EUROSMART
The Voice of the Digital Security Industry

Strengthening physical access control

Recommendations for NIS 2 and the Directive on critical entities

During the past few years, the EU discussion on critical entities has been focused on cybersecurity. There are good reasons for this: critical entities increasingly rely on digitalisation and cyber-threats are constantly on the rise. A recent ENISA study[1] shows that most critical entities have reported major information security incidents.

This focus was illustrated by the adoption of the NIS Directive[2] in 2016. This Directive created a unique framework to guarantee a high level of cybersecurity among operators of essential services (OES) and digital service providers (DSP). Last December, a new version of the NIS Directive (NIS 2)[3] was proposed by the Commission. If this new version is adopted, NIS would cover a greater number of sectors (e.g., trust services) and stronger enforcement would apply. A new distinction between essential entities and important entities replaces the former OES/DSP distinction.

Eurosmart welcomes this NIS 2 proposal, in particular the introduction of a dedicated article on certification and new requirements on encryption. However, Eurosmart would like to underline that **physical security should not be overlooked**. This is particularly the case for physical access control. Fraudulent physical access to critical infrastructures, e.g. through badge theft, can be the first step for a logical attack. Cases of hybrid-attacks should be fully taken into account by EU policymakers.

The new proposal on the resilience of critical entities[4] is a step in the right direction. It establishes physical security requirement for critical entities. Eurosmart particularly welcomes the consistent approach whereby the list of sectors for essential entities (NIS 2) corresponds to the list of sectors for critical entities. This shows that the European Commission takes seriously the link between physical security and digital security.

However, Eurosmart believes that the concept of physical access control should be better covered in these new legislative initiatives. In this paper, Eurosmart explains the importance of physical access control and how it should be better taken into account in the EU legislation.

---

[1] ENISA, NIS Investment Report, 11 December 2020.

[2] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[3] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final, 16 December 2020.

[4] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities, COM(2020) 829 final, 16 December 2020.

Physical access control: a crucial security component

Information systems used by critical entities are made up of hardware, software, communications, and data. These information systems are operated in company buildings, in the buildings of their subcontractors or in internalised or outsourced data centres. Therefore, the security of information and network systems also relies on the physical security of its servers, routers, and datacentres. This means that critical entities must take measures to control who can physically access their premisses, including their digital infrastructures.

Towards hybrid attacks on critical entities

Cybersecurity and physical security should go hand in hand as both notions are increasingly intertwined. It is crucial not to overlook the possibility of a physical attack against an IT system.[5] After all, physical attacks on buildings and data centres are much easier to implement than logical attacks. Once entered within a building premise, it is easy for an intruder to use a computer which has been left.

Therefore, systems for secure physical access control are required. Those shall be carefully designed and set up to be protected against the following threats:

- Badges are potential attack vectors, if they are stolen or loaned to a third party. **Badges shall be security certified**;
- When biometry is used with badges, access control terminals must be protected against spoofing. **Biometric terminals shall be evaluated against spoofing attacks**;
- In general, it may be possible to tamper with access control terminals. **Therefore, terminals shall also be security certified**;
- Also, it may be possible to tamper with the data exchanged on the physical access control IT infrastructure. **Access control IT infrastructure shall guarantee integrity, authenticity and confidentiality**.

If these conditions are not met, an intruder may pass through the security as if he was taking advantage of an employee's courtesy holding the door for him/her.

Nowadays, the trend is towards hybrid attacks: physical attacks by intrusion into buildings or data centres, and logical attacks by the Internet vector. In this case, the attacker often leverages physical threat vectors to bypass digital controls.[6] This can happen if an infected USB key is left in the premises of critical entities, if an attacker breaks into the server room, or, as mentioned earlier, if an intruder pretends to be an employee. The intruder can subsequently install rogue devices to get confidential data or simply look over the shoulder of a system engineer while the latter is typing his/her password.

In this scenario, attackers use flaws in physical controls, either flaws in the equipment (unsecure badges) or in the employees' training (lack of awareness regarding potential intruders).

[5] Mike James, "How Your IT System Could Be at Risk from a Physical Attack", National Cybersecurity Alliance, 19 February 2019.

[6] Resolver, "Physical and Cybersecurity Defense: How Hybrid Attacks are Raising the Stakes", 2018.

A topic of importance for national security agencies

Physical access control already has a particular relevance for OES and DSP in the framework of the NIS Directive. Today, when it comes to notification of critical IT systems to national authorities, OES and DSP first notify their IT systems for physical access controls.

This topic is gaining so much importance that national security agencies start looking into the matter. This is the case of the French cybersecurity agency, ANSSI, who has published its recommendations[7] last March. It provides guidance on security of access control system, and functional and security architecture. At European level, ENISA is preparing a guide on security requirements for physical access control system for OES and DSP, with the aim of bringing convergence between Member States.

Addressing access control in NIS 2 and the proposal on critical entities

Both NIS 2 and the Directive on the resilience of critical entities are adequate frameworks to address physical access control. This is obvious for the proposed Directive on the resilience of critical entities; its Article 11 states the following:

> *Member States shall ensure that critical entities take appropriate and proportionate technical and organisational measures to ensure their resilience, including measures necessary to:*
> *[…]*
> *(b) ensure adequate physical protection of sensitive areas, facilities and other infrastructure, including fencing, barriers, perimeter monitoring tools and routines, as well as detection equipment and* ***access controls****;*

The topic of physical access control is also relevant in the context of NIS. Recital 14 of the proposed Directive on the resilience of critical entities explains how NIS 2 and the Directive on critical entities are complementary in this respect:

> *(14) Entities pertaining to the digital infrastructure sector are in essence based on network and information systems and fall within the scope of the NIS 2 Directive, which addresses the physical security of such systems as part of their cybersecurity risk management and reporting obligations. Since those matters are covered by the NIS 2 Directive, the obligations of this Directive do not apply to such entities. […]*

Thus, entities from the digital infrastructure sector shall take measure relating to physical security pursuant to NIS 2. This was already the case in the first version of NIS, as shown by this ENISA's mapping of minimum security measures for OES, which explicitly mentions "Physical and environmental security" and "Access control" in the "Authentication and identification" section.

Therefore, most of Eurosmart's recommendations on physical access control equally apply to NIS 2 and the Directive on the resilience of critical entities.

Specific recommendation for the proposal on critical entities

Eurosmart recommends adding an article to create an expert group dedicated to physical access control. This expert group would be tasked with drafting the supporting documents (e.g., guidelines)

[7] ANSSI, Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection, 4 mars 2020.

and advising the institutions regarding the implementation of the directive. This expert group should be composed of representatives from the European Commission, ENISA and relevant stakeholders.

Specific recommendations for NIS 2

The physical security requirements of digital infrastructures are defined by NIS 2, not by the proposal on critical entities. It is also worth noting that important entities are only covered by NIS 2, not by the proposal on critical entities. Therefore, it is essential to include requirements on physical access control in the revised NIS directive. Physical access control should be explicitly mentioned in the text of NIS 2 itself. A point should be added to Article 18 paragraph 2 to mention "Strong access control" as a measure to be taken by essential and important entities.

In addition, NIS 2 should refer to the expert group on physical access control established by the proposal on critical entities – as proposed above. This expert group should provide guidance and advice for the implementation of both directives.

Recommendations for NIS 2 and the Directive on critical entities

Recommendation 1: Include specific security requirements covering physical access controls for critical entities in the supporting documents (e.g. guidelines) of NIS 2 and the Directive on the resilience of critical entities.

Recommendation 2: Require security certification of critical sub-systems, access badges, readers and controlling and processing unit involved in physical access control at level "High", pursuant to the Cybersecurity Act (CSA). More precisely:

- **Access badges** shall be security certified in accordance with the EU CC scheme – currently under preparation, with the assurance package AVA_VAN.5. This level of security certification is needed as the access badge holds very sensitive assets (e.g. cryptographic key) and may be used by malicious actor;
- **Controlling and processing unit** shall be security certified in accordance with the EU CC scheme – currently under preparation, with the assurance package AVA_VAN.3. This level of security certification is needed as it holds sensitive assets (e.g. cryptographic key);
- **Readers** shall be security certified, **biometric readers**, when used, shall be evaluated pursuant to ISO/IEC 30107 level 2 at least to testify their resistance to spoofing attacks.

Recommendation 3: The communication protocol between the physical elements installed in the buildings must be resistant to level "High" pursuant to Cybersecurity act (CSA).

Recommendation 4: Rely on ENISA's future guidance and the above-mentioned expert group to define mandatory requirements to be applied in NIS 2 and the Directive on the resilience of critical entities.

These recommendations could be implemented via implementing and/or delegated acts.

It is worth mentioning that the above-mentioned observations are also relevant for the proposal for a Digital Operational Resilience Act (DORA) covering the financial sector.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **GS TAG**, **Huawei**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Thales**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**,), consulting companies (**Internet of Trust, Trust CB**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is a member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU-level, like CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 35 | mail Contact@eurosmart.com