solution is EAS - Electronic Article Surveillance. The basic principle of EAS has not changed too much since the 1960s. It is based on the premise that goods are tagged with an electronic label that communicates with an antenna in the shop, usually located near the entrance/exit of a shop. When the tag comes within range of the antenna, an alarm sounds, alerting staff and management that an item is leaving the shop illegally. Retailers basically have a choice with EAS between discreet hidden tagging, where the RF label is inside the packaging, and overt tagging, where a clearly visible label, sometimes even with the RF circuit itself, and a security message are placed on the label. "In terms of theft prevention, you should definitely go for the visible labelling," explains Hans-Jürgen Nausch from Checkpoint Systems. "Thus, EAS labels not only increase the effort and risk of being caught for more professional thieves, but also effectively deter casual thieves. This has also been proven by research."

EAS - contemporary article surveillance

EAS has been available in various technology formats for over 40 years. However, acoustic-magnetic (AM) and radio frequency (RF) technology have prevailed. These technologies differ in one key respect: the frequency at which they operate, measured in hertz. While AM was originally the preferred frequency for EAS, there has been a recent trend towards RF - and there are several reasons for this: "Among other things, RF systems are more energy-efficient in operation than AM systems, which is of course particularly attractive in times of energy scarcity and rising energy costs. Their total

energy consumption is about 70 per cent lower per shop, and in addition, consumption can be reduced even further by coupling them with intelligent power switching software," elaborates Hans-Jürgen Nausch of Checkpoint Systems. "RF systems are also ahead of the game when it comes to complying with some of the directives that apply in Germany. For example, when using EAS systems, retailers are required to carry out a risk assessment regarding exposure to electromagnetic fields (EMF exposure). Our RF-based systems of the EVOLVE and NEO series fulfil all the requirements applicable in Germany in this respect. This has also been confirmed to us by the BGHW, the professional association for trade and goods logistics. "Even though the general mode of operation of the EAS has not changed since its beginnings, there have been numerous advances since the introduction of digital, software-controlled solutions - especially in the RF area. Improvements in CPU capacity have taken the technical operating capabilities of RF systems to a much higher level. For example, the latest technology uses secure wireless communication instead of hardwired cabling. Wider coverage areas allow for wider aisles of up to 2.70 metres between antennas. Software filtering reduces false alarms and allows for better alarm integrity than ever before, and remote connectivity reduces system downtime in the event of an emergency.

"But the improvements in modern EAS systems are not just about performance, they are also about improving the customer experience. There is a wide range of design options and additional features, which means that no retailer today must choose between merchandise security and shop appearance. The classic "gate look" is passé," reports Hans-Jürgen Nausch of Checkpoint Systems. "The restrictions on the product side that earlier systems had also no longer exist. EAS labels are now available for all product types, including food-safe and microwaveable labels that can even be applied to metal containers such as cans."

Another plus point that EAS systems,

and especially RF-based EAS systems, bring: They support customer self-checkout, because deactivation of an RF label can be done both when the cashier is scanning the barcode and by the customer himself at a self-checkout device (SCO). This capability allows RF-based EAS systems to be integrated into any self-service application and can be further enhanced by the option to deactivate labelled products only after payment has been completed.

Two steps to EAS deployment

Ideally, a retailer looking to deploy an EAS solution would equip every single item in its shops with security labels. However, the reality is often different: Applying security labels on a day-to-day basis in shops is no easy feat, as most retailers are short on available staff. There are often simply not enough employees to devote to the comprehensive label fitting and at the same time to the actual tasks such as sales and customer advice within regular working hours. And the allocation of additional working hours for the application of security labels generates significant costs. "To make the introduction of EAS as profitable as possible, we recommend two points to retailers, which are best combined. First, item protection should initially focus only on, say, the 20 most frequently stolen items. Firstly, this reduces the implementation effort and secondly, these goods account for a disproportionately large share of the total loss. If you concentrate on them, you can reduce losses in a shorter time than if you try to protect entire groups or ranges of goods across the board. It is not uncommon that losses on these high-risk items could be reduced by up to 50 percent in the process," explains Hans-Jürgen Nausch of Checkpoint Systems. "Secondly, retailers should first test their chosen EAS programme in a pilot project before rolling it out on a large scale. This allows you to predict and prove the return on investment (ROI), even if each shop has a slightly different ROI, before a large investment has been made. It also shows whether the retailer has really chosen the right EAS solution for them, and the team also learns to use the solution effectively and efficiently before going 'nationwide' on a permanent basis." In simple summary, for such a pilot project, the right shops need to be chosen - as representative as possible of the overall risk profile - the appropriate products need to be included - preferably the high-risk items at the beginning, which are easy to label - and the right time needs to be set - between three and six months. And not to forget: The respective branch team must be on board to make the pilot project successful.

Source tagging as a solution

A special solution for EAS in retail is source tagging, a kind of cooperation between retailers and manufacturers. This involves labelling products at the source before they enter the shop. This solution is becoming more and more popular because it offers several advantages. The shop staff no longer must label the products themselves and can concentrate on the core business. Labels can be systematically applied to each item in the same place - where they do not obscure information or diminish brand impact. And item protection is more comprehensive: source tagging means that products are protected from the source to the shop, not just at the point of sale. When source tagging is done with RFID, it can enable product tracking throughout the supply chain, reducing the number of lost items, streamlining processes, and enabling better availability on the shelf at the end of the chain. It also makes it more difficult for products to be diverted into the so-called grey market, which is responsible for large economic losses, and for counterfeits to spread.

Summary

EAS solutions, especially RF-based ones, are an effective measure for theft prevention and at the same time an opportunity to present goods openly and promote sales. They continue to evolve with technological advances, allowing retailers to keep pace and integrate security measures more and more easily into everyday operations. But they are not the only viable way. "In our experience, a complete solution for theft prevention should always include all three methods - EAS, camera surveillance and security staff," advises Hans-Jürgen Nausch of Checkpoint Systems. "When these three protection methods are used in parallel, they can offer retailers significant benefits in total. But even the best combination will not deter all criminals. The goal is to establish a level of protection that deters most thieves and lowers theft rates - tailored to the individual risk profile of the shop or location in question."

EUROSHOP 2023

Are autonomous stores the future of retail?

Checkout-free stores Ringing in the changes

The digitalisation of the retail industry, which has been advancing at a rapid pace in recent years, has also led to equipping physical stores with more and more technological intelligence. Versatile automated store concepts have emerged where the shopping process is largely digitalised. That is why the topic of smart stores is one of the hot topics at EuroShop 2023, The No.1 Retail Trade Fair, from 26 February to 2 March in Düsseldorf.

It's nearly 40 years ago that inventor David R Humble came up with the idea of the self-service checkout machine after allegedly standing in a long queue at a grocery store in South Florida. Since then, the technology has evolved massively and is appearing in more and more retail stores. In fact, the global market grew by 11 per cent last year, according to strategic research and consulting firm RBR's report, Global EPOS and Self-Checkout 2022, with 200,000 self-service units shipped globally in 2021. The technology promises huge benefits, such as shorter wait times for customers and improved store efficiency for retailers but, as with most things, it's not without its flaws. Now, with the likes of Amazon rolling out fully automated stores, where customers can skip the checkout process altogether, is retail moving towards a more frictionless future?

"The old 20th century days of scanning every single item, one at a time, slowly, over a barcode scanner, is on the way out," declared Will Glaser, CEO of US-based Grabandgo. "The shopper is in the position to choose the store that they prefer based on both price and convenience."

In 2018 online retail giant Amazon

ALDI SHOP&GO
Welcome to
Aldi SHOP&GO
Greenwich
Opening Times
Monday – Saturday
7am – 11pm
Sunday
11am – 5pm
Bank Holidays
8am – 8pm
TEAM GB
ALDI
Everyday Amazing.
RED WINE
CRAFT ALES
BEER
GREETINGS CARDS
App
Download our SHOP&GO App to enter.
Once registered, scan your SHOP&GO QR code at the gates.
Shop
Just pick up an item or bag it.
If you change your mind, just put it back. You won't be charged.
& Go
No tills or queues, that's it.
You'll be charged and receive your receipt via your App.

made headlines when it opened its first cashierless store in its hometown of Seattle, featuring the company's 'Just Walk Out' technology. Today, there are more than 40 Amazon Go and Amazon Fresh locations across the US and the UK, with more expected to open around the world.

The so-called Just Walk Out shopping experience uses the same types of technologies found in self-driving cars, including computer vision, deep learning algorithms and sensor fusion, enabling customers to enter the store, grab what they want and leave.

While Amazon currently has the largest number of checkout-free stores globally (according to RBR), other supermarket chains, including Tesco, ALDI and REWE, are experimenting with technology to remove friction from the in-store shopping experience. By the end of 2027, RBR predicts there could be more than 12,000 stores with checkout-free technology operating around the world.

"Physical retail is undergoing unprecedented change, with retailers investing heavily in technologies to transform their stores, making customer journeys smoother, and helping to offset rising labour costs and shortages in several markets," says Alex Maple, who led RBR's study, Mobile Self-Scanning and Check-Out Free 2022.

"In general, retailers are always looking to improve the customer experience as well as to reduce costs," continues Maple. "The increasing deployment of self-checkout terminals, for example, illustrates that retailers are happy to use technology if it means they can reduce staffing costs and increase points of sale, offering the customer new, convenient ways of completing the checkout process. With checkout-free technology, successful implementation would differentiate such stores from the competition, lower staffing costs (potentially significantly), reduce shrinkage (which is a potential issue with self-checkout/mobile self-scanning) and provide a 'frictionless ex-

perience' to the customer. "Convenience is one of the main reasons the technology works well in small-format stores in busy locations," claims Maple. "The pandemic also made checkout-free technology more appealing to some as it minimises human contact and could be considered a more hygienic way to shop."

A year ago (October 2021), the UK's largest supermarket chain, Tesco, opened its first checkout-free store in central London, following a trial at the company's headquarters in Welwyn Garden City. Tesco partnered with Israeli computer vision start-up Trigo to install EasyOut technology at its 'GetGo' store in High Holborn so that customers with the Tesco.com app can check-in to the store, pick up the groceries they need, and walk straight out without visiting a checkout. The combination of cameras and weight-sensors establish what customers have picked up and then charge them directly through the mobile app when they leave the store.

More recently, Trigo worked with German supermarket chain REWE Group to open its second hybrid autonomous grocery store, in Berlin. It has also collaborated with ALDI Nord on an AI-powered cashierless discount store in Utrecht, The Netherlands. "Trigo's solution has a two-sided value proposition," explains Shay Ziv, VP Marketing at the company. "For shoppers, we help save time and enhance the user experience by removing checkout lines to create a seamless shopping experience. For retailers, we are modernising the way they operate by saving costs on store operations and driving efficiency. Our solution also has a direct impact on their bottom line as it reduces shrinkage and helps grow the average shopper basket size."

