VIDEO® EXTRA

Foresight is better than hindsight

Effective cybersecurity helps protect video security technology from misuse

Page 3

The white hackers

How cybersecurity experts put video solutions to the test

Page 3

No more ugly duckling

How video security becomes a strategic IT component

Page 7

Is your camera phoning home?

The losses due to cyberattacks in 2017 and 2018 have been estimated to be around 43 billion euros. For example, the Siemens group alone is attacked 1000 times every day*! And yet the significance of video security systems as potential weakpoints is underestimated by many. This is much to the satisfaction of the attackers, as evidenced by the infamous attacks in recent years targeting IP-based cameras such as Carbanak, Mirai or Persirai. But video management systems and processors (CPUs) also come under fire.

** Source: Wirtschaftswoche*

Page 2

Manufacturer Security

Trusted advisor or risk factor?

In matters as sensitive as security technology, there is more at stake than the technical solution. Customers want to know "who they are dealing with". Some indicators may yield critical information about the trustworthiness of a manufacturer.

Page 8

Security in planning

Nine stadiums secured in record time

Companies from all over the world and in all industries trust the video security technology from Dallmeier. Often their decision is made on the basis of a consideration which has nothing to do with the equipment technology: they value the special approach of Dallmeier in project planning and implementation.

Page 6

Is your camera "phoning home"?

VIDEO TECHNOLOGY IS OFTEN THE STEPCHILD OF CYBERSECURITY

Security specialists at many banks in several different countries were undoubtedly blindsided in 2013 when Russian hacker groups "purloined" a sum of more than a hundred million euros in the course of the "Carbanak" campaign: In these attacks, surveillance cameras inside the financial institutions were compromised, allowing the perpetrators to secretly view screen contents and keyboard entries to identify employees as primary phishing targets from their name tags, and to learn about the employees habits and reactions, among other things.

Then in 2016 and 2017, two further attacks called "Mirai" and "Persirai" gained unwelcomed notoriety. These were designed to paralyse central IT services through large-scale Distributed Denial of Service (DDoS) attacks. Mirai and Persirai are botnets which consist entirely of IP cameras. In the case of Persirai, over 1000 different camera models were impacted.

With its device search engine Shodan, security manufacturer Trend Micro found about 120,000 IP cameras worldwide which could theoretically be incorporated in the Persirai botnet. According to Trend Micro, many of the users affected are probably entirely unaware that their cameras are even vulnerable to attack via the internet.

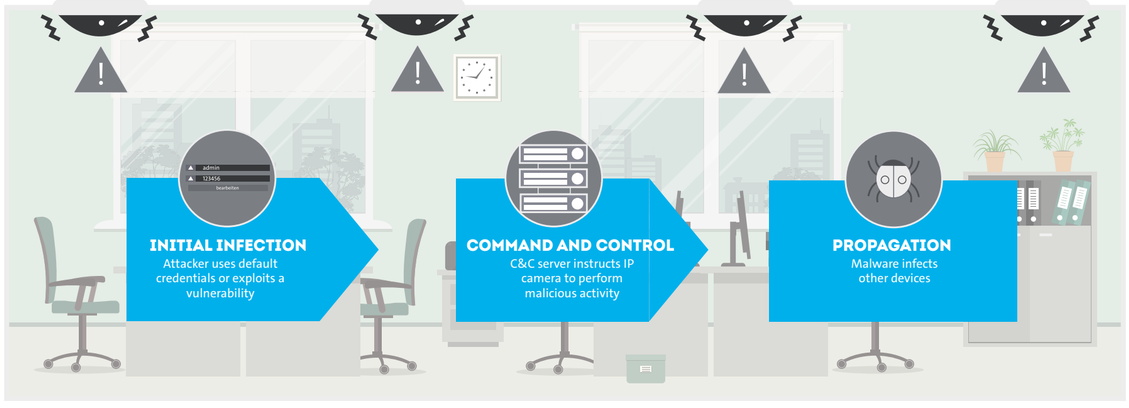
Attackers are thrilled to find an open back door

It must be said, an IP camera is not just a camera, it is a fully networked "IoT" device and comes with all the capabilities and risks associated with this complex technology. In theory, the "embedded systems" that are installed on it are open to attack like any other network system: Many are preset at the factory to connect to external servers automatically, to enable updates, for telemaintenance or for storing data in the "cloud" for example. These connections bypass the firewall; as a rule, the user has no control over the data that is transmitted via these connections. In some devices, backdoors have been found, created either inadvertently or deliberately. Some devices are also manipulated in a specific manner by intelligence services, industrial spies or organised crime. These compromised systems pose a significant security risk for the entire network and company concerned.

