MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH INGÉRENCE ÉCONOMIQUE DGSI #113

Mai 2025

RISQUES LIÉS AUX DÉFAILLANCES EN MATIÈRE DE SÛRETÉ BÂTIMENTAIRE

Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes.

Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Il est également disponible sur le site internet : **www.dgsi.interieur.gouv.fr**

Par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à :

> **securite-economique@interieur.gouv.fr**

RISQUES LIÉS AUX DÉFAILLANCES EN MATIÈRE DE SÛRETÉ BÂTIMENTAIRE

Les entreprises et laboratoires de recherche sont confrontés à des menaces émanant d'acteurs aux profils multiples. Si les risques cyber sont généralement bien identifiés, les menaces résultant de failles dans la sécurité physique tendent à être négligées alors qu'elles peuvent créer un terrain propice aux actions malveillantes.

Pour assurer pleinement sa protection, toute entreprise ou laboratoire de recherche doit établir une politique de sécurité prenant en compte la totalité des risques auxquels l'entité peut être exposée, qu'il s'agisse de risques d'origine externe comme interne, et prévoir des mesures adaptées à la sensibilité de son activité.

Dès lors, l'adoption d'une politique de sûreté bâtimentaire est essentielle pour limiter les risques d'intrusion susceptibles de conduire à des vols d'informations ou de matériels sensibles, à des dégradations ou à des actes de sabotage, à des actes d'espionnage ou encore à des campagnes d'atteinte à la réputation.

1 INTRUSION NOCTURNE D'UN INDIVIDU DANS UN SITE SENSIBLE PLACÉ SOUS ALARME PAR UNE PORTE LAISSÉE NON-VERROUILLÉE

Un individu a pu s'introduire de nuit au sein d'une infrastructure sensible en empruntant une entrée secondaire laissée ouverte. S'il n'a commis aucune dégradation ou vol, le dispositif de vidéosurveillance a révélé qu'il avait pris de nombreux clichés de zones précises à l'intérieur de l'enceinte, laissant penser à une opération de repérage pour de futures actions malveillantes.

La présence de l'individu ayant déclenché une alarme automatique, le service de gardiennage a pu venir à sa rencontre pour le contrôler. Il a simplement indiqué s'être perdu et ne pas savoir qu'il s'agissait d'un lieu interdit au public.

Si le dispositif de vidéosurveillance et la présence d'une équipe de gardiennage ont permis la détection rapide de l'individu, l'application des mesures de sûreté existantes, comme la vérification quotidienne de la fermeture systématique de chaque accès, aurait pu empêcher l'intrusion, et limiter le risque que représente la potentielle circulation des clichés pris par l'individu.

2 VOL PAR EFFRACTION AU SEIN DES LOCAUX D'UNE ENTREPRISE SENSIBLE DÉPOURVUE DE SYSTÈMES DE DÉTECTION ET DE PROTECTION

Un site d'une entreprise exerçant dans un domaine stratégique a fait l'objet d'un vol avec effraction. Lors d'un week-end prolongé, plusieurs individus se sont introduits dans les lieux en escaladant la façade pour atteindre les bureaux d'un étage intermédiaire, dépourvus de système d'alarme et de vidéosurveillance.

Brisant une fenêtre, ils ont ensuite dérobé plusieurs ordinateurs, un coffre-fort contenant des informations sensibles, ainsi que des jeux de clés du site. Les individus ont pu quitter les lieux sans être inquiétés. L'entreprise a déposé plainte dès que le vol a été constaté.

À la suite de ces vols, les responsables de l'entreprise ont pris conscience des vulnérabilités bâtimentaires auxquelles ils étaient exposés et ont pris des mesures pour rehausser le niveau de sécurité physique de leurs locaux.

3 VOL D'ORDINATEURS ET DE DISQUES DURS AU SEIN D'UN CENTRE DE RECHERCHE EN RAISON D'UNE SÛRETÉ BÂTIMENTAIRE INSUFFISANTE

Au cours d'une nuit, au milieu de vacances universitaires, un important centre de recherche a été victime de vols ciblés. Plusieurs individus ont contourné les systèmes de détection anti-intrusion, présents uniquement dans les couloirs, en brisant les fenêtres de nombreux bureaux et salles de travail.

Les individus ont dérobé plus d'une dizaine d'ordinateurs portables et de disques durs, dont certains n'étaient pas chiffrés, permettant un accès libre aux données de recherche stockées sur les supports numériques.

La direction de l'établissement a procédé à un dépôt de plainte dès le constat du vol et a fait renforcer la fréquence des rondes du service de surveillance. Une réflexion a été engagée pour généraliser la présence des systèmes anti-intrusion et de vidéosurveillance.

Commentaires

Les mesures de sûreté bâtimentaire contribuent à la politique globale de sécurité d'une structure, entreprise ou laboratoire de recherche, au même titre que la protection cybernétique ou la protection juridique.

