MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH DGSI #67

SEPTEMBRE 2020

INGÉRENCE ÉCONOMIQUE

LES RISQUES INDUITS PAR LES INTRUSIONS HUMAINES

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.

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

LES RISQUES INDUITS PAR LES INTRUSIONS HUMAINES

Les intrusions d'individus sur les sites des entreprises, dans les laboratoires ou dans des établissements publics représentent l'une des principales menaces auxquelles doivent faire face les acteurs économiques français. Les motifs à l'origine des intrusions sont variés (commettre un vol crapuleux, se livrer à de l'espionnage industriel et capter des informations sensibles, saboter une installation, etc.) et leurs conséquences, parfois difficiles à identifier de prime abord, peuvent s'avérer particulièrement dommageables (pertes financières inhérentes au vol de matériels, destruction de biens, atteinte à la réputation, captation de données sensibles, etc.).

L'absence ou la vétusté des mesures et systèmes de protection et de surveillance, le faible niveau de sensibilisation et de formation des employés aux bonnes pratiques et au respect des règles en vigueur, ou encore la forte exposition médiatique sont des facteurs de risque qui accroissent la vulnérabilité des entités françaises face au risque d'intrusion.

Par ailleurs, la crise sanitaire et la lutte contre la COVID-19 ont parfois conduit les entreprises à assouplir provisoirement leurs procédures internes relatives à la sûreté bâtimentaire, facilitant ainsi les intrusions et la commission d'actes malveillants.

PREMIER EXEMPLE

Dans la nuit du vendredi au samedi, un individu a pu pénétrer sur le site d'une grande entreprise française en escaladant le mur d'enceinte de l'établissement. Profitant du fait que certaines portes n'étaient pas verrouillées afin de faciliter les accès en raison des mesures sanitaires, l'individu a pu accéder aux locaux abritant les bureaux dédiés aux travaux de recherche et développement (R&D) où il a dérobé plusieurs équipements informatiques. À noter que ce dernier ne s'est pas intéressé aux matériels neufs, pourtant beaucoup plus performants et d'une valeur marchande élevée, mais a préféré dérober des ordinateurs et des supports de stockage, entreposés dans des armoires qui n'avaient pas été fermées à clef.

Ces équipements informatiques contenaient des informations particulièrement sensibles, voire stratégiques pour le développement de l'entreprise. Les données n'étaient pas cryptées et les ordinateurs étaient protégés seulement par un mot de passe à l'ouverture de la session.

La faible résolution des caméras, due à l'obsolescence du dispositif de vidéo-protection, n'a pas permis d'identifier l'individu malveillant.

DEUXIÈME EXEMPLE

En pleine journée, une entreprise stratégique française a été victime d'une intrusion de la part d'un individu qui a pu pénétrer dans l'enceinte de l'entreprise à bord d'un véhicule, en profitant de l'entrée sur le site d'un camion de transport. Une fois à l'intérieur, l'intrus a été en mesure de prendre plusieurs photographies. Repéré par des employés, il a pu être intercepté par un membre du personnel chargé de la sûreté de l'entreprise, qui l'a interrogé sur la raison de sa présence à l'intérieur de l'établissement, avant de procéder à son expulsion. L'individu, d'origine étrangère, s'est montré incapable d'expliquer la raison de sa présence à l'intérieur du site de l'entreprise française. Les images de vidéo-protection n'ont pas été conservées par l'entreprise.

Si cette intrusion n'a pas mis en danger la société française, des matériels, parfois issus de plusieurs années de R&D, auraient pu être volés, représentant ainsi un lourd préjudice, notamment pour les clients de l'entreprise. Néanmoins, l'étude détaillée des photographies prises lors de l'intrusion pourrait permettre à un individu malintentionné d'obtenir des informations précieuses.

TROISIÈME EXEMPLE

À plusieurs reprises et sur une courte période de temps, un site industriel a fait l'objet de plusieurs actes malveillants, notamment le vol d'un ordinateur contenant des informations stratégiques. Le matériel informatique volé se trouvait dans une pièce fermée à clef, bien qu'aucune effraction n'ait été constatée. Toutefois, l'entreprise ne disposait pas d'un registre permettant l'identification des personnes détentrices d'une clef et autorisées à accéder au local où se trouvait l'ordinateur.

La même société a également été victime, quelques semaines plus tard, de dégradations volontaires. Si aucun vol n'a été commis, la piste de l'acte de sabotage est privilégiée. L'individu malveillant a profité de la désactivation, au cours d'une coupure de l'électricité, des caméras de vidéo-protection pour commettre son méfait.

Si pour le premier vol, le préjudice est estimé à plusieurs milliers d'euros, les dégradations volontaires représentent, quant à elles, un préjudice de plusieurs dizaines de milliers d'euros. Dans les deux cas, les circonstances dans lesquelles les actes malveillants ont été commis laissent penser que le ou les auteurs connaissaient les locaux et les procédures de l'entreprise ou ont pu bénéficier de complicités internes.

COMMENTAIRES

Les intrusions représentent une menace sérieuse pour les entreprises, les laboratoires de recherche et les établissements publics. Les conséquences de ces intrusions dépendent des motivations de l'intrus, mais aussi des mesures de prévention mises en place par l'entité.

Pour prévenir les tentatives d'intrusion, les acteurs économiques français doivent se doter d'une politique de sûreté bâtimentaire rigoureuse, qui implique des infrastructures, des équipements et des mesures de protection adaptées, et sensibiliser leurs personnels, afin d'assurer la protection des personnes et des biens, de renforcer la protection des données sensibles et de préserver la réputation de la personne morale.

Par ailleurs, les mesures nécessaires et obligatoires permettant de répondre aux enjeux de la crise sanitaire et lutter contre la Covid-19 ne doivent pas faire oublier les impératifs de sûreté bâtimentaire et le besoin de protéger les informations sensibles et stratégiques.

PRÉCONISATIONS DE LA DGSI

FACE AUX RISQUES D'INTRUSIONS PHYSIQUES, LA DGSI ÉMET LES PRÉCONISATIONS SUIVANTES :

- Renforcer les moyens de protection, de surveillance (physique et logique) et de vidéo-protection, dans les zones périphériques et périmétriques de la société, ainsi que dans les zones de valeur identifiées.
- S'assurer régulièrement du bon état des dispositifs de protection périphérique (clôtures, murs d'enceinte, portails) et réparer sans délais toute dégradation ou altération de leur efficacité.
- Asservir dans la mesure du possible les entrées du site et des zones sensibles à un lecteur de badge afin de limiter l'accès aux seules personnes autorisées, permettant ainsi un réel contrôle des flux et une traçabilité efficace.
- Concilier les contraintes inhérentes au contexte sanitaire (accès et ouvertures facilités, portes laissées ouvertes) avec les impératifs de sûreté bâtimentaire. En effet, des individus malveillants profitent de la situation exceptionnelle pour s'introduire et commettre des vols sur des sites plus vulnérables qu'à l'accoutumée.
- Réfléchir à la pertinence d'organiser, ponctuellement, des tests d'intrusions physiques, à l'image des exercices d'évacuation incendie, destinés à évaluer le respect des procédures de sécurité Dans tous les cas, tester régulièrement les dispositifs de sûreté (alarmes, portes, etc.) afin de vérifier leur efficacité, d'anticiper leur remplacement en cas d'obsolescence et de veiller à leur bonne utilisation par les personnels.
- Inciter les collaborateurs à adopter de meilleures pratiques en matière de conservation des données sensibles de l'entreprise, notamment concernant le rangement des équipements électroniques nomades mis à leur disposition.
- Disposer des registres et des outils nécessaires afin d'identifier, notamment lorsqu'il s'agit de prestataires externes et de sous-traitants, les personnes physiques autorisées à accéder aux différents locaux de l'entreprise, identifiés au préalable, où sont stockés des matériels critiques pour la société ou des informations sensibles.
- Évaluer les conséquences d'une intrusion en termes de réputation vis-à-vis de ses clients et partenaires commerciaux, notamment dans le cadre de contrats sensibles ou qui impliquent des mesures de sûreté particulières.
- En cas d'intrusion, envisager un dépôt de plainte auprès des services de police ou de gendarmerie, ou directement auprès du procureur de la République. Dans la limite du respect des lois et réglementations en vigueur, collecter et conserver les différents éléments qui pourront permettre aux services enquêteurs de mener leur enquête et d'identifier les individus qui se sont introduits sans autorisation sur le site de l'entreprise.