

Smart Buildings face à NIS2 : la sécurité physique à l'épreuve du risque cyber

Le nouveau défi des infrastructures connectées



A l'ère des bâtiments dits « smart », la frontière entre sécurité physique et sécurité numérique s'est définitivement effacée. Désormais, **un pirate informatique peut** non seulement dérober des données confidentielles, mais aussi **verrouiller à distance des accès sécurisés ou paralyser les systèmes** de désenfumage d'un site industriel.

Face à cette convergence des menaces technologiques et physiques, **les organisations doivent nécessairement décroiser leur gestion des risques**. Cette mutation opérationnelle est aujourd'hui dictée et accélérée par le durcissement des obligations réglementaires européennes, au premier rang desquelles figure la directive NIS2.

Le Salon EXPOPROTECTION se positionne au cœur de ce nouveau paradigme de la « sécurité globale » pour guider les entreprises vers une gouvernance plus unifiée des risques.

Quand le virtuel menace directement le réel

Le déploiement massif de la Gestion Technique du Bâtiment (GTB/GTC), du contrôle d'accès par badge mobile, de la vidéosurveillance intelligente et des objets connectés (IoT) crée **une dépendance numérique systémique** et **élargit considérablement la surface de vulnérabilité des infrastructures**.

Une simple intrusion au sein du système d'information (IT) peut désormais se traduire par **des impacts physiques immédiats**, comme l'ouverture non autorisée d'un accès ou le blocage complet des issues de secours lors d'une évacuation. Une attaque cyber sur des systèmes connectés produit ainsi des effets directs sur la sûreté et la production.

De plus, la digitalisation des **Systèmes de Sécurité Incendie (SSI) interconnectés à la GTB et aux outils de supervision** augmente le **risque qu'une panne numérique ou une cyberattaque** rende indisponibles les alarmes et les systèmes d'extraction de fumée. Un système de supervision compromis dégrade simultanément la sûreté et la lutte contre l'incendie.

C'est précisément pour parer à ces menaces systémiques que la **directive européenne NIS2** impose des mesures strictes de gestion des risques et de gouvernance à l'échelle de l'UE. En France, sa transposition s'articule avec le **projet de loi sur la résilience des infrastructures critiques** et la **directive REC** (Résilience des entités critiques). Cette double pression pousse les organisations à adopter une approche multirisque et des Plans de Continuité d'Activité beaucoup plus structurés.

Bâtir la résilience globale

Face à ces menaces hybrides, EXPOPROTECTION défend une approche intégrée et transverse de la sécurité. Il est devenu indispensable de dépasser la gestion en silos pour **piloter la sûreté, l'incendie et la cybersécurité comme un portefeuille de risques interconnectés**.

La solution réside dans la segmentation stricte des réseaux, le déploiement d'outils de supervision fine et la prévision des modes dégradés. Les entreprises doivent impérativement intégrer des procédures opérationnelles (papier + terrain) prêtes à prendre le relais dès lors que le numérique défaille.

Pour améliorer la résilience, les fonctions de RSSI (Responsable de la Sécurité des Systèmes d'Information), de **Directeur de la sûreté & gestion de crise** et de Responsable **SST** (Santé et Sécurité au travail) **doivent collaborer de manière coordonnée**. Cette préparation passe par des exercices de simulation réguliers combinant des scénarios multirisques (ex. panne informatique majeure survenant simultanément à une intrusion physique).

L'esprit des réglementations NIS2 et REC est de préparer les organisations à absorber le choc, résister et se rétablir rapidement. Bien appréhendée, la gestion de ces vulnérabilités cyber-physiques transforme la sécurité en un levier stratégique pilotable, créateur de valeur et de confiance.

Paroles d'experts :

« L'essor des bâtiments intelligents lie désormais indissociablement sécurité physique et cybersécurité : une faille numérique peut directement compromettre les infrastructures et la sécurité des occupants. Face à ces risques imbriqués, l'ingénierie du risque exige une approche globale, sécurisant en priorité les accès critiques comme la télémaintenance.

Cette transformation impose aussi une convergence organisationnelle. Décloisonner les compétences en faisant collaborer experts IT et spécialistes de la sûreté au sein d'équipes mixtes devient indispensable. Une telle coopération renforce l'anticipation et la prévention pour bâtir une réponse intégrée, seule protection durable face à des menaces complexes. » Laurence Marchal, Présidente de l'Agrépi.

