Dallmeier

CYBERSECURITY FOR VIDEO SECURITY SYSTEMS

BEST PRACTICE GUIDE




MADE IN GERMANY

See more.

CYBERSECURITY CONCERNS VIDEO EQUIPMENT TOO

Who should read this document?

This best practice guide is intended primarily to help:

- Video security system integrators
- Network administrators
- IT security officers
- Executive managers
- Decisionmakers

Cybersecurity as one of the biggest challenges

Like all modern networked devices, today's video security systems are complicated computer systems. Accordingly, hackers can try to take control of these systems, for example. But the users themselves may also jeopardise the security of the entire network and the company by their actions. Consequently, in recent times data security and cybersecurity are now among the biggest challenges that have to be addressed when planning, installing and upgrading digital network infrastructures for modern video security systems.

Dallmeier implements „Security by Design“

This is why Video-IP products from Dallmeier are developed with special emphasis on the „cybersecurity“ factor. The security of digital information as it is being processed is a top priority for Dallmeier. Each product, whether hardware or software, is subjected to a process of continuous improvement, to ensure that it always conforms to the latest technological security standards. For this purpose, Dallmeier network products regularly undergo internal and external penetration tests. This enables Dallmeier to respond quickly to current cyber-threats and ensure optimum protection against the newest attack scenarios.

Understanding cybersecurity as a process

But a video security system cannot provide effective, successful defence against cyber-attacks unless a consistent network security concept is in place and applied to all of the devices, components and applications in use on the network.

USEFUL DOCUMENTS AND INFORMATION

The Best practice guide as helpful reference

This best practice guide gives general notes about the most important security measures for video security systems and proven practices for the effective protection of digital network infrastructures. It can be helpful in identifying critical vulnerabilities in the network, to protect it effectively against targeted attacks from within or from the outside.

Dallmeier product documentation

This best practice guide only provides a general description of the more important measures for safeguarding digital network infrastructures. More detailed information and descriptions of Dallmeier products can be found in the documentation for the respective product at www.dallmeier.com.

Third-party manufacturer product information

Current documentation for products supplied by third-party manufacturers, such as routers, switches, firewalls, anti-virus protection programs etc. can normally be found on the internet on the corresponding product pages of the manufacturer concerned.

Further recommendations and guidelines

You can also learn about the most recent legal regulations, guidelines and recommendations in your country by consulting the respective officially recognised agencies. In Germany for example, visit the Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security] (BSI) at https://www.bsi.bund.de/EN/.

Contents

BEST PRACTICE AT A GLANCE

This chapter gives a preliminary overview of the subject of cybersecurity. Based on the three most critical IT security objectives Confidentiality, Integrity and Availability, the significance of each in video security systems is explained. The chapter is completed with notes on the functions of the Dallmeier data protection and data security module and first best practice recommendations.

BEST PRACTICE AT A GLANCE

More detailed information about the functions of the Dallmeier data protection and data security module is provided in the brochure entitled „Video security, data protection and data security“. More on Page 19.

This chapter describes the most important technical measures and strategies for safeguarding digital network infrastructures. A range of solution approaches and security functions that have been implemented in Dallmeier devices and applications will also be presented.

Network segmentation

A network-based video security system should always be operated in a separate network. In this way, this initially prevents the unintended flow of data between the components of the video system and the workstations of other areas of the company. However, the most important point is that the number of possible attack points on the video network is reduced significantly.

Physical separation

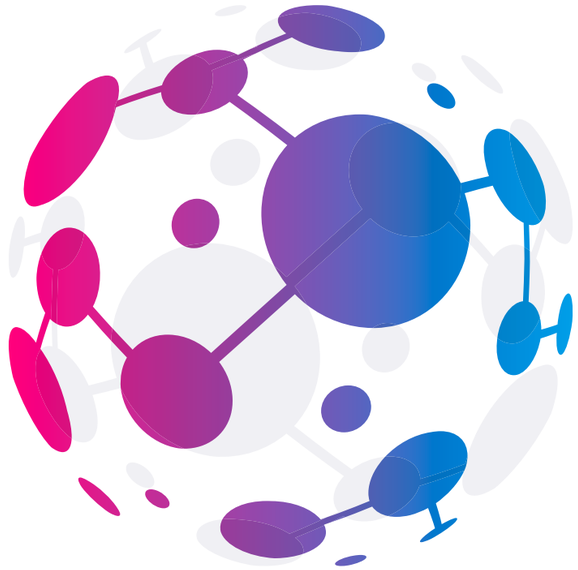
The best way to create separate networks is to ensure that the network segments are physically separate. This means that no shared switches are used and any and all wire connections between the segments are prevented.

VLAN

Since physical network segmentation entails greater cost and more administration, it is recommended to implement a dedicated virtual network LAN (VLAN) for the video network. VLANs allow several logically separate network segments to be defined on a unified physical infrastructure.

ViProxy

If the video security system is operated in a separate network, in some cases it is still desirable to be able to access the live images and recordings from the work network. In such cases, it is recommended to use the ViProxy function, as it is supported by all Dallmeier recording systems.
Among other things, ViProxy allows the first ethernet interface of the recording system to be used for connecting to the video system. The second ethernet interface is used to connect to the work network. In this way, ViProxy serves as a security gateway / proxy server and prevents unauthorised access to the video material.



TECHNICAL MEASURES

Network infrastructure

Managed Switches

In a network-based video security system, only managed switches should be used. With managed switches, network ports that are not being used can be deactivated. This then makes it impossible for unauthorised devices to gain access to the network via a LAN interface which is not being used.

MAC address filtering

Managed switches typically offer MAC address filtering functions. This allows the definition of only one specified list of devices that can be connected to the switch. Other devices connected to the switch are ignored, even if the port was used by a valid device previously.

DHCP server

Dallmeier cameras and recording systems support the Dynamic Host Configuration Protocol (DHCP). This enables the assignment of network settings (IP address, subnet, gateway) via a central DHCP server. If the network settings are configured via a DHCP server and not directly on the device, a static DHCP should always be used. In this mode, the IP addresses are assigned to the corresponding MAC addresses manually on the DHCP server. Then, the assigned IP addresses cannot be used by another device which is connected to the network afterwards.

Time server

The network-based video security system should be equipped with a time server, with which all devices are synchronised by means of a Network Time Protocol (NTP). This ensures that the correct time and date are set on all devices so that log files and event logs can be evaluated.

SNMP monitoring

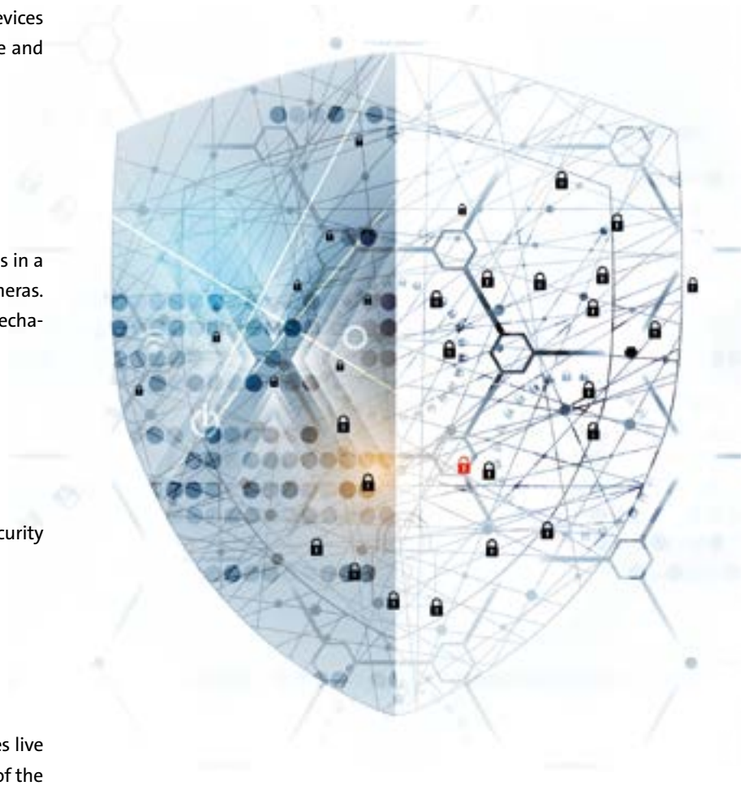
The Simple Network Management Protocol (SNMP) makes it possible to monitor all of the devices in a network from one central workstation. It is supported by all Dallmeier recording systems and cameras. However, it should be noted that versions 1 and 2 of the SNMP protocol offer almost no security mechanisms. Therefore, only SNMP v3 should ever be used to monitor the devices.

Wireless LAN / WiFi

For reasons of security, WLAN connections should be avoided entirely in a network-based video security system. WLAN networks are extremely vulnerable to man-in-the-middle attacks.