Earlier this year, ALDI also opened a checkout-free store in the UK, using an AI-powered solution from technology provider AiFi. Like the other stores, ALDI Shop&Go allows customers to complete their shop without scanning a single product or having to go through a checkout. The store even uses facial age estimation technology from Yoti to authorise the purchase of alcohol (store colleagues are on hand to verify age for customers who opt to not use the system). Meanwhile, in the US, bookseller and stationery retailer WH Smith has opened its first checkout-free store at LaGuardia Airport, New York, using Amazon's Just Walk Out technology. According to Rebecca Hobbs of trends intelligence agency, Stylus, there are several driving forces spearheading the growth in autonomous stores, other than the sheer speed and convenience usually seen as the key benefits. "The most consumer-facing one is that brands are able to unify online and offline consumer

data more easily," she says. "They can establish a system whereby consumers have to 'sign in' to a customer account to enter a shop, thus giving every in-store customer the same profile as online customers have, allowing brands in-store data and data on a customer from across both online and in store. This helps them to establish spending patterns and make stock and merchandising decisions.

"These stores can even tell what a consumer picks up and then discards," adds Hobbs. "If many customers pick up an item, discard it, then choose to buy that product online, that would validate the choice to have it in-store as a route to discovery. This level of connectivity will power the rise of omnichannel retail – a word that's been thrown about for years but will come into its own with this kind of technology."

Inevitably, with this new technology comes much uncertainty, particularly around data privacy and the loss of human interaction. "[Checkout-free] technology is perfect for a very specific type of shopping mission, where the consumer knows what they want and doesn't want anything to stand in their way]," claims Ian Johnston, founder of retail design agency Quinine. "[However], I worry that this technology leaves part of our society behind. I do wonder if this kind of shopping experience alienates those who can only pay in cash."In addition to economic exclusion, Johnston believes that these formats also need to address the needs of a broader range of consumers and shopping missions, including addressing consumers' accessibility and inclusivity needs. "At present, these formats appear to be tied to retailers' belief that consumers want frictionless experiences," he says. "I worry that retail brands and businesses focusing solely on delivering this type of frictionless shopper mission for customers forget to consider that many shoppers want or need sticky experiences that involve high levels of human and social interactions that add value and build extreme levels of trust and loyalty."Moreover, there will be people (either based on demographic or attitudinal outlook) that simply don't want to have to 'sign in' digitally to every store they enter, argues Hobbs. "I don't foresee a near future (within five years) where every store will be automated," concludes Hobbs, "but as this tech gets cheaper, as consumers become more attuned to it and as the use of cash continues to decline, it will certainly accelerate."

The state of the art and innovations around Smart Stores and Autonomous Stores can be found at EuroShop in the Retail Technology dimension in Halls 4, 5, 6 and 7a. EuroShop 2023 is open to trade visitors from Sunday 26 February to Thursday 2 March 2023, daily from 10.00 to 18.00. **[www.euroshop-tradefair.com]**

10 contributions for a safer Internet of Things

How manufacturers and users can limit the risks of connectivity

Technical article by Jörg von der Heydt, Regional Director DACH at Bitdefender

The connectivity of local IT to the internet is becoming denser. Smart hardware and sensors are increasingly becoming part of corporate networks, making the attack surface more confusing and thus more prone to error. Manufacturers and users are first in line to ensure security. IT administrators must not lose control of the new connections to the Internet of Things or must first gain it.

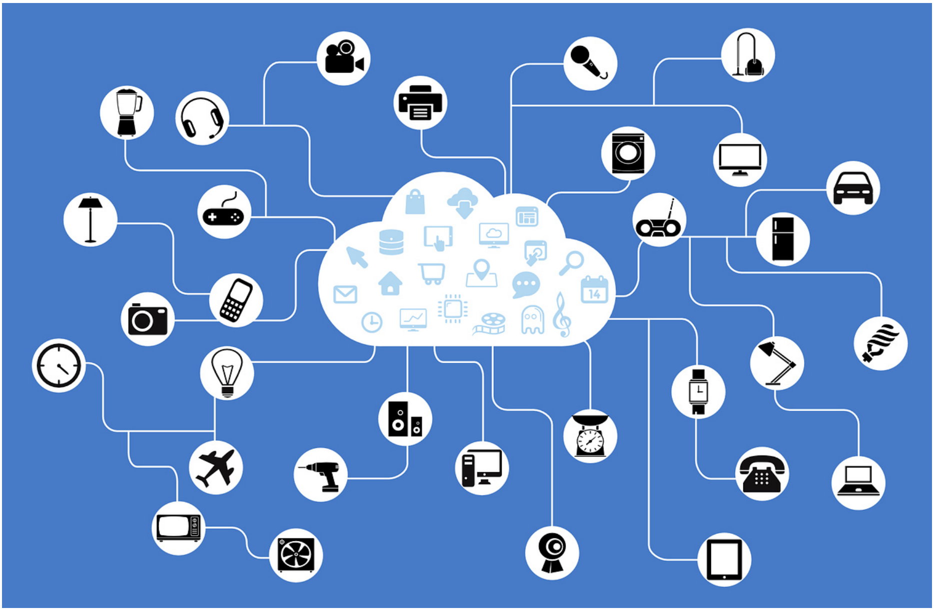
In addition to video cameras or other connectivity hardware, remote office also opens new risks. Employees who work from home may open new vulnerabilities by unknowingly and thus uncontrollably connecting their Internet-of-Things (IoT) hardware to a corporate network via their PC system. Internet-connected devices in a wide variety of sectors - such as industry or healthcare - are creating more touch points to the Internet and thus new potential backdoors into the network. Even if IoT and IT do not yet merge completely, the risk for users is increasing.

Even if the trend slows down somewhat - the signs continue to point to expansion: according to the experts from IOT Analytics Index, the number of IoT devices grew by eight percent to 12.2 billion worldwide in 2021. According to Verizon's 2022 Mobile Security Index, 31% of those surveyed responsible for purchasing, managing, and securing IoT devices admitted that hackers had compromised their IoT. Two-thirds of these experienced a "major impact": 59% complained of system failure, 56% of data loss and 29% had to pay compliance fines. 41% of respondents admitted to sacrificing IoT security concerns to get their jobs done.

Various stakeholders are responsible for the security of IoT devices, such as trade associations, authorities, and national governments. However, a primary responsibility lies with manufacturers and users. IT administrators need to be aware that "irresponsibility" can become a security risk for them.

What can manufacturers do? - Enforce security standards

- **Co-develop security:** Making IoT functionalities more secure often requires only a few precautions, as many risks stem from negligence and lack of transparency in development. When manufacturers create undocumented users with default passwords, these are not known to the user. Forgotten over time, they are nevertheless fully functional and often have extensive rights. Hackers take advantage of this and search for vulnerabilities with automated tools. Therefore, manufacturers



must disclose these accounts so that users can deactivate them or provide them with their own access data. IT administrators must expect cybercriminals to escalate the rights of unknown users.

- **Raise risk awareness:** Manufacturers should make changing the password at set-up mandatory by default to educate users to be better and more aware of their own passwords. This simply and very effectively creates more security. It also protects IoT identities, which can then be monitored by an identity management solution.

- **Automate updates:** Since users are usually too comfortable to perform updates or simply forget to do so, manufacturers should take on this task themselves and offer automated updates. After all, it is important to always keep the software for IoT products up to date. Users expect the plug-and-play promise to be kept or simply do not have time for the IoT administration effort. The responsibility to offer up-to-date software lies with the manufacturer to an even greater extent in the Internet of Things than in classic IT.

- **Use standard operating systems:** According to Bitdefender data, proprietary operating systems cause 96 percent of all discovered security vulnerabilities. And this even though they only account for 34 percent of the devices monitored. Therefore, standard operating systems should be a purchasing criterion when choosing IoT hardware.

- **Security through cooperation:** Equally important is the cooperation of manufacturers with IT security experts, which often works well. However, there are still manufacturers of IoT hardware who do not name a security contact. This delays the joint remediation of vulnerabilities to the detriment of users. IT administrators should follow the communications of the IoT hardware manufacturer of their choice to learn about any zero-day vulnerabilities that may have been discovered.

What can users do? - Recognise the value of security

- Don't be lulled into a false sense of security: IoT hardware is quickly installed by individual employees or even building technicians who do not always have the IT security expertise of an IT department. They often ignore the resulting risk. This consists, for example, of using a hijacked IP video camera for a distributed denial of service attack. Other attackers try to use it to get into the company network. The private user may not notice this danger because it does not directly affect him and the behaviour of his computer. The user should always keep this in mind and carefully seek the way into the Internet of Things. IT administrators should educate their staff about these risks. A procurement department that provides its own IoT hardware helps prevent proliferation and can gain control.

- **Quality has its price:** security is usually not an empty brand promise, and therefore users should rather not save at the wrong end. If you don't want to spend a lot of money, you are more likely to buy a risk. Compared to no-brands, which often leave a lot to be desired in terms of security and have no or at least no realistically accessible support, expensive devices here offer added value in terms of security, documentation and support. Every security team in a company benefits from this.

- **Short lifespan = security with an expiry date:** Many devices are only designed for a short period of use and are not intended to exceed this. Companies often use their video camera or door security system, for example, for as long as they work. In the meantime, manufacturers may have discontinued their support and the systems become obsolete in terms of security technology. Without updates, this creates security gaps due to threats that become known to hackers in the meantime. IT security officers should remove obsolete hardware.

- **Password discipline:** Pre-set passwords should be changed immediately. Continuous change or a suitable password manager is recommended for further operation. For most hackers, pre-set passwords are easy to crack when they use tools to specifically search for IoT devices.

- **Finally . Don't forget your own data protection:** All IoT devices share data - that's their job, that's what they were designed for. A server for this information outside the EU certainly has different and often weaker data protection specifications. Anyone who wants to maintain control over the increasing amount of data that will also be transported via the Internet of Things in the future should pay attention to this from the very beginning.

Last Line of Defence

In the face of such externally imposed problems, IT security managers must above all gain and maintain visibility over connectivity to the internet. The confusing and dynamic nature of this area of IT, which is often beyond their control as shadow IT, does not make this task easy. Above all, it is important to control access to the corporate network via IoT at the latest. An IT security that holistically monitors IT can also keep an eye on the IoT endpoints and their impact on the behaviour of PCs, systems, and applications.

Author: Jörg von der Heydt, Regional Director DACH at Bitdefender

SURVEY BY G DATA AND STATISTA:

Germany: IT security sentiment has declined

Study "Cybersecurity in Numbers" reveals major shortage of IT security professionals in Germany

What is the state of IT security in Germany? The short answer is: Poor. The Corona pandemic and the Ukraine war are influencing the mood. The new magazine "Cybersicherheit in Zahlen" by G DATA CyberDefense and Statista contains a detailed picture of the situation. The employee survey it contains shows the biggest problem areas of digitalisation in Germany: Shortage of skilled workers, fear of cyberattacks and lack of knowledge about what to do in an IT emergency.

The current study "Cybersecurity in Numbers" by G DATA CyberDefense and Statista proves: The Corona pandemic and the Ukraine conflict have also left their mark on IT security. The G DATA Index Cybersecurity has declined by two percent within one year.

This means that the perceived IT security in Germany has decreased. In particular, the index values for expertise and the feeling of security have fallen. At the same time, the perception of risk has declined.

In the professional environment, one third of the respondents assess the risk of falling victim to cybercrime as high or very high. In the private sphere, the proportion is even higher - at 38 percent. One possible reason: many people lack the skills to protect themselves and their digital devices accordingly.

"For many years, cyber security was mainly a topic for the IT department, which management only wanted to deal with selectively at best. This was and is a misjudgement," says Andreas Lüning, co-founder and board member of G DATA CyberDefense. "IT security may start with technology. But it doesn't end there by a long shot. Managers must set an example of a good error culture and encourage employees to report errors that could endanger security."

Great staff shortage in IT security

For the second time, Statista conducted a representative study on the state of IT security in Germany on behalf of G DATA. More than 5,000 employees were surveyed in a professional and private context.

The survey shows how great the lack of personnel in IT is: Overall, 36 per cent of respondents complain about a lack of employees in the IT sector. The situation is much more dramatic in small companies. In companies with fewer than 50 employees, more than two-thirds of the survey participants speak of a lack of staff. It is therefore not surprising that employees for IT in general are desperately sought - especially for the area of IT security. More than 44 percent of respondents from large companies have the greatest need for action here.

The survey shows how great the staff shortage is in IT: Overall, 36 percent of respondents complain about a lack of employees in the IT sector. The situation is much more dramatic in small companies. In companies with fewer than 50 employees, more than two-thirds of the survey participants speak of a lack of staff. It is therefore not surprising that employees for IT in general are desperately sought - especially for the area of IT security. More than 44 percent of respondents from large companies have the greatest need for action here. "The study by G DATA and Statista shows that there is no such thing as one hundred percent IT security. We should not offer attackers more attack surfaces than necessary," says Robin Rehfeldt, Senior Analyst at Statista. "In the second edition of 'Cybersecurity in Numbers', we focus on companies and organisations, look at systems, structures, or processes. And ask: How can and must companies position themselves in a world that is becoming more dangerous? How does security work - for the institution, the management, the employees?"

Comprehensive reference work on IT security

These exclusive figures are just a glimpse into the "Cybersecurity in Numbers" magazine by G DATA, 'Brand Eins' and Statista. In addition to a large-scale employee survey, the magazine contains exciting figures on IT security and serves as a broad reference work on the topic of cyber security:

- The number of reported phishing cases has increased by more than 1,560 percent within five years (source: FBI).
- The annual damage caused by ransomware has increased by 358.5 percent in Germany from 2019 to 2021.
- One third of German companies fell victim to a phishing attempt in 2021, according to the "Germany secure online" initiative.

"Cybersicherheit in Zahlen" is characterised by a high density of information and particular methodological depth.

The magazine "Cybersicherheit in Zahlen" is available for download free of charge here with contact details: www.gdata.de/cybersicherheit-in-zahlen

G DATA IT Security Trends 2023

Professional cybercriminals further increase risk for companies

Social engineering and misuse of standard applications pose a massive threat to IT security in Germany

To increase their profits, cyber criminals are using increasingly sophisticated and efficient methods. To do so, they refine and change their methods of infiltrating networks on the one hand and use new tools for their attacks on the other. Therefore, vulnerabilities in systems that are used across the board are a particular risk. This includes, for example, the Java vulnerability Log4Shell, which criminals used to gain access to company servers and which is still being exploited. This shows that a single gap is enough for attackers to compromise several hundred or even thousands of companies at the same time. Therefore, administrators must always keep servers and end devices up to date with the latest software.

"A central problem for IT security in Germany is and remains that companies do not take warnings about vulnerabilities or security risks seriously," says Andreas Lüning, co-founder and CEO of G DATA CyberDefense. "They continue to underestimate the real risk of a cyber-attack for themselves and rely on the principle of hope. In this regard, responsible parties must act now, because in view of the tense economic situation, no company can

afford to lose sales or business interruptions that have their origin in an IT security incident."

Rootkit renaissance

Another avenue of attack: rootkits are once again increasingly used in attacks in which cybercriminals combine various malicious programmes. This is because rootkits can be used to hide malware from security solutions. In this way, criminals' logins to the computer are disguised, as are the files and processes associated with this process. Researchers have demonstrated in a feasibility study that attackers copy rootkits from GitHub, a platform for managing open-source software, and incorporate these programmes into their attack chains to infiltrate companies.

"The problem is that rootkits are not considered malware in the original sense and are therefore legally made available on GitHub," comments Karsten Hahn, Lead Engineer Prevention, Detection and Response at G DATA CyberDefense. "Especially for criminals with little IT knowledge, such offers are interesting, because programming rootkits is anything but trivial."

Without skilled workers, IT security is lacking

One major challenge affects small and medium-sized enterprises in particular: The lack of trained IT security specialists. The lack of know-how has a lasting effect on the level of IT security. Medium-sized companies cannot close this gap on their own. One way out of this dilemma is offered by managed security services and employees trained in cyber dangers. It is important that companies act now. An attack on IT with potentially uncontrollable consequences can happen at any time.

Targeting end users: iPhone as a target

Private smartphones remain an attractive target, not only because users use them for mobile banking and payment or as digital keys. In the future, cyber criminals will increasingly target iPhones. The reason: iPhone users are considered to have more purchasing power and are therefore more lucrative for attackers.

"The criminals exploit vulnerabilities in the iOS operating system in particular, because this gives them root rights and thus complete control over the device," warns Stefan Dekker, mobile security expert at G DATA CyberDefense. "The current year has shown how serious the situation is, as Apple has had to provide patches for critical gaps several times." Users must therefore install provided patches and updates for their smartphone as quickly as possible.

Social engineering: humans in the crosshairs

As technological protection against malware has improved significantly, cybercriminals continue to adapt their attack methods.
Social engineering attacks can hit anyone and are aimed at grabbing personal data or information from victims. Smartphones play a decisive role here: attackers are increasingly contacting their potential victims via messenger services such as Whatsapp or Telegram.

Current fraud attempts show how real the danger is. Perpetrators have shifted the grandchild trick into the digital space, so to speak as "grandchild trick 2.0". Perpetrators pretend to be a family member in need and try to persuade their victim to transfer a larger sum of money.

Anyone who receives an emergency call should - as difficult as it may be - keep a cool head and analyse the scenario. And check on another channel (e-mail or telephone call) whether the emergency described has occurred.

More functionality for BWV solution

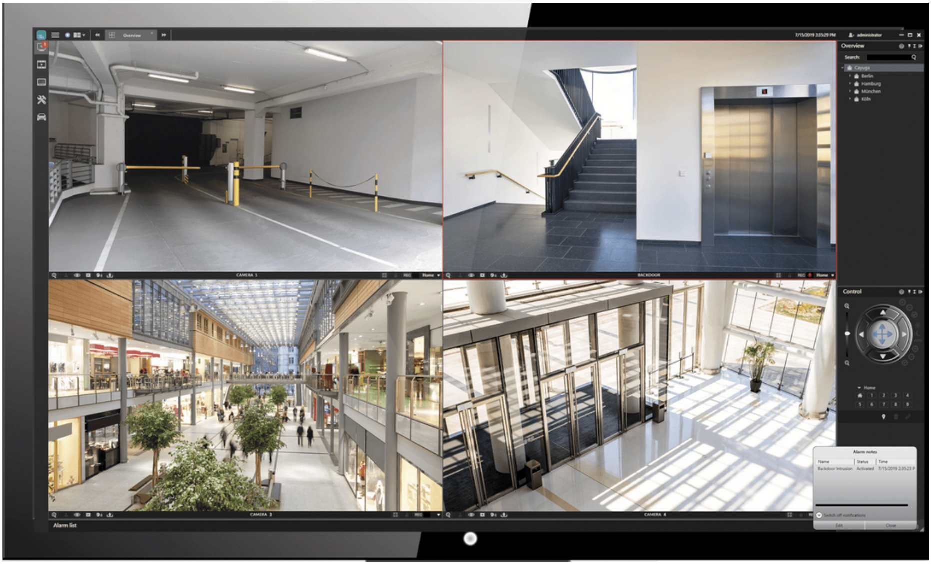
Qognify VMS 7.2 supports the investigation process and adds cloud functions

Qognify, a provider of video and enterprise incident management solutions, has launched the second version of its video management software, Qognify VMS. The latest software release - Qognify VMS 7.2 - features expanded support for body-worn cameras, additional features to support investigations and a new web client architecture.

Qognify VMS 7.2 addresses the increasing use of body worn video (BWV) in many areas, from law enforcement and security applications to customer service and quality control. As BWV has become an important component in the security ecosystem of many Qognify VMS customers, the need to integrate BWV footage into a fully featured VMS environment for investigative purposes is becoming increasingly apparent. In this context, it is critical that the BWV integration framework can maintain the chain of evidence of captured footage for law enforcement applications. As such, Qognify has worked closely with BWV system manufacturers to ensure that chain of evidence protocols is adhered to - especially when devices are used in multiple shifts by different users. With Qognify VMS 7.2, these advanced features are now available to organisations using Axis BWV. Integration with other manufacturers will follow in future versions.

In addition to supporting more video sources, Qognify VMS 7.2 offers new enterprise-class features to simplify investigations and improve data protection. Cameras, site plans and layouts can now be given logical labels and thus grouped accordingly. For example, if operators want to see video feeds from all cameras in a particular stairwell, they simply select the appropriate entity label, and all corresponding cameras are automatically displayed - regardless of where they may be in the logical structure of the installation. This allows operators to get a full picture of the situation more quickly and realise efficiency gains. As the investigation process is often linked to data protection issues, with Qognify VMS 7.2 it is now also possible to restrict access to certain cameras to specific workstations. In addition, a new static scramble feature allows a specific area within the camera image to be blurred using an adjustable privacy mask, opening video masking to a whole new range of applications.

Qognify VMS 7.2 also continues the company's strategic initiative to develop enterprise-class cloud capabilities. As part of the release, Qognify now offers cloud storage offerings tailored to the specific needs of video management. Using traditional cloud storage solutions often comes at an unpredictable cost, as the cloud storage provider typically charges for retrieving video material from its servers.



Many IT departments cannot factor this into their budget structure, which often discourages them from using this technology. In contrast, Qognify only charges for the volume of cloud storage used on a terabyte basis, regardless of how often the customer needs to retrieve video - resulting in consistent "pay as you go" costs that are easy to budget for.

The new software release also offers a first look at Qognify's new web client architecture, which features powerful video rendering.

Yaniv Toplian, VP R&D at Qognify, explains Qognify's approach: "Many VMS web clients either require the installation of additional software components, making them inflexible and posing cybersecurity risks, or they compromise on display performance and latency. To overcome this, we have developed a revolutionary new streaming and playback technology that enables the display of video streams with very low latency in a standard browser environment without additional software components. This is all the more important as the web client is an integral part of Qognify's comprehensive cloud strategy, which aims to provide companies with the highest level of flexibility for their deployments."

The new Qognify Web Client creates a framework that enables companies to improve their investigation and response processes through adaptive workflows and enhanced communication and coordination capabilities. Limited functionality will be available for Qognify VMS 7.2, which will continue to expand with each new release.

Jeremy Howard, Vice President of Sales, Physical Security - Americas at Qognify, highlights another important aspect of the new version 7.2: "Following the launch of Qognify VMS in April this year, we have experienced massive interest from customers currently using other Qognify VMS products to transition to our new flagship solution as it uniquely meets the specific requirements and use cases of many industries. We are excited to be able to offer this level of flexibility to our customers and want to make their transitions within our solution portfolio as easy as possible. With the new release, we have therefore enhanced Qognify VMS with some true enterprise functionality that customers have come to value in other VMS solutions from us. In addition, we are providing powerful practical tools to support a smooth transition."

For customers looking to upgrade from Ocularis to Qognify VMS, a powerful upgrade tool is therefore available that automates large parts of the conversion process and enables efficient conversion of even large systems with several hundred cameras in less than a day. While the recordings remain untouched as both systems use the same recording platform, the upgrade tool transfers users, groups, permissions, and views from Ocularis to Qognify VMS.

Qognify VMS 7.2 is available immediately worldwide.

Frequentis

Saarland Integrated Control Centre

Commissioning of the emergency call enquiry and radio switching system by ZRF Saar - Award of contract for the new procurement of the emergency call enquiry and radio switching system for the control centres of ILS Saarland Strengthens market position in the BOS sector - Fully redundant communication system based on Voice over IP (VoIP)

ZRF
Zweckverband für Rettungsdienst und Feuerwehralarmierung Saar
3431
Deutsches Rotes Kreuz
RETTUNGSDIENST
Notruf 112
NOTARZT

Frequentis Deutschland GmbH was awarded the contract for the project by the Zweckverband für Rettungsdienst und Feuerwehralarmierung Saar (ZRF Saar) during an EU-wide tender for the delivery and integration of the communication systems at the main site in Winterberg and at the redundancy sites in Merzig and Bexbach.

Saarland has almost 1 million inhabitants and an area of around 2,570 km². The ILS Saarland is the only control centre for non-police emergency response in Saarland. Its main tasks are answering emergency calls, alerting the emergency services, coordinating rescue operations, and dispatching ambulance transports.
Against the background of long-term economic efficiency in use and operation and necessary further developments of the system technology, the following objectives of the procurement measure resulted:

- Very high availability of the communication technology

- Comprehensive system networking of the new communication technology for flexible staffing of available workplaces and use of resources at the locations

- Expandability of the system with a view to further future services and a changed environment

- Economic efficiency by integrating the new communication technology into the existing modern IT infrastructure of the ZRF

- Favourable use of standard applications and open source, i.e., fundamental renunciation of special developments specific to the control centre.

To meet these requirements, the ASGARD communication system will now be used. ASGARD integrates all means of communication of a control centre into one application and thus enables a uniform, fast and, above all, safe operation optimised for the needs of modern security centres.

The proven Frequentis software solution - the ASGARD communication system is already in use in about 50 control centres in Germany - ensures communication management for these tasks thanks to its high flexibility and fail-safety, as well as the diverse possibilities for integration into infrastructures.

Rainer Buchmann, Head of Department at ILS Saarland: "We are looking forward to the cooperation with Frequentis. With Frequentis, we have found a company that can provide us with a modern IT and communication system "from a single source" and based on modern IP technology.
With this system, the Saarland's non-police emergency services will be optimally prepared for future requirements and upcoming major emergencies."

Reinhard Grimm, Managing Director of Frequentis Germany, emphasises: "With ASGARD, we can provide BOS control centres with an optimal product for their diverse tasks. We are proud of this showcase project, ILS Saarland, and of the confidence that ZRF Saar has in Frequentis."

Sepura

500,000th TETRA radio put into service in Germany

Sepura has commissioned its 500,000th TETRA radio in Germany, with the device to be used in the city of Munich's underground network. Stadtwerke München is currently installing a new digital radio system in the Munich underground network as part of a project to replace the previous analogue radio technology. As part of the new solution, Sepura - through its German exclusive partner SELECTRIC Nachrichten-Systeme GmbH - is supplying over 1,800 Sepura SC20 TETRA radios and accessories for the new network as part of a tender.

Hendrik Pieper, Managing Director of SELECTRIC, has been working with Sepura since the manufacturer entered the German market. He said: "Sepura's products are known worldwide as robust and reliable products. We have succeeded in the world's largest TETRA market by combining Sepura products with excellent customer service for users in public safety and commercial organisations across the country. We look forward to continuing to support these customers in the future."

In addition to the Sepura handheld radios, SELECTRIC's offering also included handheld microphones and charging stations that were custom designed by WETECH to the customer's specifications for use in the vehicles. SELECTRIC also took care of the integration of the TETRA communication network into the existing control centre, programmed the Sepura TETRA radios, conducted training for the radio users and accompanied the deployment with comprehensive technical support. The full takeover into active operation is expected by the end of 2023.

Hooman Safaie, Regional Sales Director at Sepura, said, "We are proud to reach the milestone of half a million radios installed in Germany. We are increasingly seeing commercial organisations with mission-critical requirements, such as Stadtwerke München, choosing Sepura radios and benefiting from the proven, robust design and flexible features that can be tailored to their operational requirements. We look forward to providing German users with first-class communication solutions for many years to come

JOHNSON CONTROLS

Fire protection and security solutions for buildings

Advanced CKS software solutions for control centres, including the new CEUS Alarm Display Web, and enhanced features of Tyco Integrated Systems Manager (TISM), which helps improve safety and efficiency in buildings - these were just some of the innovative solutions Johnson Controls showed at this year's PMRExpo.

The three days were all about making processes and workflows more effective and sustainable for secure digital communication. At Johnson Controls, this includes networked building security systems and control centre software.

"We have an extensive portfolio in store for trade visitors to the fair," announced Jörg Keßler, General Manager Germany at Johnson Controls. "In addition to the intelligent software solutions CELIOS, CEVAS and CKS Datawarehouse, we will, for example, present our new CEUS Alarm Display Web to the public for the first time in Cologne."

Another trade fair highlight from Johnson Controls was the latest developments of the TISM platform, which enables complete and reliable integration of the entire building security and communication technology in a central software platform. This makes buildings and environments safer once again - and in an efficient way.

The PMRExpo stand of Johnson Controls in detail:

1. intelligent software solutions rescue service, fire brigade + C.o

/ CELIOS mission control system

From the acceptance of a mission to its management: the mission and hazard management system CELIOS from CKS Systeme has been supporting the control centres of rescue services, fire brigades and police for many years. In Cologne, Johnson Controls will present its software innovations, among others, for the areas of message and status overview, processing of measures as well as web client and interfaces.

/ CEVAS Fire Brigade

The CEVAS Fire Brigade System is especially suited for reporting and statistics of fire brigade operations. It supports control centres in optimising their reporting and ensuring quality - for example, by automating and greatly simplifying the creation of statistics and documentation. It uses data from the CELIOS control centre system, creates reports independently, including image attachments, and includes comprehensive master data management. CEVAS also supports fire brigade control centres in mission accounting.

/ Statistics module CKS Datawarehouse

The CKS Datawarehouse database enhances CELIOS, CEVAS Fire Brigade and CEUS for even more efficient operational planning by providing all relevant data clearly arranged on interactive dashboards, thus helping emergency services to make good decisions even faster and based on data.

/ CEUS Alarm Display Web

The new CEUS Alarmdisplay Web now displays current operations of the control centre on a modern interface in the browser - independent of operating systems and without extensive installation. Via the alarm view of the add-on, the persons in charge not only see the respective status of their vehicles, but also the most important operation parameters. They are also shown the location of the operation in a satellite image or as a classic map. In idle mode, the guard display offers additional information such as a weather map or a live TV stream.

2. Networked security, building and communication technology

/ TISM security platform

With the Tyco Integrated System Manager (TISM), Johnson Controls offers an independent and user-friendly solution for the integration of security systems in a central software platform.

By collecting, logging and visualising the events, data and information of connected security systems, such as video, access or intrusion detection systems, TISM enables its users to identify and analyse situations better and faster - and thus become significantly more efficient.

Whether control centres or buildings of a completely different kind: in addition, action plans as well as routines running automatically in the background relieve the users and ensure that the security and building management systems run smoothly.

The CKS Systeme GmbH dispatch system for fire brigade and rescue service control centres as well as police and industrial control centres.

The demands placed on dispatchers in control centres are subject to major change: intensified threats, changing operational conditions, standardisation work, advancing networking and digitalisation require a high degree of flexibility, both in terms of work processes and control centre technologies. Today, a command and control system must meet a wide variety of demands and adapt quickly and easily to ever-changing customer requirements. To achieve this, the underlying control centre software in particular should be scalable.

Whitepaper-Download: https://tinyurl.com/5cbcsn2p

PMRExpo 2022
powered by PMeV

Emergency services receive new safety-critical applications

Integrated communication solutions can optimise the way emergency forces work and operate and bring about lasting changes to safety in the field.

At PMRExpo 2022 in Cologne, Germany, Motorola Solutions demonstrated how its integrated portfolio of solutions can help public safety agencies and organisations, as well as mission-critical organisations, provide their responders with the information they need to make better and safer decisions.

Highlights of the PMRExpo show include the first mobile safety-critical software solution based on Apple CarPlay, which allows responders to access and process data from their cars through a single, intuitive interface. The new solution is already being used by more than 6,000 Western Australia Police officers, who coordinate around 84,000 calls for service each month via the new app. The new software solution is part of Motorola Solutions' comprehensive and fully integrated portfolio of TETRA and advanced broadband solutions, body cameras and video security solutions, software applications and cyber security and managed services.

"With our innovative strength, we help first responders to simplify and optimise their work in frontline operations," explains Axel Kukuk, Country Manager Germany at Motorola Solutions. "Our portfolio integrates terminals, video solutions and infrastructure, which are often seen separately, into one overall solution. This helps responders access data they need to make more effective decisions."

- **Digital Policing:** PSCore, the new smart mobile application platform for public safety, is the first of its kind in the world to work with Apple CarPlay. It integrates seamlessly with many public safety systems and simplifies officer workflows by providing access to critical details through a single, intuitive interface.

- **Seamless Broadband MCPTT and LMR:** WAVE PTX is a push-to-talk service that connects teams across multiple devices, networks and technology. With Critical Connect, Motorola Solutions is demonstrating a cloud-based communications solution that removes barriers between different communications networks and supports seamless voice and data communications across different security organisations and across country and network boundaries. The goal is to decisively improve communication between authorities during large-scale operations or cross-border disaster situations.

- **TETRA and LTE devices:** The MXP 7000 is a portable all-in-one device for mission-critical communications. It combines TETRA and 4G LTE voice and data communications to improve situational awareness, safety and productivity of responders.
The versatile MXM7000 can transform any vehicle into a mobile broadband hotspot with its LTE connectivity. It extends connectivity and coverage by linking a range of communication devices.

- **Cyber Security:** Motorola Solutions' ActiveEye Managed Security Platform provides continuous visibility into security-related activity with automated notifications and reports. It is based on a flexible architecture that can evolve with modern IT systems.

- **Video security and access control:** At PMRExpo, Motorola Solutions will present its scalable video portfolio. This includes the VB400 bodycam and video management solutions, the M500 in-car video system and the L5M (Automatic Number Plate Recognition) mobile ANPR system that maximises recognition and data capture. Also, the Openpath keyless entry solution, which provides reliable access control with intelligent video and intercom capabilities, cloud-based software and an open ecosystem.

www.euro-security.tv: Video statements from the Motorola stand at PMR Expo 2022

Ricardo Gonzalez
MSSSI VP EMEA Strategy and Marketing, MOTOROLA SOLUTIONS

Darren Wood
Solution Architect - International Mobile Video, MOTOROLA SOLUTIONS

Kostyantyn Steblovskyy
End User Video Account Executive, MOTOROLA SOLUTIONS

PMRExpo 2022
powered by PMeV

Airbus

What is Tactilon Agnet?

Tactilon Agnet brings secure group ommunication to smart devices

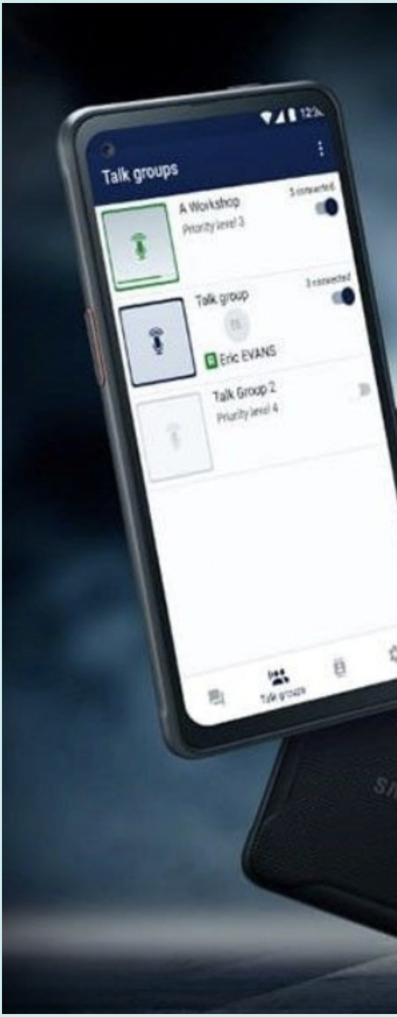
With Tactilon Agnet, smart device users become part of the professional world - voice, data, video, and localisation services are all available, providing the reliability and security that professional users expect. Tactilon Agnet is an extensible collaboration solution that takes full advantage of smartphone capabilities in a secure and controlled way. The workers needed for an operation can be connected easily and securely, even if they use different devices and technologies. Tactilon Agnet meets the needs of public safety organisations as well as commercial users. Tactilon Agnet runs on traditional or rugged smart devices and provides a very simple and intuitive user interface for workers in the field.

Airbus

Download data sheet for Tactilon Agnet 900

Tactilon Agnet 900 provides apps for voice, images, location and other professional applications over broadband in centrally controlled user groups.
All this includes quality of service management and end-to-end encryption according to 3GPP standards for mission-critical services.

Agnet 900 is designed for professional use in police, fire, healthcare, defence and for SWAT teams and is perfect for group communication with different requirements.
The application runs on traditional or rugged smartphones and tablets and offers a very simple and intuitive user interface for the staff in the field.



securelandcommunications.com

Co-operation with Samsung

Samsung collaborates with Airbus on smartphone with integrated Tactilon Agnet solution

Samsung has just launched a new

XCover6 Pro smartphone that offers new and improved options to users of critical communications. The new Samsung smartphone, combined with the Airbus Tactilon Agnet MCX solution, has won the ICCA award for best MCX solution of the year, enabling successful mission- and business-critical communications even under demanding conditions.

Airbus has developed and tested the Tactilon Agnet solution together with Samsung, and the just launched XCover6 Pro smartphone delivers new service delivery solutions and MCX services for demanding users. Samsung Knox products complement Tactilon Agnet deployment with easy-to-use firmware management, a licence server for offline activation, bulk enrolment and numerous other features to support users of critical communications. With Samsung Knox Security, security and quality management can be implemented even more efficiently. "This announcement demonstrates that a global and leading technology company can meet mission-critical user requirements for endpoints. Airbus' Tactilon Agnet solution for Samsung Knox-enabled smartphones ensures quick and easy deployment, use and security of MCX services," says Samuel Gustafsson, Head of European Sales at Airbus. Samuel Gustafsson continues: "The Tactilon Agnet service on the new XCover6 Pro offers users new features without compromising efficiency and security, which are increasingly important in critical communications." "Security and usability are of paramount importance to government organisations when selecting mobile technologies," emphasised Neil Barclay, Head of B2G, Samsung Europe. "Leveraging our enterprise-class security and staging tools, we have worked with Airbus to establish a unique and easy-to-deploy platform that manages and protects the most sensitive and confidential information on a best-in-class PTT device." The new Samsung XCover6 Pro (pictured below) offers numerous features for field use, including protection

in demanding conditions, programmable hardware keys, a high-performance battery with fast-charging technology and a mono speaker for clear voice communication. In addition, the Samsung XCover6 Pro features a chipset to support LTE and 5G and improve the quality of video streaming and video conferencing capabilities. The International Critical Communications Awards 2022 named Airbus Tactilon Agnet 500 as the best MC-X solution of the year.

Hexagon supports smart city transformation in Brazil

The Brazilian city of Manaus is deploying a Hexagon solution in its City Cooperation Centre (CCC) to support the transformation of the city into a smart city. The integrated technologies provide a real-time operational overview of the city and its respective automation initiatives, as well as AI-based services that accelerate emergency response and improve public works.

Established in 2021, the Manaus CCC houses the civil defence, municipal guard, transport, and urban mobility agencies. The centre aims to improve the quality of life of 2.2 million inhabitants by better predicting and responding to citizens' needs through better collaboration between public organisations
.

Hexagon's solutions provide the information and capabilities that enable the CCC to automate incident detection and response - from public safety emergencies to parking violations to infrastructure repairs. By integrating data from surveillance systems, weather stations, public applications and sensors throughout the city, Hexagon systems will generate notifications that are automatically analysed and assigned to the appropriate department for response. The new coordinated workflows will allow authorities to identify and address problems and emergencies more quickly.

"This is a significant technological development because it allows us to monitor and respond to incidents in real time," said Sandro Diz, Superintendent of the Manaus City Cooperation Centre. "The next step is to integrate other agencies and services outside the municipality so that the city will be even more connected.

Manaus CCC is using HxGN OnCall Dispatch, Hexagon's industry-leading computer-aided dispatch solution, to centralise dispatching and incident response dates and workflows, including HxGN OnCall Dispatch | Smart Advisor, a supporting artificial intelligence (AI) solution that evaluates operational data and alerts staff to emerging situations. The centre will also use Hexagon's Physical Security Information Management (PSIM) capabilities to integrate and analyse data from sensors and other systems to provide real-time monitoring and unprecedented situational awareness.Staff will also use Hexagon's M. App Enterprise to visualise and analyse data to improve planning and operations through intuitive map-based dashboards and applications. "By integrating, modernising and digitising city operations, Hexagon is helping Manaus bring its smart city project to life," said Sergio Nunes, senior vice president for Latin America at Hexagon's Safety, Infrastructure & Geospatial business. "The use of emerging technologies such as the Smart Advisor AI assistance solution makes Manaus a pioneer among South American cities, and we are proud to support their efforts."

What is HxGN OnCall Dispatch?

The dispatch software for emergency and disaster management

The HxGN OnCall Dispatch product suite provides police, fire, EMS and industrial dispatch centres with high quality dispatch capabilities to minimise staff workload and increase dispatch centre performance - both during incidents and major events.

HxGN OnCall Dispatch is the next generation flexible dispatch product suite. It offers dispatch functions for control centres of all types and sizes - including the connection of mobile task forces. The HxGN OnCall Dispatch product suite is either installed on-site, in the cloud or pro ided as SaaS (Software as a Service). The product suite is used to handle incidents at control centres and emergency call centres, remote duty stations, mobile units and anywhere first responders and emergency assistance are needed.

HxGN OnCall Dispatch:

- Increase the capacity of dispatch management
- Improve situational awareness and coordination
- Optimise communication
- Optimise inter-organisational collaboration
- Improve reporting and transparency
- Increase public confidence in the work of BOS.

The product suite is accessed via browser and / or mobile app . HxGN OnCall Dispatch can be adapted to needs and new technologies faster and more cost-effectively than traditional systems. With its flexible licensing structure and functionality, Advantage also includes HxGN OnCall Dispatch | Dashboard for dynamic visual overviews of events, units and tasks.

HxGN OnCall Dispatch | Viewer is a way to add basic functionality to access information from the dispatch system while reducing staff workload. The Viewer is a user-friendly web application that allows users outside the control room to view events, browse real-time and historical information, and create incidents - as long as they are not emergencies.

Emergency call centre and operations control centre

In emergency call centres and dispatch centres, every second often counts.

The call takers and dispatchers must be able to record incident-relevant information in an uncomplicated manner and initiate measures quickly.

Advantage provides a clear picture of the situation and enables faster procedures without overloading the user with unnecessary information.

Advantage optimises the coordination between the control centre and the emergency services and supports cooperation across organisational boundaries.

The solution includes:

- An innovative user experience (UX)
- Faster procedures
- Optimised workflows
- A comprehensive situation picture
- Automatic user support
- NG112 and message-based communication with the control centre
- A map provider of your choice
- Uncomplicated configuration

Building design with advanced IP video systems

Integrating video security into building plans with AXIS Plugin for Autodesk® Revit®

Network-based video security, audio and other networked sensors are an important part of any new building today. In the past, video security solutions were at best added as an afterthought to finished buildings, but today they are already being planned as an integral part of the building infrastructure. In this article, we show how Axis supports this via the AXIS Plugin for Autodesk® Revit®, one of the world's most popular building design software solutions..

Among other building systems and infrastructures - from power supply to network cabling, from heating, ventilation, and air conditioning (HVAC) to plumbing: Network-based video security, network audio and associated sensors are now key components of any new building. As these technologies become more comprehensive and advanced, and given innovations in advanced analytics based on deep learning, network video, audio and their associated sensors are given other important roles in addition to providing security. Combining technologies can optimise building use, increase energy efficiency and, of course, ensure the protection of the people who use and occupy the building.

Integration of network video into the structure of a building

Given their great importance, architects must plan network video and audio into the structure of a new building from the outset, alongside the other important services and components. To do this, they need to be able to add the devices and associated technology directly into their design solution. The AXIS Plugin for Autodesk Revi gives architects and building designers access to the entire portfolio of Axis technologies. Autodes Revit is one of the most popular BIM (Building Information Modelling) software solutions.

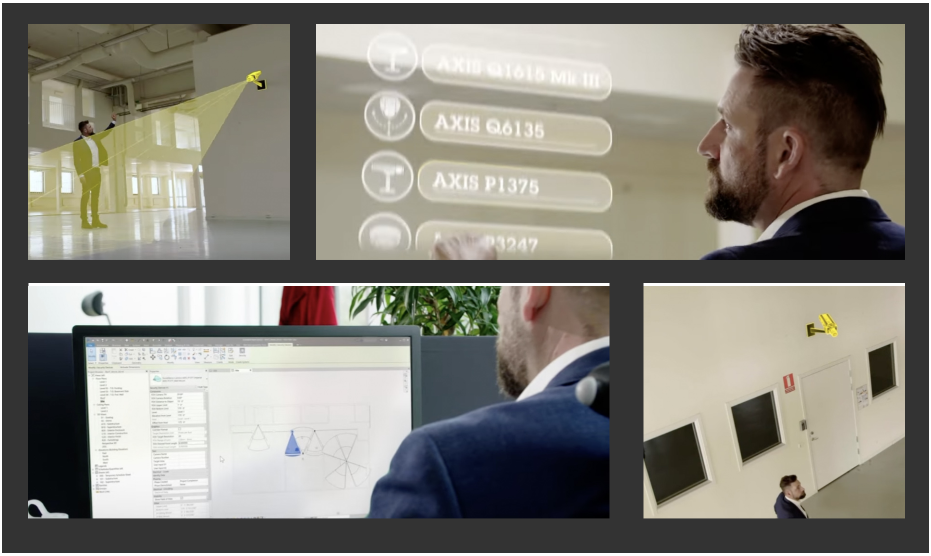
The software enables architects, designers, structural engineers, mechanical engineers, electrical engineers, planners, and construction professionals to design buildings and structures and their components in 3D and create coordinated designs and plans from concept to completion. In Autodesk Revit, every aspect of the building can be planned and specified, from foundations to furnishings.

The AXIS Plugin for Autodesk Revit supports all current versions of Autodesk Revit (including the latest version 2023) and brings the Axis portfolio of network devices into the designer's building design. The plugin not only allows the targeted selection of a specific Axis product and its integration into the 3D projects, but can even display, visualise and customise the coverage of individual security cameras or speakers according to the client's requirements.

Full interactivity in planning the security solution

Of course, each Axis camera has its own specific technical characteristics and optimal application areas. Therefore, it is important that building designers consider the technical parameters of the model-specific device when planning the video security or audio solution in a building. With Axis Camera Viewer, when inserting a camera into a project, the designer can view a complete 3D visualisation of the covered area from the camera's point of view. This is an intuitive way to check camera positioning and settings. This visualisation is indispensable if you want to take customer expectations into account early in the design process.

When a camera is added to a project,



the plug-in simulates the hardware control of the cameras. Once the camera position is selected and the mounting configuration is set, the camera height, pan and tilt angle and zoom are set to define the field of view of each unit.

There are several pixel density (PPM/PPF) settings to illustrate the field of view for industry standards - from detection to identification - and ensure consistency with actual results. Finally, there is a setting to illustrate the corridor format, a 90° rotation of the camera lens to verify that a scene is fully covered.

Once the desired settings are set for all cameras, solid or transparent objects in the projected field of view are detected with the Collision Detection function. This rendering provides a realistic 2D representation of the camera's field of view and shows exactly what the camera can detect.

The designer's perspective

Nathan Mudler, production manager at Guidepost Solutions LLC, uses the AXIS Plugin for Autodesk Revit every week. He explains its benefits: "The plugin adds useful functionality to Autodesk, both as solution design support and by providing easy access to up-to-date content from Axis, such as product information and configurations."

"We use it in design projects for the commercial, healthcare and education sectors, and I find the 3D view and collision detection incredibly handy to automate work that I previously had to do manually.

For example, we recently completed a project where we developed 3D views and applied Collision Detection to a plan with 120 Axis cameras. Automation saved us a lot of time, plus we were able to provide a very detailed design to the installers on site, which also made for a more efficient system installation."

The designer's perspective

Nathan Mudler, production manager at Guidepost Solutions LLC, uses the AXIS plugin for Autodesk Revit every week. He explains its benefits:

"The plugin adds useful functionality to Autodesk, both as solution design support and by providing easy access to up-to-date content from Axis, such as product information and configurations."

"We use it in design projects for the commercial, healthcare and education sectors, and I find the 3D view and collision detection incredibly handy to automate work that I previously had to do manually.

For example, we recently completed a project where we developed 3D views and applied Collision Detection to a plan with 120 Axis cameras. Automation saved us a lot of time, plus we were able to provide a very detailed design to the installers on site, which also made for a more efficient system installation."

Network-based video security, network audio and analytics are now as important to a building's infrastructure as any other basic service.

The AXIS Plugin for Autodesk Revit makes their integration intuitive in the fundamental design tool for architects and building designers worldwide.

[https://youtu.be/5t-s8AiXyfk]

ASSA ABLOY Opening Solutions

Opening's Studio software streamlines the specification process for a luxury project in Dubai

Quality and accuracy are critical to delivering luxury projects that deliver on their promise and are worthy of investment. For Six Senses, The Palm, Dubai - a 5-star hotel and branded residences - award-winning architects Brewer Smith Brewer Group sought a partner to streamline Building Information Modelling (BIM) and hardware specification. They chose the experts and software from ASSA ABLOY Opening Solutions.

Brewer Smith Brewer Group (BSBG) is a long-time proponent of the BIM process. It has found that the process increases productivity and reduces delivery times. It has helped them create a portfolio that has industry-leading technical efficiencies in both design and construction.

They use BIM from the concept stage to coordinate the flow of information between designers, engineers, and external contractors. Proper BIM collaboration improves workflows and fosters creativity and a methodical, technically savvy approach to building design. It also ensures open, transparent communication throughout the project. The extensive experience and knowledge of ASSA ABLOY's specification teams made them the ideal partner to work with on such a prestigious project in Dubai.

Acceleration of the project delivery

An important tool for optimising the collaboration between BSBG and ASSA ABLOY at Six Senses, The Palm, was the Openings Studio software. "Openings Studio from ASSA ABLOY was preferred because of its BIM integration with Revit model development and the ease of communication between the architects and the hardware specialists," explains Adam Drawl, Senior Architect at BSBG.

Detailed specifications for door solutions can be created in Openings Studio and then exported to the design software when the project manager needs them. Integration with Revit makes it easy to share information and update hardware sets within the BIM environment.

As the design progresses, Openings Studio simplifies updating and prevents unwanted loss of information. Data on hardware and certification requirements, including fire and egress classes, was always available. The collaboration accelerated the specification of a wide range of ASSA ABLOY solutions for around 3,500 openings - from steel and wooden doors to access control readers, electromechanical locks, and door closers.

"Our specification teams can offer a whole range of project support," says Bala Vignesh from ASSA ABLOY Opening Solution EMEIA. "Being based across Europe and the Middle East, they have in-depth knowledge of local standards and certifications - for green building or fire safety, for example." "They also offer a range of tools that support collaboration and save time for architects and project managers. Not only Openings Studio, but also a BIM library that can be easily imported to support any design or construction workflow." "The onboarding and follow-up were excellent," confirms Mr Drawl. "The ASSA ABLOY team has always been readily available and proactive in helping develop the hardware and addressing any issues that have arisen. Their expertise is key.

[Pdf download https://tinyurl.com/yc4uaxd7]

In the Heliosklinik Cuxhaven, the access systems are maintained by dormakaba - on behalf of VAMED.
©Adobe Stock dormakaba

VAMED trusts in dormakaba for the maintenance of its door and gate systems on dormakaba

Access solutions for a Smooth operational flow

Left Automatic swing doors for fast and safe transport of hospital beds.
©dormakaba

The door systems are also regularly maintained at the Helios Clinic in Kiel.
©Adobe Stock dormakaba

The VAMED group, headquartered in Vienna, is a globally recognised partner for the planning, equipping, construction and operational management of health care facilities. For four decades, VAMED has realised more than 1,000 healthcare projects in 98 countries worldwide. In Germany, the hospital service provider has also been implementing efficient models for the construction and modernisation as well as the technical operation of hospitals for 40 years.

VAMED Germany stands for efficient and modern hospital infrastructure. The company plans, constructs, modernises and operates technology and buildings in such a way that doc-

Nationwide, more than 250 highly qualified service technicians from dormakaba ensure the maintenance and repair of door systems in over 100 hospitals managed by VAMED.
©dormakaba

tors and nursing staff can care for their patients optimally and efficiently at the same time. With VAMED as a partner, hospitals can fully concentrate on their core tasks of medicine and care.

Modern hospitals and healthcare facilities need a strong infrastructure of technology and buildings. Only if everything functions smoothly in the background can doctors and nurses concentrate fully on their work. To ensure smooth operations, VAMED relies on intelligent access solutions that control the flow of people, provide barrier-free, hygienic access for staff and visitors, and ensure safety and fire protection. For example, automatic revolving doors are used in the corridors for fast, trouble-free transport of hospital beds, and automatic sliding doors allow quick access to treatment rooms.

Especially in hospitals, the functionality, durability and quality of door systems are essential over the entire life cycle. Especially in safety-relevant areas, such as operating theatres or intensive care units, trouble-free operation is indispensable. The doors must work - and always.

To ensure this, VAMED 2020 looked for a service partner for the repair and maintenance of the automatic doors and separation systems in the more than 100 clinics managed by the company in Germany. "Our most important requirements were competence, quality, reliability and short response times," explains Sebastian Keim, head of the operating technology working groups at VAMED VSB-Betriebstechnik Süd-West GmbH. With the door and safety specialist dormakaba, which has over 250 highly qualified, factory trained service technicians, dormakaba is one of the most extensive service networks in the industry. The service hotline staff are available on request 24 hours a day, 365 days a year and can often provide "first aid" over the phone.

Strong contract partner

dormakaba's manufacturer-independent service includes sliding doors, revolving doors, swing door drives, sliding glass walls, folding leaf and space-saving doors, door closers, special door products relating to escape routes and fire protection, tripod barriers and turnstiles, personal interlocks, sensor interlocks and gates.

Of course, these also include many door systems from dormakaba itself. Now that the framework maintenance contract with dormakaba has been in place for two years, Sebastian Keim confirms the good cooperation: "We have had good experiences with dormakaba's service so far and are very satisfied with the cooperation."

Revolving doors help reduce energy demand by reducing draughts from outside. They are checked regularly.

© dormakaba

January 2022
State of Physical Security 2021:
Adapting to an uncertain future
Research insights from over 2,000 physical security professionals
Genetec
December 2022
State of Physical Security 2022:
Effectively navigating a changing landscape
Research insights from over 3,700 physical security professionals
Genetec
3

Survey on the state of Physical Security 2022

Cybersecurity concerns - Data from physical security technology is seen as a "mission critical" tool for business operations - Industry is embracing hybrid cloud infrastructures and unified solutions.

Genetec, technology provider for unified security management, public safety and business intelligence, has released the results of its "State of Physical Security 2022 Survey". More than 3,700 physical security professionals worldwide (including end-users and system integrators/installers /vendors) share their experiences on the security strategies used in their organisations to effectively meet the challenges of a changing reality.

The future of security is hybrid

Some 54% of end-users surveyed said their company plans to use a mix of on-premises and cloud-based solutions for its security strategy.

The hybrid approach allows companies to further optimise their existing on-premise investments while leveraging meaningful cloud options to reduce costs, increase security and efficiency, and enable remote access to systems and sensors.

Cybersecurity concerns are on the rise

The convergence of information technology (IT) and security is leading to new approaches to implementing and managing a strong cybersecurity strategy. 64% of IT respondents and 54% of security respondents said cybersecurity tools are a key concern this year.

Use of physical security for business operations

In the survey, nearly two-thirds (63%) of all respondents and seven out of 10 companies with more than 10,000 employees confirmed that physical security and related data are considered "mission critical".

In recent years, physical security has evolved into a strategic resource to address a variety of challenges beyond simply mitigating risk. In addition, physical security now plays a much more important role in the digital transformation of businesses.

Physical security is being unified

Most respondents (64%) said they use both video surveillance and access control in their physical security installations.
Some 77% of these confirmed that their organisation has implemented either integration between video surveillance and access control systems from different vendors or a unified video surveillance and access control solution from one vendor.
"Every company wants to use the latest technology. However, with budget constraints, skills shortages and ever-changing priorities, security managers need to do more with less," says Pervez Siddiqui, Vice-President of Offerings and Transformation at Genetec.

"A unified security platform offers organisations the opportunity to modernise their aging systems while continuing to leverage their existing infrastructure without having to develop expensive and complex custom solutions."

Survey methodology

Genetec surveyed physical security professionals from 25 August to 21 September 2022. After a review of submitted responses, results from 3,711 respondents were included in the sample analysed.

The survey was conducted in the regions of North America, Central America, Caribbean, South America, Europe, Middle East, Africa, East Asia, South Asia, Southeast Asia, Central Asia, West Asia and Australia-New Zealand.

The full report can be downloaded at https://www.genetec.com/a/physical-security-report

IDIS

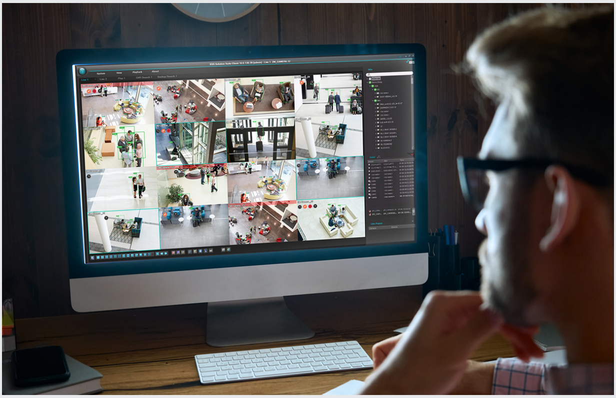
Video surveillance in hotels - for security and guest management

An eBook shows advantages of video surveillance in the Hospitality Industry

Informative guide shows how comprehensive video technology can overcome a range of challenges in the hospitality industry and have a positive impact on the bottom line The September eBook from IDIS, a Korean video manufacturer, highlights why it is crucial for hoteliers and restaurateurs to take advantage of next-generation video technology to improve operational flexibility during turbulent times.

The company's latest eBook has been written to support security planners and help their systems integrators understand how to address a range of challenges with the latest video tools - including strengthening security, increasing guest safety, and improving operational efficiency: meeting the needs of Europe's hospitality industry with cutting-edge video technology.

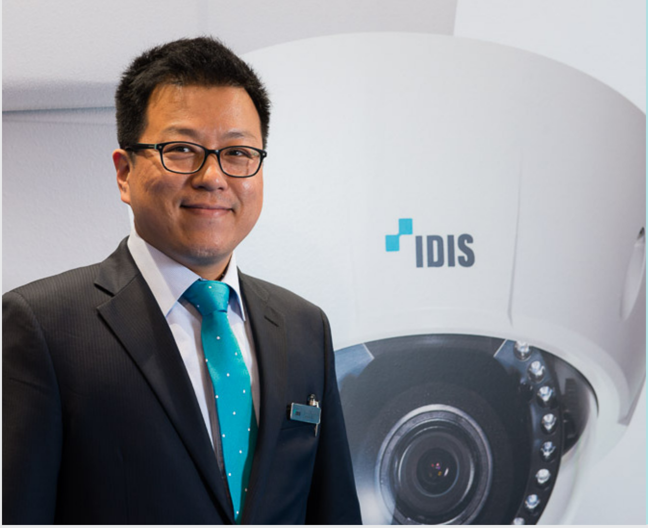
Following the impact of the COVID 19 pandemic, the European hospitality industry is facing continued pressure from rising energy costs, inflation, and the cost-of-living crisis. As a result, hotels need to consider how they can improve their flexibility and resilience and respond to changing customer demands.



Security remains a top priority for guests and is often a deciding factor for VIP and corporate clients when choosing where to stay.

Security failures can quickly lead to direct losses, including the cost of remediation, damage to reputation and loss of future business. For example, theft continues to be a major problem for hoteliers, with not only guests' property being stolen, but also that of the hotel.

Meeting the needs of the European hospitality sector with cutting-edge video tech
IDIS
Meeting the needs of the European hospitality sector with cutting-edge video tech



"IDIS' new eBook highlights how video technology can be used to help the hospitality industry evolve and modernise," says James Min, Managing Director of IDIS Europe (pictured left).

"Our experience in the sector has shown that the latest generation of video solutions can not only enhance the safety of hotel staff and guests and improve the protection of property and assets, but also improve the operational flexibility and resilience of the business."

A survey by Wellness Heaven found that "thefts in luxury hotels are skyrocketing", with mattress theft up 35% and TV theft up 11% in the last three years. Well-designed video systems are one of the most effective tools to combat security risks, especially when integrated with other building management and back-of-house systems. In addition, the latest generation of video solutions offers advantages that also give hotels a competitive edge from a business perspective. For competitive hotels, video is no longer just used to reduce costs and mitigate risk, but also to improve service delivery and efficiency in a way that adds value to the customer experience. AI-powered video analytics, for example, can be used to monitor queues and occupancies to alert managers to redirect staff accordingly, as well as heat mapping historical data to understand peak times and optimise operations to ensure consistent service.

Museum and monument from the 13th century

Video technology at Ujazdowski Castle

Protecting visitors and artworks with Hanwha Techwin AI cameras in the exhibition space at Ujazdowski Castle, Centre for Contemporary Art in Warsaw

The Centre for Contemporary Art based in Ujazdowski Castle is a space that uses art to help visitors reflect on the world. It aims to invite discussion about some of the pieces, where different art disciplines blend together in creative experiments. To achieve this, the space – which is located at the heart of Warsaw, Poland – hosts events, exhibitions, a cinema, a bookshop, a library, and an art residency programme.

State-of-the-art

The Centre for Contemporary Art, Ujazdowski Castle, needed a system that was flexible to the different needs of the many spaces in the museum, and that worked with the castle's 13th-century aesthetic. The team decided to invest in advanced IP cameras to deliver state-of-the-art video and audio analytics to protect people, assets, and artwork with great accuracy. The Wisenet P and X series AI cameras were chosen due to their built-in deep learning analytics, along with the intuitive and easy-to-use Wisenet WAVE video management system (VMS) and WAVE Video Wall (to display critical areas simultaneously).

Depth and breadth

Wisenet P series cameras are used to focus on specific areas such as high-value artwork or entrances and exits. Fisheye X series cameras monitor entire rooms to give operators a comprehensive overview of everything happening in the museum. The P series AI cameras have AI analytics and sound classification, to detect people standing or moving too close to museum exhibits. Deep learning ensures that false alarms are minimized, particularly in rooms with low-level lighting where shadows can trigger a false alarm.

As the system was installed during the Covid-19 pandemic, the P series AI cameras additionally supported with People Counting, Face Mask Detection, and Occupancy Monitoring to ensure public health measures were adhered to.

Integration with audio

The video surveillance system, powered by Wisenet WAVE, integrates with a two-way audio communication system so operators can ask visitors to step back from the exhibits when a close distance is detected.

Proximity alerts are important to the museum's security team as some exhibits are placed in the middle of, or overhanging a space, or within a room that people are encouraged to walk through and experience.

Video analytics also includes line crossing detection and intrusion, which automatically trigger alerts to the control room and also follows automatic rules (locking down an area, for example).

