
SPAC
Smart Physical Access Control
POSITION PAPER

The NIS Directive[1] created a unique framework in the world of security of information systems for critical companies (OES) and critical digital service providers (DSP). This Directive is a founding act in the European cybersecurity strategy. It is the acknowledgment that an incident in one country can have significant cross-border impacts, hence requiring a minimum common level of cyber-resilience across the European Union (EU).

SPAC, the association representing the ecosystem of physical access control and Smart Building, reflects on the future evolution of this regulatory framework.

OES and DSP are companies with a physical existence

It is important to remember that information systems used by OES and DSP are made up of hardware, software, communications, and data. These information systems are operated in companies' buildings, in the buildings of their subcontractors or in internalized or outsourced data centers.

In many recitals of the NIS Directive, this notion of physical and territorial materialization is mentioned. For instance, recital 17 explains that "computing resources include resources such as networks, servers or other infrastructure, storage […]". Recital 50 mentions "hardware manufacturers", whose products enhance the security of network and information systems. The Directive further states that "the Commission is encouraged to take into account the following examples: as regards security of systems and facilities: physical and environmental security […]" (Recital 69).

Therefore, SPAC believes that the NIS Directive is the adequate framework to address the issue of physical and hybrid attacks on OES and DSP. However, these aspects should not only be tackled in mere recitals but also in the binding provisions of the NIS Directive. This point is developed later on.

The trend is towards hybrid attacks

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.[2] After all, physical attacks on buildings and data centres are much easier to implement than logical attacks.
An attack can be carried out simply by entering the building premises and using a computer which has been left. Badges, for instances, are potential attack vectors, if they are stolen, loaned and if the biometric link is weak. They subsequently give access to the physical infrastructure. The same can happen if an intruder takes advantage of an employee's courtesy holding the door for him/her.

[1] 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.

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

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.[3] This can happen if an infected USB key is left in the premises of OES or DSP, 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 case, attackers use flaws in physical controls, either flaws in the equipment (unsecure badges) or in the employees' training (lack of awareness regarding potential intruders).

This subject is becoming important for national security agencies

Physical access control already has a particular relevance for OES and DSP. 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[4] last March. This guide gives advice on badge security, functional and security architecture. According to ANSSI, Architecture 1 completed by recommendation R37 is the most secure architecture (see Annex 1).

At European level, ENISA is preparing a security requirement guide about physical access control of OES and DSP with the aim of bringing convergence between Member States.

Recommendations for the revision of the NIS Directive

Recommendation 1: Include a specific chapter on the security and certification requirements of the physical access controls of OES and DSP in the revision of the NIS Directive.

Recommendation 2: Prescribe security certification of critical sub-systems at level High pursuant to the Cybersecurity Act (CSA), using the EU CC scheme. The critical sub-systems are access badges, system inspections (readers) and UTLs.

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 to define mandatory requirements to be applied in NIS and future legislative instrument for measures to enhance the protection and resilience of critical infrastructure.

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

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

Annex 1:

Interpretation note and editorial correction of the ANSSI guidance document[5] by the professional association S.P.A.C.: Type n ° 1 + architecture dedicated to the needs of OVI and OSE.

ANSSI has published its guide on the recommendations for securing physical access control and video protections defining 4 types of architectures between the badge and the UTL.

Note that in the current version of the guide, the title of chapter 6.5 contains an editorial error (confirmed by ANSSI) because it indicates that the 4 types of architectures concern the exchanges between the reader and the UTL and not between the badge and the UTL.

Configuration number 1: Transparent reader, end-to-end authentication: recommended by ANSSI

Configuration number 2: Smart reader, double authentication: not recommended by ANSSI

Configuration number 3: Badge not secured, with wired encryption only: to be avoided by ANSSI

Configuration number 4: Badge secured, with unencrypted wired link: to be avoided by ANSSI

Our Association SPAC, fulfilling its duty to advice, has built an architecture based on the architecture recommended by the ANSSI number 1 and has improved it by the possibility of guaranteeing integrity and confidentiality, by the encryption of sensitive data transiting through the communication bus between the reader and the UTL without impacting the transparent mode of the card. It increases the global security level of the access control in accordance with the R37 of the ANSSI guide.

The architecture number 1 allows keeping the transparent mode between the badge and the UTL recommended by the ANSSI guide. It adds on top of it the secured management of the manual PIN entry and the biometrics data as defined in the recommendation R37 of the ANSSI guide.

This new architecture type 1+ combined with a certification type CSPN of the readers and UTL is the only one suitable for the needs of French OVI and OES. It allows the secured manual entry PIN and Biometrics data.

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