« Pour garantir une installation de sécurité robuste face aux risques cyber, il est essentiel d'agir sur deux fronts complémentaires. D'une part, l'installateur doit intégrer des mesures spécifiques de cybersécurité dans son travail, en s'appuyant sur des référentiels et bonnes pratiques adaptés, afin d'accompagner ses clients vers la conformité aux exigences applicables, comme celles de la directive NIS2. D'autre part, l'installation ne peut être considérée comme conforme que si les produits utilisés offrent une robustesse réelle face aux attaques numériques, garantissant ainsi la résilience globale de l'infrastructure. La certification de ces produits, intégrant demain leur conformité au Cyber Resilience Act (CRA), vient ensuite attester et formaliser cette robustesse.

Ce n'est qu'en combinant une installation rigoureuse et des produits conçus pour résister aux cyberattaques que l'on obtient une infrastructure cohérente et durable. L'un ne peut et ne doit pas aller sans l'autre pour protéger durablement les infrastructures connectées. » Ronan JEZEQUEL, Directeur Innovation & Développement Groupe CNPP.

« Les bâtiments sont aujourd'hui de véritables systèmes numériques. Caméras, contrôle d'accès, ventilation ou gestion technique sont désormais connectés aux réseaux IP, ce qui ouvre de nouvelles possibilités de pilotage mais les expose aussi aux vulnérabilités du monde cyber. Le véritable enjeu n'est donc pas de multiplier les technologies de sécurité, mais de changer notre façon de les gérer. Les équipements de sûreté doivent aujourd'hui être administrés, surveillés et mis à jour avec les mêmes exigences que les systèmes informatiques. Cette convergence impose également de rapprocher les équipes IT et sûreté afin de construire une approche globale de la résilience des bâtiments. » Benoît Grunemwald, Expert Cyber au sein d'ESET France.

Salon EXPOPROTECTION 2026

« Décloisonner la gestion des risques face à la convergence des menaces et des technologies »,

30^e édition – Porte de Versailles Hall 1

du 3 au 5 novembre 2026

Journalistes, pensez à vous accréditer en cliquant [ici](#)

A propos d'EXPOPROTECTION :

Fondé dans les années 1960, Expoprotection célèbre en 2026 sa 30^{ème} édition. Ce rendez-vous biennal incontournable de la prévention et de la maîtrise des risques réunit près de 660 exposants et autour de 14 500 visiteurs. Le salon offre une vision à 360° unique en France du marché de la prévention des risques, qu'ils soient professionnels, industriels, climatiques ou liés aux actes malveillants. C'est l'événement idéal pour découvrir les dernières innovations du secteur, rencontrer des experts de haut niveau et faire appel à des fournisseurs de solutions performantes afin de protéger les hommes et les organisations contre l'ensemble des menaces auxquelles ils sont exposés. www.expoprotection.com

A propos de RX :

[RX](#) est un leader mondial d'événements et de salons. RX s'appuie sur son expertise sectorielle, les données et la technologie pour le développement des entreprises, des collectivités et des individus. Présent dans 25 pays et couvrant 41 secteurs d'activité, RX organise près de 350 événements par an. [RX](#) s'engage à créer un environnement de travail inclusif pour tous ses collaborateurs et collaboratrices. RX permet aux entreprises de se développer grâce à la donnée et aux solutions digitales. RX fait partie de RELX, un fournisseur mondial de données, d'outils d'analyse et d'aide à la décision pour les professionnels et les entreprises. Pour plus d'informations, visitez le site www.rxglobal.com.

[RX France](#) est créateur de places de rencontres à forte valeur ajoutée, leaders sur une quinzaine de marchés différents. Parmi les salons emblématiques de RX France et incontournables sur le plan national et international, figurent APS, Expoprotection, IT Partners, MIPIM, MIPCOM, Batimat, Pollutec, EquipHotel, SITL, IFTM, Big Data & AI Paris, MAPIC, Paris Photo, Maison&Objet* et bien d'autres... Nos événements se déroulent en France, à Hong Kong, en Italie et au Mexique. Plus d'informations sur www.rxglobal.fr *Organisé par la SAFI, filiale de RX France et Ateliers d'Art de France

Service de presse

Agence Antidox (NSI)

Kelly LEOTARDI

kelly.leotardi@nsi-adit.com

+33 7 50 87 76 62

Anne-Claire BERTHOMIEU

[anne-claire.berthomieu@nsi-](mailto:anne-claire.berthomieu@nsi-adit.com)

adit.com

+ 33 6 16 53 15 70