BUSINESS INSIGHT

Delivering CCTV in a Cyberinsecure World – Requirements in Delivery, Management and NIS2

NIS2 should be a concept in all system deliveries today. The directive, which comes into force October 2024, will affect large parts of the security industry – not least CCTV and VMS systems. Whether its a network-based CCTV system in a larger industrial production environment, a financial institution or a public infrastructure system. Important security sites have always required complex trade-offs between functionality, resilience, user-friendliness, personal privacy and system security. In recent years, the increase in cybercrime has increased the requirements for intrusion security, system security and product security, while requirements for user-friendliness and functionality have not decreased. Chess in three dimensions has become chess in four dimensions, at least.

Risks Within a Common CCTV System

A common CCTV system in a larger industry is often connected to many IP cameras on a joint or separate network connected to a server stack. The servers can have dual network cards where one is connected to the camera network and the other is connected to the industrial control network. In the control network, the operators can see and control the cameras and control the production. Often they use Ms Office applications, as well as e-mail and surf the web via the company's proxy servers. What are the risks in a system just like this?

Let’s start by having a look at the cameras and their manufacturers. There are reports about cameras with software containing malicious code. The cameras network connections are ports into the network. Access to switches or firewalls physically or via configuration interfaces. Access to servers or client computers, physically or digitally. Old or poorly updated operating systems. Parasites in the form of malicious or vulnerable code in VMS software. Lack of update routines. Lack of security awareness among users. Low or no login requirements. Open USB ports. The list goes on.

Top Management Have the Ultimate Responsibility

Primarily, the local industry's management team is liable for any breaches in cybersecurity, a responsibility that is further tightened in NIS2, where personal criminal liability for management personnel and hefty fines for the principal are included in the list of sanctions. It’s not hard to see that an industrial management group cannot have detailed control over all these risks – but they will have the ultimate responsibility. This is solved with a cybersecurity policy that sets basic requirements and describes routines and methods for planning, purchasing and managing the system.

This responsibility at the top of the pyramid also means a responsibility to validate that various suppliers meet the requirements for their partial deliveries. Be it cameras, VMS software, computers, switches, firewalls, planning or system management. All these actors must take responsibility for their safety culture and their deliveries. In the perspective of NIS2, one should not be able to escape responsibility by pushing it down to the underlying level, one must take responsibility for the underlying level meeting the requirements. At the same time, subcontractors are required to have a corresponding policy with routines and methods for planning, purchasing and managing their delivery, and to set corresponding requirements on their subcontractors.

A Relevant Cybersecurity Policy for CCTV Users

In a CCTV system, important parts will look a little different to the procuring user of the system, respectively the different supplier categories. The user should at least have control over the following personal areas of responsibility in a basic policy.

Physical Security of Servers and Networks
Secure the physical location of the servers. Implement access control and monitoring to monitor physical access.

Data Encryption and Backup
Use encryption for data in transit and at rest. Regularly back up important data and test the integrity of the backups.

Web Surfing and Email Risks
Use web filters and email scanning tools to detect and block malicious content. Educate employees about the risks of phishing and unsafe web browsing.

Third Party Risks
External vendors or software can introduce vulnerabilities. Review all third-party vendors and software for security. Implement strict controls on which third-party tools can be used and how.

Insider Threats
Employees with intent or negligence can pose a significant safety risk. Implement strict user access policies, conduct regular security training and monitor suspicious activity.

Network Segmentation and Access Control Risks
Ensure strong network segmentation between CCTV and office networks. Use firewalls and implement strict access control policies. Review and update access rights regularly.

Compliance and Policy Risks
Be informed about relevant cyber security laws and regulations. Regularly review and update the security policy. Conduct regular security audits and risk assessments. Conduct continuous monitoring of both networks for suspicious activity.

New Dimensions of Risk Analysis for Suppliers

For a supplier of software or hardware the list grows. Beyond control over the basic policy, further dimensions of risk analysis have to be considered.

Delivering Safe Software

As a software supplier it’s up to you to ensure that your product has a lifecycle that includes security at all stages of development. By scheduling regular code reviews, periodic security audits of the source code and monitoring that integrated third-party libraries are kept updated to their latest secure versions, you detect potential security issues. Regular vulnerability assessments and penetration tests identify and fix security flaws, for example, the use of automated tools alongside manual testing. Encryption for data at rest and in transit, especially for sensitive data.

Meanwhile, it’s of equal importance to deliver a software that supports strong authentication mechanisms, with a robust process for deploying patches and updates to address security vulnerabilities, communicating the availability of patches and the importance of applying them quickly. As well as providing documentation and training materials focused on the security aspects and "best practice " for users to maintain security. Communicate with customers to get reports of any security issues they encounter and when the worst happens, it's important to have a well-defined incident response plan that outlines actions in the event of a security breach.

Delivering Safe Hardware

By using trusted components you minimize vulnerabilities in the hardware design. Implement hardware-based security features, such as secure boot, (TPM) and (HSM). A secure supply chain prevents tampering or introduction of harmful components during manufacturing and distribution. Implement component traceability to ensure authenticity and to trace potential problems back to the source. Regular updates and secure processes for updating authenticated firmware.

Design your hardware to be difficult to tamper with, including tamper-proof designs that render the device unusable if tampering is detected. Embedded security features such as encryption, secure storage of keys and credentials, and secure communication protocols. The hardware must comply with relevant security standards and certifications, such as ISO 27001, FIPS 140-2, etc. End- of -Life Management with guidelines for safe disposal of hardware to prevent data leakage.

Provide documentation and training materials covering the security aspects. Educate customers on how to safely install, use and maintain the hardware. Establish a process for responding to vulnerabilities discovered, providing patches, updates or recalls, and a channel for customer feedback and support for security-related issues. Regular security audits and tests to identify and fix vulnerabilities. Include penetration testing and physical security assessments.

NIS2 for CCTV Suppliers

The policy points described above are basically just the starting point of NIS2, the whole of which can be summarized as follows in the parts relevant to a CCTV system supplier.[1]

1. **Risk Management**
   Organizations must take steps to minimize cyber risks, including incident management, stronger supply chain security, improved network security, better access control and encryption.

2. **Corporate Responsibility**
   NIS2 requires corporate management to monitor, approve and train the entity's cyber security measures. Violations may result in management penalties, including liability and a potential temporary suspension from management roles.

3. **Reporting Obligations**
   There are specific processes and notification deadlines for reporting security incidents, including a 24-hour "early warning" system.

4. **Business Continuity**
   Organizations must have a plan to ensure business continuity in the event of major cyber incidents, including systems recovery and crisis management teams.

5. **10 Minimum Measures**
   NIS2 prescribes basic security measures such as risk assessments, security policies, use of cryptography, security incident management plans, cyber security training and secure procurement and development of systems.

6. **Supply Chain Security**
   NIS2 attaches great importance to supply chain security. It requires organizations to assess the vulnerabilities specific to each direct supplier and the overall quality of their suppliers' cybersecurity practices.

7. **Penalties for Non-Compliance**
   NIS2 imposes severe penalties for non-compliance, with fines of up to €10,000,000 or 2% of global annual turnover for critical entities and €7,000,000 or 1.4% for important entities.

8. **Corporate Management Accountability**
   Organizational management can be held accountable for non-compliance, emphasizing the need for senior executives to be actively involved in cybersecurity.

Accounting for Future Cost

In summary, it can be stated that these stricter requirements will further drive costs for hardware, software, installations and management. Costs ultimately paid by the users of CCTV systems. Are you prepared to pay these? In our business as a software supplier, we have made an assessment that our cost to fully implement NIS2 increase our cost per line of code by approximately 20-30%.

To put this in perspective, one can put it in relation to the fact that the global CCTV market in 2023 was approximately $35,000,000,000[2] while the global cost of cybercrime was approximately $8,000,000,000,000[3] or 230 times higher.
A frightening figure which is also expected to quadruple by 2027.

Erik Erlandsson
Solution Manager, VideONet AB

Resources

[1] <https://nis2directive.eu/>
[2] <https://www.fortunebusinessinsights.com/cctv-camera-market-107115>
[3] <https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/>