Top 10 attacked ports for IoT honeypot - Q4/17

No.	Port	Percent
1	23/tcp (Telnet)	43,1
2	80/tcp (HTTP)	31,6
3	443/tcp (HTTPS)	7,7
4	2323/tcp (Telnet)	7,2
5	445/tcp (SMB)	5,8
6	22/tcp (SSH)	1,9
7	1900/udp (UPnP)	0,9
8	8080/tcp (HTTP)	0,8
9	2222/tcp (SSH)	0,2
10	21/tcp (FTP)	0,2

Source: Symantec Internet Security Threat Report 2018



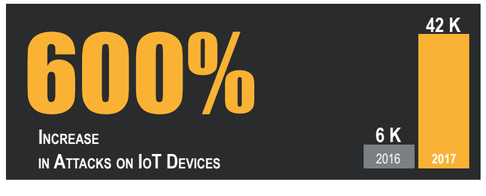
The attacker uses default access information or a vulnerability to take control of an IP camera

Source: Representation based on Trend Micro

Attacks on IoT devices increased by 600% between 2016 and 2017

IP cameras and digital video recorders (DVRs) are among the most frequently attacked IoT devices. But video management systems are also found to have security vulnerabilities with alarming regularity. And even the processors installed in the systems are generally exposed to attacks, most notably observed in the recent processor security vulnerabilities "Spectre" and "Meltdown".

At the moment, there are no signs of the threat abating: According to the "Internet Security Threat Report 2018" published by Symantec, the number of attacks on IoT devices has risen by over 600% just between the years 2016 and 2017. What is interesting is that manufacturers have only reported a "only" 13% increase in vulnerabilities reported by the manufacturers.



Top device type performing attacks against IoT honeypot

No.	Device Type	Percent
1	Router	33,6
2	DVR	23,2
3	Network	9,3
4	Satellite Dish	7,3
5	DSL / Cable Modem	7
6	SOHO Router	4,7
7	NAS	3,6
8	Camera	3,5
9	PLC	3,4
10	Alarm System	1,9

Source: Symantec Internet Security Threat Report 2018

Videotechnology & Cybersecurity

Better safe than sorry!

The threat level for IoT systems – and this includes video cameras – is something to be taken very seriously. But there are a few important principles customers can apply to protect their systems effectively from cyber threats.

The right approach

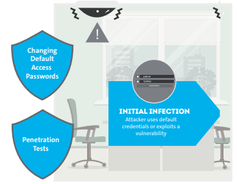
From the beginning, when planning the basic elements of video security systems, companies can implement a range of different approaches to address potential cyber threats proactively: From the complete physical separation of the corporate network and the video system, to VLAN and VPN, and finally even to a "Video Security Gateway". This last functions as a secure switching centre and monitors all connections between the corporate network and the video network.

The engineers and network planners at the German security provider Dallmeier are working meticulously in this area: Together with the customer, they draft a solution which is not only secure, but can also be integrated in seamlessly in the customer's existing network environment.

Security by Design

When choosing security systems, customers should also be guided by the criterion "Security by Design". This means that these solutions are already equipped with data security functions. In this context, a world of trouble can be headed off straight away if companies change the access information assigned as default, use strong passwords and the manufacturer implements comprehensive precautionary measures. At Dallmeier, thorough, systematic testing of its own products is an integral part of the development work. As part of this process, the company regularly hires external, reputable IT security testing organisations to simulate hacker attacks in the form of penetration tests (see below: Interview "The white hackers of cirosec").

In this way, the likelihood of a typical attack on an IP camera as described above can be reduced enormously:

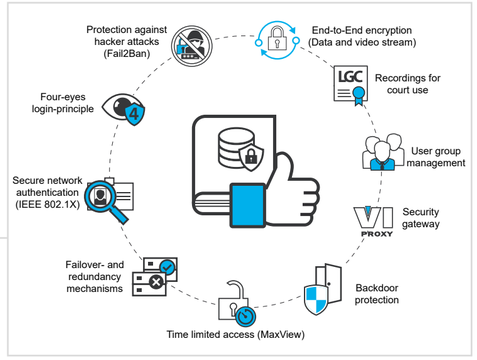


Simple but efficient: Change access identification and replace with secure passwords, and ensure that the manufacture has also carried out the development work carefully

It is also advisable to deactivate all of the ports in a video system that are not needed. In Dallmeier products, Telnet (the most frequently targeted port!) and other non-secure connections are deactivated by default. In addition, the company offers its own combined data protection and data security module, an extensive cyber security package which was developed in keeping with the guiding principle "Security by Design":

For safeguarding the network, current Dallmeier systems use authentication compliant with IEEE 802.1X, an end-to-end TLS 1.2 / 256 bit advanced encryption system (AES), and the "ViProxy" function, with which Dallmeier recording appliances act as the security gateway to the video system. Furthermore, all hardware, software and firmware solutions are developed and reviewed in-house, so hidden access capabilities through backdoors are precluded.

On the recording level, data security is assured with the optional "four eyes login principle" for viewing recordings, specification of time limited access for each user group with "MaxView", and user group administration with hierarchical structures. Reliable detection and prevention of connection attempts in hacker attacks is the province of the "Fail2Ban" function, corresponding failover and redundancy mechanisms during recording protect against loss of data. Finally, with the LGC certification Dallmeier ensures that all criteria for preservation of evidence are met, so material is admissible in court.



The data security functions of the Dallmeier data protection and data security module

Understanding cybersecurity as a process

But it is not only the technical functions that minimise vulnerabilities and protect from cyber attacks. Cybersecurity is a continuous process. In practical terms, this means: security updates for video systems should be installed regularly, and security principles implemented consistently throughout the organisation. It is also important to document all security measures thoroughly, for example using checklists and guidelines such as Hardening Guides, the purpose of which is to harden systems.

Employees and managers should refresh their knowledge with regular training courses. Because video technology can only really be secure and fulfil its purpose if everyone involved and concerned works towards the same goal and applies the technological and organisational measures with understanding: To preserve the long-term competitiveness and existence of a company and protect its employees.

The "white hackers" of cirosec

These days, almost all IoT, IT and video systems have security implications. So, it is all the more important for manufacturers to engage independent external experts to subject their system to the most rigorous testing while the systems are still in development. The foremost company for this task in the German-speaking area is Heilbronn-based cirosec. The company founder and managing director Stefan Strobel answered questions for Video Extra in an interview.

MR STROBEL, WHAT THREATS DO YOU THINK ARE THE MOST DANGEROUS WITH REGARD TO VIDEO TECHNOLOGY?

Like all modern networked devices, today's video technology systems are complicated computer systems which have an operating system, many communication interfaces and a large number of functions. Therefore, they are targets for hackers trying to take control of the systems, so that they can command them at will or even load their own software onto the systems. In this way, a surveillance camera which is intended to protect the company can become a backdoor for criminals. Through it, the hackers gain access to the company network, from where they may then succeed in stealing company secrets.

WHY IS THE TOPIC OF SECURITY SO IMPORTANT EVEN AS EARLY AS PRODUCT DEVELOPMENT?

Often it is not possible to completely eliminate security problems that only become known after product development has been completed, because the security of an IoT product has its origins even in the secure design of the hardware. The application programs cannot be added until the essential security functions have been built into the hardware. But many vulnerabilities in IoT systems arise due to programming errors during development. To avoid this, the developers have to understand how an attacker operates so that they can program with this in mind.

WHAT SERVICES DOES CIROSEC OFFER, AND WHAT DOES THIS MEAN FOR THE END USER?

We advise and support our customers in almost all aspects of information security. Our main activity is the testing of systems, called "penetration tests". This is when our specialists attempt to attack the IT systems or products of our customers using the techniques and tools of hackers. In this way, vulnerabilities are discovered before a criminal can find them and cause real damage.

ARE THERE REGULATIONS OR CERTIFICATES, ACCORDING TO WHICH INDEPENDENT PENETRATION AND OTHER SECURITY TESTS ARE CARRIED OUT?

Unfortunately, the official looking certificates you see sometimes on websites or products are more marketing than real confirmations of security. True standards, which are also recognised internationally, usually apply only to the processes in an organisation. So, it is most important to know who is doing the testing and how much experience they can bring to bear.

THE PENETRATIONS AND SECURITY TESTS ARE COMMISSIONED BY THE MANUFACTURERS – HOW DO YOU SAFEGUARD YOUR OWN INDEPENDENCE?

Our good reputation on the market is very important to us. For this reason, we decline requests to test when we have the impression that the customer does not want us to find anything, or does not allow us sufficient time to conduct an appropriate test.

HAS THERE BEEN AN INCIDENT IN THE FIELD OF VIDEO SECURITY WHICH YOU FOUND PARTICULARLY MEMORABLE?

Probably the best-known incident was undoubtedly concerned surveillance cameras that were being sold by a discounter in the autumn of 2015. Many private individuals bought the cheap cameras at the time and connected them to their private networks or WLANs. The cameras activated themselves on the home internet routers without the knowledge of their owners and were freely accessible on the internet. In February 2016 with the aid of the IoT search engine Shodan, over 10,000 unprotected cameras were found and controlled remotely.

Stefan Strobel,
Founder + Managing Director cirosec

Only a holistic approach offers security!

What customers say about the data protection solution from Dallmeier

das Stadtwerk.Donau-Arena: Peter Lautenschlager, Operations Manager

"We want happy visitors and fans. With the solution from Dallmeier, we have obtained exactly the right degree of data protection while offering the highest level of security. We are very glad to have chosen the right partner in Dallmeier."

Data protection

- Observe principles of "Privacy by Design"
- No data protection without data security
- Functions for conformity with GDPR principles

Page 7

Cybersecurity

- Observe principles of "Security by Design"
- Video technology satisfies IT guidelines
- Understand cybersecurity as a process

Page 2 + 3

What customers say about the cybersecurity solution from Dallmeier

Seven Luck Casino: IT manager, GKL

"The Dallmeier solution is widely respected as one of the most stable casino security systems available, and the technology has lived up to its reputation in our tests as well."

Linz PlusCity shopping centre:
Michael Pechmann, Safety and technical officer

"We deal openly with the topic. The visitors appreciate that and we don't have to hide anything."

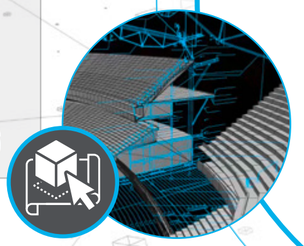
Dallmeier

#SecureVideotechnology

Planning

- Take data protection aspects into account
- Minimise uncertainties during implementation
- "What we plan is what you get" – modern 3D planning

Page 6



IT-friendly video systems

- Small number of systems, low complexity
- Demand investment security
- Integration in central data centre resources

Page 7

What customers say about the Dallmeier planning concept

Linz PlusCity shopping centre: Herbert Zachhuber, G4S

"Dallmeier delivers first-class products. Only a short orientation period is needed, the 3D project planning and pre-installation in the Factory Acceptance Test (FAT) Centre help to shorten both configuration and installation times significantly. All systems are operational quickly, within the planned timeframe, and ensure a smooth workflow immediately."

das Stadtwerk.Donau-Arena: Peter Lautenschlager, Operations Manager

"From the very beginning, we were able to obtain a very precise picture of what we would get later. And in the end, everything from the camera viewing angles to image resolutions over the entire observation area matched what was shown in the 3D model simulation exactly. So, we were very soon able to plan with great confidence, keep a clear idea of costs throughout the process, and were completely satisfied after implementation. What we did find surprising was how much planning and project work could be done even at a very early stage using the 3D technology."

What customers say about Dallmeier as manufacturer

Your Homes Newcastle: Steven Studley, Technical Specialist

"By switching to Dallmeier the police have regained their confidence in the system!"

City of Gaillard: Jean-Paul Bosland, Mayor

"Dallmeier is a company with vision and makes every effort when during the development of its products and solutions to ensure that they can be expanded and upgraded with ease for years to come. This ensures a high degree of investment confidence. We are convinced that Dallmeier technology will meet our needs in future as well."