Ces mesures doivent couvrir l'ensemble du spectre de la sûreté bâtimentaire : dissuader, bloquer, ralentir et détecter les intrusions pour permettre l'intervention des forces de l'ordre. Elles débutent à l'extérieur de la structure et doivent prendre en compte l'ensemble des accès aux bâtiments (fenêtres, portes, terrasses accessibles, etc.). À l'intérieur des locaux, l'accès aux espaces doit être réglementé en fonction de la sensibilité des travaux menés. Les matériels ou les informations sensibles doivent être placés dans des zones sécurisées.

La politique de sûreté bâtimentaire doit être intégrée dans une démarche de réévaluation et de recherche d'amélioration constante en vue de s'adapter à l'évolution des menaces et d'éviter l'obsolescence des moyens déployés pour protéger l'entité.

Même si une entité dispose de moyens financiers limités, des mesures simples et peu coûteuses, parfois simplement d'ordre organisationnel, peuvent déjà permettre de relever significativement le niveau de sûreté physique des locaux.

Effectuer un bilan des dispositifs de sûreté existants

- **Effectuer un audit de sûreté bâtimentaire.**

  La réalisation d'un audit permet de cartographier les locaux de l'entité, de hiérarchiser les différents espaces selon leur niveau de sensibilité et d'identifier ainsi les vulnérabilités existantes pour instaurer des mesures de protection adaptées.

  La DGSI propose gratuitement, et sur simple demande, des missions de conseil en sûreté bâtimentaire. Cette prestation consiste en une évaluation des risques d'intrusion physique dans les bâtiments d'entités sensibles, publiques ou privées. Des préconisations adaptées à chaque situation sont formulées afin de permettre aux entités visées d'améliorer leur niveau de sûreté.

- **Effectuer des tests d'intrusion physique pour évaluer son dispositif de sûreté.**

  À l'issue d'une évaluation de la sûreté bâtimentaire de ses locaux, il peut être utile de mener ponctuellement des tests d'intrusion pour vérifier l'efficacité du dispositif mis en place, la réactivité des équipes de sécurité ou pour sensibiliser les personnels aux risques d'intrusion ou d'effraction. Ces tests permettent de mettre en exergue les défaillances dans les dispositifs ou la politique de sûreté des locaux.

- **Réévaluer périodiquement les processus de sécurité.**

  La sûreté bâtimentaire doit être considérée comme un processus de vigilance constante et s'inscrire dans une démarche de réévaluation périodique pour tenir compte de l'évolution des menaces et s'assurer de l'efficacité des mesures établies. Il est donc recommandé de réitérer les audits à intervalle de temps régulier pour formaliser d'éventuels nouvelles mesures et les communiquer à l'ensemble des salariés.

Instaurer des mesures de protection adaptées au niveau de sensibilité des locaux

- **Mettre en place des mesures élémentaires d'ordre organisationnel visant à contrôler les accès aux différents espaces.**

  La délivrance de badges d'accès dotés de codes-couleurs en fonction du statut des personnels (visiteur, prestataire, salarié), permet de développer une culture interne de sûreté. Un accompagnement obligatoire des visiteurs peut être envisagé. De même, le verrouillage des portes des bureaux et des salles hébergeant des données sensibles peut être rendu obligatoire et soumis à des contrôles aléatoires.

- **Renforcer les protections extérieures du site.**

  À l'extérieur du site, des clôtures ou de simples barrières levantes peuvent déjà avoir un effet dissuasif et limiter les intrusions à répétition. Une signalétique claire permet également de mettre en tort des individus qui prétendraient ne pas avoir connaissance de l'interdiction d'accéder au bâtiment sans autorisation. La robustesse des fenêtres et des portes d'accès peut également être renforcée par l'installation de volets roulants, de barreaux ou de vitrages renforcés.

- **Envisager d'installer un système de détection d'intrusion pour protéger l'intérieur des locaux.**

  Différents types de détecteurs peuvent être installés : détection d'ouverture, de choc ou encore de présence. Ces détecteurs peuvent être couplés à un système de surveillance vidéo et/ou un système d'alarme, relié à un poste de sécurité chargé d'intervenir ou de procéder à une levée de doute en cas d'événement signalé. Ces dispositifs sont non seulement dissuasifs, mais ils permettent également de localiser rapidement les incidents et de faciliter l'intervention des forces de l'ordre.

En cas d'incident lié à une intrusion physique

- **Déposer plainte auprès des services de police ou de gendarmerie.**

  Le dépôt de plainte est une procédure simple, rapide et gratuite. Il permet à la victime de se prévaloir de ce statut auprès des services de l'État et de pouvoir bénéficier d'un accompagnement adapté.

- **Contacter la DGSI afin de signaler l'incident.**

  Le service dispose d'une adresse électronique dédiée aux sujets de protection économique :

  securite-economique@interieur.gouv.fr

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité