MITIGATING SECURITY RISKS FOR INTELLIGENT BUILDINGS

Vincent Dupart, President of S.P.A.C. and Anne-Isabelle Parodi, General Secretary of S.P.A.C. discuss the security of smart technology

What is an intelligent building, what are the benefits and the risks?

Vincent Dupart: Smart buildings make it possible to 'intelligently' optimise the use of assets, operations and the consumption of resources. All infrastructures are being transformed thanks to connected technology.

For example, smart thermostats can change the temperature remotely, or smart lighting can be controlled and adjusted from almost any smartphone or from any connected device.

Convergence of operational technology and computer systems is essential to support these smart devices but, without strong security measures, it can make facilities vulnerable to multiple cyberattacks.

If a hacker can enter a smart building through an operational entry point, he/she can potentially gain access to the building's computer network, opening new opportunities for the hacker. And all operational technologies, such as connected devices or security objects, connected or not, as well as communications protocols are an entry point to access the organisations' networks.

Before we go any further, could you explain what the S.P.A.C. Alliance is please?

Vincent Dupart: Companies are increasingly subject to physical attacks. Attackers can take advantage of weak physical security solutions to gain access to computer networks and to implement logical attacks. They can also gain access to the computer network through any connected operational device. That is why cybersecurity and physical attacks should go hand in hand as both notions are increasingly intertwined.

And in addition, operational technologies, connected or not, are more present in company premises and can be an entry point to access organisational networks. Faced with these serious physical threats, we decided to create S.P.A.C.

S.P.A.C. is an alliance whose goal is to build a strong and open physical security industry including connected industry.

What are the assets used by S.P.A.C. to fulfil its objectives and which are adaptable to smart buildings?

Anne-Isabelle Parodi: To promote strong physical solutions, S.P.A.C. is based on the French and European regulatory framework and on the SSCP communication protocol.

Following the rise of hybrid attacks against sensitive or critical infrastructures, the European Commission and European security agencies such as the A.N.S.S.I. have defined a regulatory framework to fight against these attacks.

These Directives. like the NIS Directive, define recommendations to be implemented in our operational systems and in protocols to resist all cyberattacks. In addition, these institutional entities recommend security certifications of all devices and protocols included in an infrastructure.

S.P.A.C. is the first alliance in Europe to meet all these challenges: we offer functional certification with the SSCP Communication protocol and we count among our members the certifications providers that can be useful to provide a high level of security for your smart building.

It is important to mention that the SSCP protocol offers the possibility of communicating on wired and wireless links and with different hardware objects, which is mandatory for a smart building. And the SSCP protocol is a European Standard allowing integrity and confidentiality by the encryption of sensitive data.

For more information about S.P.A.C., please contact: https://en.sp-ac.org/

THE **SECURITY** EVENT

7-9 SEPTEMBER 2021

NEC BIRMINGHAM UK

THE UK'S NO.1 COMMERCIAL, ENTERPRISE & DOMESTIC SECURITY EVENT

1000+ PRODUCTS & SOLUTIONS

LIVE DEMOS & **WORKSHOPS**

CPD ACCREDITED CONTENT

ONE PASS, SIX EVENTS
REGISTER FOR YOUR FREE TICKET

WWW.THESECURITYEVENT.CO.UK

CO-LOCATED WITH:

THE FIRE SAFETY EVENT · THE HEALTH & SAFETY EVENT · THE FACILITIES EVENT · THE EMERGENCY SERVICES SHOW