Easy management

"Our operators can manage everything easily through Wisenet WAVE, including alarms so they are not distracted by false alarms being sounded all of the time. There is also the option to search using AI attributes and different parameters and to create rules that automate processes. All of this helps to make our security more intelligent and efficient," explains Rafał Filipowicz, Head of IT and Multimedia Department at Ujazdowski Castle.

WAVE also comes with an intelligent de-warping function that reduces the distortion from the fisheye lens. Operators can more clearly and accurately see what's happening in a room.

Monitoring everything

The WAVE video wall functionality allows the Ujazdowski Castle team to create multiple layouts of the most critical parts of the museum, such as its most valuable exhibits. Operators can proactively monitor what's happening in these high-value spaces. Video analytics running in the background will issue automatic alerts for any events that need further investigation — ensuring that operators don't miss a thing.

Sailing club in Finland trusts in PULSE

A Finnish sailing club saves its members time by securing its premises with cloud-managed, energy-saving locks

Many companies know the problem. Securing scattered locations poses problems for facility managers. Replacing cylinders when a key is lost often involves travel and high costs. All alternative access control systems that rely on electricity can be difficult or impossible to use at remote sites. Battery-less, wireless electronic locks managed remotely via cloud software help overcome these challenges.

The Näsijärvi Sailing Club in Finland has several bases spread across Lake Näsijärvi, some of which are up to 2 hours sailing distance from each other. There were many mechanical "skipper keys" in circulation that allowed club members to unlock and use these facilities. However, the registers of key holders and the whereabouts of many traditional mechanical keys were no longer up to date. This presented a security problem that could not be solved by either mechanical security or traditional access controls. The sailing club was looking for a solution to increase its security while saving effort and costs.

To find a new, more efficient solution, the sailing club was looking for a programmable digital key system that would allow it to regain control over the security of its facilities. It needed wireless locking devices suitable for the club's remote locations and powered by the user key.
To manage it all, software was needed to per form system management tasks from any location: a system that makes it easy to revoke access rights for missing keys, and an audit trail feature that allows security administrators to review access logs when a problem occurs.

More control with programmable smart keys

Näsijärvi Sailing Club chose the key-operated PULSE access control solution from ASSA ABLOY's corporate brand ABLOY to secure its premises and manage access for club members. Around 55 PULSE cylinders have been deployed at various locations across the sailing club. Eligible members now carry an individual key with which they can open all approved PULSE locks around the lake.

Why is PULSE the best solution for clubs with remote locations?

PULSE locks are ideal for an environment like Lake Näsijärvi where access points are scattered. They generate all the power they need for the lock electronics from the keystroke.
This innovative power generation technology means that no cables or batteries are needed, saving the sailing club operating and maintenance costs. The PULSE cylinder range includes door locks, cam locks, furniture locks and curtain locks that can be used in the harshest outdoor climates. Almost any cylinder can be exchanged for a PULSE device and connected without cables or drilling.

Another advantage is that a PULSE system is so easy to manage. The club manages it itself, which also saves on additional administration costs.
Safe facilities can be hours away by boat: PULSE saves unnecessary trips. "The PULSE system makes it possible to update and deactivate keys at any time via readers and the cloud service," says Ari Karjalainen, CEO of Ajan Lukko Lock and a member of Näsijärvi Sailing Club.

Incidents can be easily investigated by looking at the audit trails of keys or locks: "In cases of vandalism, the access register can be used to check who entered the building with which key and when," Karjalainen adds.

Vanderbilt University

Artificial intelligence Eliminates highway congestion

Vanderbilt University researchers succeed in experiments with specially equipped vehicles

Artificial intelligence in networked cars prevents traffic jams on highways that seem to occur for no reason. A team led by Daniel Work from Vanderbilt University (www.vanderbilt.edu) has demonstrated this experimentally. The scientists equipped 100 cars to communicate with each other via radio and exchange traffic information without the driver having to tune in.

Automatic Safety Distance

The cars were also equipped with Adaptive Cruise Control (ACC). This technology allows the driver to set the speed of his car, which is precisely maintained when no obstacle appears. The car then brakes automatically, i.e. keeps a safe distance, and accelerates again when the obstacle has disappeared. For the experiment, the researchers modified ACC so that it reacts to the entire flow of traffic, including what is happening ahead, on the basis of artificial intelligence.

Equipped in this way, the vehicles rolled along a 24-kilometre stretch of Interstate 24 (I-24) between 6am and 9.45am, always going back and forth. The thesis was that phantom traffic jams do not occur when five percent of the cars are equipped with modified ACC and artificial intelligence.

300 sensors for Traffic Control

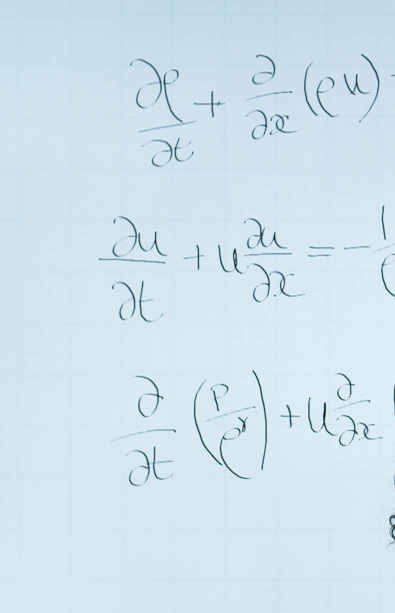
The decision-making of the cars took place on two levels. At the cloud level, information about the traffic situation was used to create an overall speed plan. This plan was given to the cars, which used artificial intelligence algorithms, in real time so they could optimise driving. The researchers determined the impact of the connected cars on the morning traffic flow on a 6.4-kilometre stretch of I-24 equipped with 300 sensors.Because the cars could see far ahead, so to speak, they adjusted their speed to get through without braking if possible. In this way, they smoothed the flow of traffic and prevented speeding as well as sudden braking, which causes traffic jams in heavy traffic. Those driving behind the brakeman have to brake more sharply than those in front because of the reaction time. This continues to the rear, so that at some point it comes to a standstill.

National Institute of Standards and Technology

Internet router to monitor breathing in future

Distortion of signals is a warning signal according to the National Institute of Standards and Technology

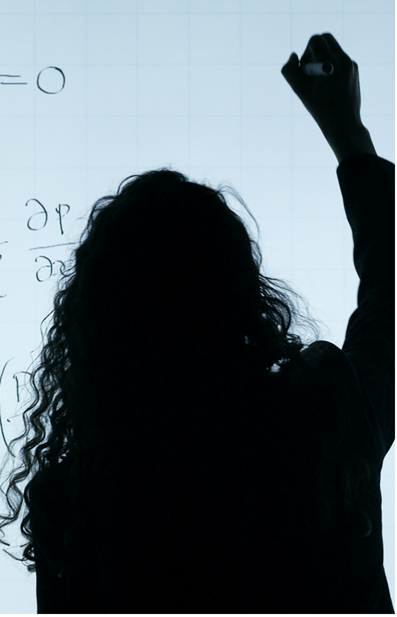
The signals emitted by internet routers can not only be used to connect tablets and smartphones to the network. With the help of the wireless access point, the breathing rate of a person in the room can also be measured - namely when the wireless ad-


$\frac{\partial \rho}{\partial t} + \frac{\partial}{\partial x}(\rho u)$
$\frac{\partial u}{\partial t} + u\frac{\partial u}{\partial x} = -$
$\frac{\partial}{\partial t}\left(\frac{p}{\rho^{\gamma}}\right) + u\frac{\partial}{\partial x}$

apter built into mobile end devices connects to a local area network (LAN) or another wired data network. According to experts at the National Institute of Standards and Technology (www.nist.gov) (NIST), the router thus becomes an early warning device for respiratory disorders that pose a health risk.

Electromagnetic waves

The electromagnetic waves that routers emit bounce off some obstacles or penetrate matter, including human bodies. When they move, such as when they breathe, they are additionally altered. These interactions do not interrupt the internet connection, but they can signal that someone is in trouble, at least with the NIST researchers' new system. In 2020, NIST



scientists wanted to help doctors fight the COVID-19 pandemic. Patients were isolated and ventilators were in short supply. Previous research had explored the use of Wi-Fi signals to detect people or movement, with only moderate success.

The researchers led by Jason Coder used channel state information (CSI), the signal that laptops, smartphones and other terminals emit. It's always the same, and the access point receiving the CSI signals knows what it's supposed to look like. But as the CSI signals travel through the environment, they become distorted. The access point analyses the extent of the distortion to adjust and optimise the connection. The team modified the firmware on the router to interrogate these signals up to ten times per second to get a detailed picture of how the signal is changing.

Hit rate 99.54 percent

To train the system, the KIST scientists used a mannequin that had been developed for training purposes. It simulates all conceivable types of breathing, from normal breathing to abnormally slow and abnormally fast breathing, as well as asthma and lung disease. In all these cases, the body moves in a very specific way. The doll's breathing movements change the path of the CSI signal. With Deep Learning, the engineers finally succeeded in achieving a hit rate for respiratory diseases of 99.54 percent.

Georgia Institute of Technology

New printer ink is transparent and conductive

Georgia Tech's process can be used to produce flexible conductive tracks and also films

Researchers at the Georgia Institute of Technology (www.gatech.edu) (Georgia Tech) have developed a new printer ink that can be used to make flexible conductive traces and films that are also transparent. The scientists started with the popular polymer PEDOT (poly-3,4-ethylenedioxythiophene), which meets the requirements for conductivity and transparency but is insoluble. This makes it unsuitable for the production of a printer's ink.

Side chains for solubility

James Ponder, himself a chemist, and a team of chemists and engineers then had a bright idea. They attached others to the PEDOT molecules, forming so-called side chains. Now the newly formed molecules were soluble, but printed conductors or films were not particularly conductive with them, because the side chains are made of a kind of wax that belongs to the insulators.

"We want the side chains for processing, but we don't want them in our final product. So we add side chains that once we're done printing, we can sort of wash them off," Ponder says. So the team members created the polymer with side chains, print or spray it on, chemically cleave the side chains and wash them away with common industrial solvents. A final conversion step creates a flexible, highly conductive, stable film.

Ideally suited for bioelectronics

There are already companies interested in licensing the technology because the films have some important advantages. One of the most widely used transparent conductors for flat panel displays, photovoltaics, smart windows and other applications is indium tin oxide. However, the material has some drawbacks, says John Reynolds, Ponder's PhD supervisor.

"It's quite difficult to make curved and flexible devices with this material because it's brittle." The PEDOT variant, on the other hand, is flexible and ideally suited for electronic devices that are attached directly to the skin or even implanted, among other things, he says. "This is where the new material will shine, in bioelectronics," Reynolds believes.