Mobile access

For mobile access to video data, Dallmeier offers the DMVC Server software. This not only enables live images to be displayed, but also recordings to be played back on mobile end devices with the aid of the corresponding Dallmeier app. The DMVC app can be purchased for various mobile operating systems in the customary app stores.



TECHNICAL MEASURES

Authentication and encryption

Network authentication

A network-based video security system should be protected in accordance with the IEEE 802.1X standard by the use of secure authentication. This network function uses a certificate system (EAP-TLS) to verify newly connected devices and if the requisite authorisation is missing it disables the network communication. This almost completely precludes the risk of any man-in-the-middle attack.

Encryption

The use of end-to-end encrypted video and data transmission with 256-bit TLS 1.2/AES via DaVids and HTTPs offers the highest possible protection against unauthorised access, including within a network-based video security system. With this technology, the network subscribers such as a camera and a recording system negotiate a secret key for encoding the transmitted data. Since this key is only known to the end devices, unauthorised reading of the video and data transmission by other network subscribers is effectively prevented.

Operating systems of camera and recording systems

Dallmeier camera and recording systems are equipped with a Linux operating system that is strongly adapted hardened with regard to system security. It does not offer any possibility to import or execute an external program.

Services and ports

All services and ports that are not needed throughout the IT system should be deactivated in order to minimise points that are vulnerable to attack. In addition, all services running on servers and client PCs should be checked regularly with the aid of a port scanning program.
On Dallmeier devices, all technologically insecure ports such as those for UPnP, Telnet, SSH or FTP are disabled by default. SSH access to Dallmeier devices is only possible in certain exceptional circumstances, and then only after consulting with Dallmeier Service.

Access control

In order to ensure effective protection from data manipulation, access to devices throughout the entire IT system should not be possible until authentication with a user name and password has been completed successfully. For network-based video security systems, the requirements should be stricter still.

Default passwords

The cameras and recording systems of a video security system are always configured with default passwords by the manufacturer to facilitate initial access. But it is imperative to change these passwords with new, strong passwords immediately upon first activation.

Four eyes login principle

In order to avoid unauthorised access to recordings, Dallmeier recording systems should be safeguarded by the four eyes login principle. In this case, access is only possible with an additional password supplied by a second person.

TECHNICAL MEASURES

Admin account

All devices in a video security system should be provided with a full authorisation Admin account to be used by system administrators with full access rights. Separate user accounts with restricted rights should always be set up for engineers who are tasked with maintaining the devices, for example.

Client software

Besides the cameras and recording systems, the video security system evaluation stations should also be protected by powerful passwords. The client software for evaluating live images and recordings should also be protected by separate passwords for the various user groups.

User groups

The access rights for the various user groups should always be defined according to the requisite data protection level and documented so as to ensure subsequent verification. This can be done directly on or in the cameras, recording systems and client software, or optionally with centralised user administration with the aid of an active directory (AD) service using LDAP.

Remote configuration

Dallmeier offers the PService software for easy, centralised commissioning and administration of a video security system. For reasons of security, the option for remote configuration of the IP address via PService should always be deactivated after the individual devices in the system have been commissioned and configured.

Internet connection

Demilitarised zone (DMZ)

In order to minimise exposure to security threats from outside, computers and servers holding sensitive data should not be accessible directly via the internet. Of course, this also applies for cameras, recording systems and video management applications.
Regardless of the above, if it is necessary to allow access from outside, a „demilitarised zone (DMZ)“ should be set up. A DMZ is a special area in the network by which the internal network (LAN) is isolated from the internet (WAN) with the aid of a firewall. For highest security, a DMZ should be created with two firewalls from two different manufacturers, in case a vulnerability in the firewall from one manufacturer is susceptible to exploitation.

Firewalls

For smaller networks, setting up a demilitarised zone (DMZ) may involve disproportionately high investment in time and labour. At the very least, special firewall computers should be set up and configured with restrictive firewall rules as protection against attempts to break into the local network. The use of firewalls is also advisable for companies in order to separate areas with different levels of sensitivity from each other.

Internet PC

In order to avoid the extra costs and administrative effort associated with a DMZ, small companies can implement a standalone PC which is not connected to the internal network for internet searches. Files that are downloaded can then be scanned for harmful code locally first and optionally transferred to the internal network by downloading to a data carrier.

Virtual Private Network (VPN)

Telecommuters who need a connection to the company network should access the internal network via a Virtual Private Network (VPN). In this case, the VPN protocol should be reinforced with encryption that allows interception- and manipulation-proof communication to comply with the most stringent transmission security requirements.

TECHNICAL MEASURES

Patch management

All network components (firewalls, routers, switches etc.) throughout the IT system should be based on the latest software version at all times, particularly in terms of security patches. It is also essential to check the security patches for the operating systems on servers and client PCs regularly, and update them appropriately if necessary.

Dallmeier offers software updates for all cameras and recording systems on the Dallmeier website. Each update is accompanied by a technical report which provides information about all security-related aspects and innovations.

Updates from Dallmeier are always protected against alterations by third parties. If just a single bit in the update file is modified, it is no longer accepted as valid and the update process is not initiated.

All updates should first be tested thoroughly for compatibility and flawless functioning in a test environment to avoid jeopardising the ongoing operation of the IT system. Loading of updates should also be planned and documented meticulously.

This chapter describes general preventative measures applicable for all aspects of cybersecurity and makes further recommendations intended to help you raise the level of security for your company's data and IT systems.

Basic principles

Introduce a company-wide security concept

Introduce a security concept that is consistent and applicable throughout the company. Use precisely defined checklists to test the directives defined therein and ensure that they are implemented.

Document security measures

Document the security measures that are introduced thoroughly and clearly. This will ensure that security-related tasks can still be completed effectively if the responsible system administrator or IT security expert should be unavailable.

Organise training and advanced training courses

Organise regular training and advanced training courses for members of the technical and management teams and for other employees to maintain awareness of IT security and data protection, and to ensure the best possible preparation for current cyber threats.

Conduct penetration tests

Make sure that penetration tests are run regularly both by in-house staff and external parties so that potential vulnerabilities in your IT systems can be identified and eliminated as early as possible.

Prohibit employees from using their own data carriers

To prevent data theft, prohibit employees from using their own data carriers.

GENERAL MEASURES

Access rights

Deactivate unnecessary user accounts

Check whether any user accounts were set up during installation of the operating systems, such as a guest account or auxiliary account to enable remote support. Accounts that are not needed should be deactivated to increase your systems' security.

Prohibit employees from loading untested third-party software without approval

To minimise the risks of attacks on your IT systems by computer viruses or ransomware, ensure that employees do not install software from external sources on client PCs.

Check system logs

Check the event logs for your applications, network components and video security systems regularly: This way you can detect security-relevant events such as unauthorised access attempts quickly.

Restrict administrative access rights

Limit the number of system administrators who have full access rights to your IT systems. Only assign trustworthy, incorruptible individuals to positions and areas with security implications.

Store passwords for staff who are approved to deputise for system administrators in secure location

Authorised individuals must be identified by name in advance of any absence of a system administrator with full privileges, so that they can have temporary full access to the corresponding IT systems. In this case, it is absolutely imperative to document and store the passwords for these deputies in a secure location (e.g., in a sealed envelope in a safe). Every time these stored passwords are accessed (for eyes login principle is recommended) must be documented.

Physical protection

Mount cameras and network devices in places that are difficult to reach

To prevent hardware manipulation, or even destruction of the devices, mount cameras and other network components such as routers in places that cannot be reached easily. In any case, recording systems should be set up in server rooms that are protected against unauthorised entry.

Install entry control systems

Install systems to control entry to network rooms and other security-related areas, so that only authorised individuals are granted physical access to sensitive data and systems.

Data and system restoration

Carry out data backups

Carry out data backups regularly and store the backups in a separate, secure location. Backups should be carried out at regular intervals in order to provide effect protection against loss of data. The backups should also be subjected to random checks for correctness and restorability.

Create system images

Create system images regularly to ensure that your IT systems can be restored quickly in the event that they do become infected with malware or possibly damaged hard disks.

Topic website “Cybersecurity”

Visit our web page dedicated to the subject of video security and cybersecurity. There you will find additional helpful information collected conveniently in one place:

Legal notice

The content of this document is published for informational purposes only. It is not to be interpreted as comprehensive advice regarding protection against cyber threats. Dallmeier does not guarantee that its products are immune to potential cyber attacks. Moreover, your video security system and/or network may still be exposed to a threat of cyber attack after you implement the content of this document.

Dallmeier

Dedicated to quality. Driven by passion.

Dallmeier electronic GmbH & Co.KG
Bahnhofstr. 16
93047 Regensburg
Germany

Tel: +49 (0)941 8700-0
Fax: +49 (0)941 8700-180
info@dallmeier.com
www.dallmeier.com

MADE IN GERMANY

See more.