Trusting manufacturers

- Single-Source Manufacturer
- Experience and roadmap
- "Made in Germany": top quality standards

Page 8

What customers say about the IT-friendly approach from Dallmeier

Studio City Casino: Leroy Daniel, Executive Director MCE Surveillance

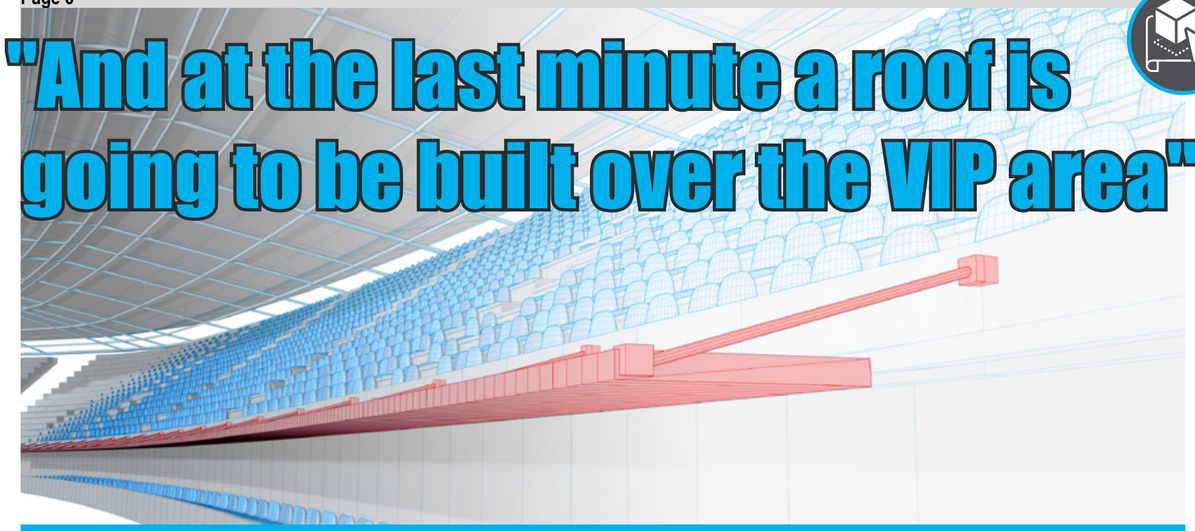
"Some of the key integrations that make Dallmeier unique and enhance our ability to protect the business, is the customized development of high-level interfacing to our core systems around the casino. Interfaces include gaming machines, intelligent gaming shoe, point-of-sale, security access control and intruder detection system and RFID gaming chips."

IKEA: Andrea Tomasekova, Administration Manager / CZ, HU, SK

"The Dallmeier technology has already proven itself in a major expansion. It is a good feeling to know that the video system can also grow with a new modernisation or expansion."

Frankfurt Airport:
Maurice Dengel, divisional management Fraport & Rhein-Main

"The installation was simple and uncomplicated."



"And at the last minute a roof is going to be built over the VIP area"

Video security in record time for nine stadiums

Companies in all industries and located throughout the world rely on video security technology from Dallmeier. Besides the technical advantages, however, it is often something else entirely which makes the difference: the remarkable approach the German manufacturer has adopted for project planning and implementation.

"What we plan is what you get"

The example of the stadium illustrates: An entire team of experts is dedicated to 3D planning at Dallmeier. These experts build precise, three-dimensional simulations of the customer's environment ideally from 2D or 3D plans. Even photographs and "Google Maps" information are sufficient. The complete solution is then simulated exactly in the finished 3D model. Even blocked fields of view for the camera, called "adumbrations", are revealed and eliminated by repositioning the cameras or adding further components. In this way, the customer has an exact plan of the future layout, in which all details have been taken into account.

Specification of 250 pixels per metre

As part of the 3D planning approach, the security objectives are defined precisely with the customer. For example, one feature which is often required in stadiums it that a minimum resolution density of 250 pixels per metre (px/m) or higher is achieved in all areas that are accessible to the public. This parameter is defined in a DIN rule and ensures that unknown individuals can be identified with certainty. And with the 3D simulation it is child's play to ensure that these requirements are achieved literally in every last corner: Colour coding makes it possible to say exactly where the value has been reached, and where the planning needs to be overhauled.

The story of the VIP roofs

The effectiveness of this method was demonstrated for example during a project involving several large stadiums: the project was already well advanced when it was suddenly announced that the upper tiers of the spectators' stands in all stadiums were also to be roofed over. Normally, given the time pressure this would represent a practically impossible challenge for any planner! But not for the Dallmeier 3D project planning team. The required changes in camera models and positioning were implemented in less than two days.

From planning straight to the installation site

A particular bonus of 3D planning is the automatic generation of "CamCards" – precise configuration documents for each individual camera. With this information, the person tasked with building the system on site knows exactly which camera must be mounted where, at what height and at what angle, what IP address it has, and so forth. Besides the enormous time savings, the major advantage lies in the stability of the planning – it can be predicted with a high degree of accuracy how much time and labour it will take to install the total solution.

No experiments: Test of the entire system before shipment

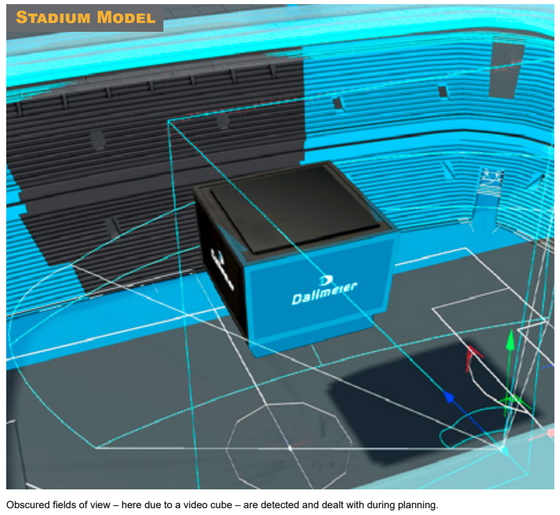
The problem is a familiar one particularly to the decision makers in the IT department: Complex systems have been implemented, and only then does the real integration work start. Of course, this approach is fraught with problems, and not only for stadiums. This is why Dallmeier has chosen a completely different way, with the "Factory Acceptance Test (FAT)": All components of the solution are set up on the Dallmeier FAT Centre, and the final environment is tested in live operation until everything functions flawlessly.

Coverage for large expanses: From the stadium to Cologne cathedral square

An equally important factor in the decision by stadium operators to work with Dallmeier was the company's patented Panomera® technology. Panomera® cameras are equipped with up to eight sensors per system, thus enabling coverage of immense expanses at a precisely defined pixel density and with considerably fewer cameras. This in turn reduces management effort while increasing operating convenience and thus also security. Both are responsible for a significant reduction in total operating costs.

The fact that the systems are not only suitable for use in stadiums is demonstrated by the numerous projects Dallmeier has completed all over the world, including casinos in Macao, very many logistics enterprises, or even in the "Safe City" field, such as the Cologne cathedral square, where a total of eight Panomera® systems have provided security since 2016 and replicate a solution which would otherwise require the deployment of over 100 conventional PTZ cameras.

"What we plan is what you get" – 3D planning and real situation compared



Obscured fields of view – here due to a video cube – are detected and dealt with during planning.

GDPR

The World DID NOT end!

Jürgen Seiler, Managing Director davidiT

Many customers remember all too clearly: The never-ending stream of emails from services, some of which already long forgotten, notifying that they had updated their data protection statement. Or the countless timers or countdown displays giving the impression that the world was going to end on 25 May 2018. That was the exact date when the new General Data Protection Regulation went into force in all member states of the European Union. Like the turn of the millennium, however, it turned out to be a storm in a teacup: feared "tides of notices to desist" did not come to pass, and it is still permitted to be called by your name in doctor's surgeries.

Video security is not mentioned in the GDPR

But there is much that remains as nebulous as before in practical implementation. On the subject of video security, for example, for which the GDPR contains no specific regulations. Instead the general regulations and principles must therefore be applied to video security if personal data is processed with systems to which the regulation is applicable.

Where can customers find help?

A close look at short paper No. 15 from the Data Protection Conference (DSK) will answer many questions about formal changes in accordance with the GDPR. And the Quick Guide "Video security according to GDPR" from Dallmeier outlines the most important GDPR regulations in the context of video security. This handy guide to interpretation also offers specific recommendations and refers to technical functions which can help interested parties to achieve GDPR conformity.

Users who need the detailed information about the technical functions will find it in the brochure "Video security, data protection and data security".

Here you will find all important information on every aspect of video security and GDPR

Thieves, tricksters, shysters:

EYES PEELED WITH GDPR CERTIFICATES!

In general, the EU supports voluntary certification procedures and data privacy seals or data protection certificates as ways to increase transparency and make compliance with the GDPR easier. However, there is no requirement to obtain certification or to use certified products. Furthermore, it is only possible to have processing operations certified. This means that products such as a surveillance camera in principle cannot be certified. Both the certification bodies and the data protection certificates themselves must have been accredited officially in accordance with the GDPR by a national accreditation office or the supervisory authorities. This means that not every data protection certificate necessarily has the desired legal effect and can render possible fines less effective.

From "ugly duckling" to strategic IT component

EVERY CUSTOMER INTEGRATES VIDEO SECURITY DIFFERENTLY

IT security and physical security – video, fire, access control and intrusion alarm systems – continue to draw closer together. At the same time, more and more often the most important decision makers in matters relating to video security technology are the IT managers. Oliver Koch, CIO at Dallmeier, explains this occasionally rocky road in an interview.

MR KOCH, THE RESPONSIBILITY FOR VIDEO SECURITY IS DEVOLVING MORE AND MORE OFTEN TO THE IT DEPARTMENTS. HOW DO YOU SEE THIS CHANGE AS AN IT MANAGER?

The most significant driver behind this paradigm shift, as it is being experienced by many companies, was of course the changeover from analogue technology to IP-based systems. This was what made it possible to incorporate it in the IT structure. As is often the case, it is not easy to make generalisations: Every company is different, and we are seeing very different strategies.

WHAT APPROACHES DO YOU OBSERVE?

For some customers, specifically larger corporations, the highest priority is centralisation and consolidation. Other companies still strive to keep video security and IT completely separate, because integrating them in central data centre systems brings disadvantages as well as benefits. This is the case for instance when maintenance work on central server or storage systems affect the availability of video systems and coordination between the IT and security departments is less than optimal.

WHAT DEMANDS ARE MADE BY CUSTOMERS WHO EXPECT THE MOST COMPLETE INTEGRATION POSSIBLE IN CENTRAL, STANDARDISED IT SYSTEMS?

The solutions offered by a manufacturer must be as adaptable as possible to the requirements. For customers who are pursuing a very "IT oriented approach", this means that it must be possible to integrate the recording and management systems in virtual server environments seamlessly, for example under VMware. Integration in AD structures, support for all common monitoring systems (such as Nagios, PTRG, Solarwinds etc.) with SNMP or integration in the ERP systems for Business Intelligence tasks are also important. These customers are also enquiring to an increasing degree about integration in cloud services (such as Azure or AWS).

OTHER CUSTOMERS ARE LOOKING SPECIFICALLY FOR "STAND-ALONE" SOLUTIONS WITH A HIGH DEGREE OF MANUFACTURER UNIFORMITY. WHAT IS MEANT BY THAT?

For many of our customers "autonomous operation" of their video security systems is more important than being able to use centralised resources. They quite specifically want stand-alone systems, with dedicated recording hardware, for example. One argument they offer is often data protection and data security. In this regard, customers expect solutions "from a single provider" to allow the individual systems to be coordinated with each other more effectively, and so provide a greater degree of security. This approach is quite often also the less expensive option – contrary to popular opinion. What is important for us as a manufacturer is that we can cater to both requirement profiles equally effective.

WHAT OTHER TRENDS DO YOU SEE AS IMPORTANT FOR THE FUTURE?

Customers are also expecting more flexibility in terms of the nature of the acquisition. Here we are talking more and more often with IT, IT-, security- and purchasing-managers who are interested in subscription or even "as-a-service" models or hybrid purchasing variants. The advantages are quite clearly greater flexibility and a different cost structure – operational expenses instead of capital expenses.

Oliver Koch, CIO Dallmeier

Another trend is the growing perception of video technology as a component of the IT-infrastructure which can do far more than video surveillance. Just think about the capture of video data for process optimisation or for improving marketing activities.

We are just now also receiving very positive feedback from IT departments regarding our planning approach: The combination of 2D and 3D planning with our "Factory Acceptance Test" provides the customer with a "plug and play" approach with extremely reliable planning and almost 100% percent calculability of the implementation. Something completely new to many IT managers.

Security + Manufacturer Trust

HOW A MANUFACTURER BECOMES A "TRUSTED ADVISOR"

Precisely in matters as sensitive as security technology, there is more at stake than the technical solution. Customers want to know "who they are dealing with". Some indicators may yield critical information about the trustworthiness of a manufacturer.

The manufacturer's financial situation
A takeover of the technology provider does not necessarily have to have negative consequences. But of course, it raises concerns, for example whether development of the solution portfolio will continue, or whether the quality of customer service will remain the same. Financially independent companies can offer advantages in this regard.

Political background conditions
In August 2018, the US House of Representatives and Senate passed a law prohibiting public authorities from purchasing and using systems from two major Asian manufacturers. For customers, this has entailed substantial additional expense and effort to purchase and implement new equipment. When choosing a provider, customers should examine each candidate very carefully, precisely with consideration for industrial espionage and political pressure, and considering the country of origin and the country's political structure.

"Single Source of Trust"
The term "manufacturer uniformity" expresses the approach many customers adopt, according to which they obtain as many components as possible from a single manufacturer. Development within the same company often makes it possible to integrate the elements subsequently with due consideration for security questions. The opposite approach is called "Best of Breed". In this case, customers expect to get the best individual solution available on the market for each application. There are cogent arguments for both approaches.

Experience and durability
Many customers are of the opinion that a trusting partnership must also be based on the experience a manufacturer contributes, its awareness of quality, and also the commitment with which it pursues its objectives for the future. Indicators of such may be the production depth – how much of its own development and production is carried out in-house, but also things like roadmaps and investments for the future.

"Security needs trust. That is why we attach great importance to developing solutions of superior quality which will not only last a long time, but because of their open platforms will also allow the integration of third-party systems and new developments and innovations. Our experience particularly in the last few years has also shown that manufacturer uniformity make a valuable contribution to better overall security. At Dallmeier, we have been living by the fundamental guiding principle of "Security by Design" anchored in the GDPR for already 35 years."

Dieter Dallmeier
Founder & CEO, Dallmeier electronic

"By switching to Dallmeier the police have regained their confidence in the system!"

Steven Studley, Technical Specialist, Your Homes Newcastle

Check your PROVIDER:

7 questions to ask the manufacturer

Make an appointment with one of our experts

Find out more about Dallmeier in a 100 second portrait on YouTube

Here you can find further information about video technology & cybersecurity

HOW NEUTRAL IS SECURITY TESTING?

How important is it to the manufacturer to obtain a neutral evaluation of the degree of security of its systems, for example by independent penetration tests during and after development?

HOW DEEP IS THE VALUE ADDED IN PRODUCTION AND DEVELOPMENT?

Deep integration usually improves the quality of total solutions and consequently the customer benefit as well. What proportion of the portfolio originates in-house? Where is production performed?

DOES THE MANUFACTURER BELIEVE WHOLEHEARTEDLY IN THE IDEA OF THE PLATFORM?

As with all trends towards greater "manufacturer uniformity", given the complexity of modern systems it is very important that they are open, fully support standards such as ONVIF, and allow third-party systems to be integrated easily.

HOW WELL DOES THE MANUFACTURER KNOW THE TECHNOLOGY AND THE INDUSTRY?

There is no substitute for years of experience in video security technology and a profound knowledge of the industry. The manufacturer should be able to demonstrate these qualities.

DOES THE MANUFACTURER OFFER COMPLETE SOLUTIONS OR MODULES?

Particularly with regard to security considerations, the "everything from a single supplier" approach has advantages because the individual elements are perfectly tune to each other.

IS THERE ANY DOCUMENTATION OF THE MEASURES AND FUNCTIONS FOR DATA SECURITY AND DATA PROTECTION?

The GDPR threatens severe consequences if its principles are ignored. A manufacturer should document credibly and comprehensibly how the complex, interrelated issues of data protection and data security are addressed.

WHO AM I DEALING WITH?

When choosing a manufacturer, aspects such as possible political influence in the country of origin or financial dependence on shareholder interests must also be considered.

MASTHEAD

Editor: Dallmeier electronic GmbH & Co.KG, Bahnhofstr. 16, 93047 Regensburg, info@dallmeier.com, www.dallmeier.com
Contact Person: Press department Dallmeier, presse@dallmeier.com
Picture Credits: Shutterstock, Fotolia. For all other images copyright is with Dallmeier electronic GmbH & Co.KG
Layout and Editorial: Dallmeier electronic GmbH & Co.KG
Overall Responsibility: Georg Martin M.A., CCO, Dallmeier group of companies

Further information

Made in Germany