MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

FLASH DGSI #93

AVRIL 2023

INGÉRENCE ÉCONOMIQUE

IDENTIFIER LES OPÉRATIONS DE REPÉRAGE PRÉALABLES À UN ESPIONNAGE INDUSTRIEL

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

Vous comprendrez que, 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

IDENTIFIER LES OPÉRATIONS DE REPÉRAGE PRÉALABLES À UN ESPIONNAGE INDUSTRIEL

Les opérations de repérage désignent l'ensemble des actions menées dans le but d'identifier les failles de sécurité d'un site où peuvent être entreposés des biens ou stockées des données sensibles et de valeur. Elles ont souvent pour objet de préparer un vol, une dégradation ou une démarche d'espionnage industriel. Les opérations de repérage peuvent concerner tout type de structure (start-up, PME, grand groupe, site industriel, laboratoire ou centre de recherche, etc.), dès lors que ses bâtiments abritent des biens ou données dont la valeur matérielle ou immatérielle peut présenter un intérêt.

Les opérations de repérage peuvent être plus ou moins intrusives et se dérouler soit aux abords d'un site, notamment afin d'effectuer des prises de photographies, soit directement à l'intérieur des locaux, accomplies par des individus qui contourneraient les dispositifs de sécurité pour pénétrer dans un site sans autorisation. En outre, le développement et la commercialisation à moindre coût de nouvelles technologies facilitant la surveillance, à l'image des drones, a engendré une multiplication notable des opérations de repérage.

PREMIER EXEMPLE

Un drone survole à plusieurs reprises un site industriel.

Un site industriel sensible, spécialisé dans la conception de machines et de systèmes d'automatisation pour l'industrie et filiale d'un grand groupe d'ingénierie, a fait l'objet, en l'espace d'une semaine, de trois survols de drones avec prises de photographies.

Le premier survol a eu lieu un soir vers 20 heures. Le drone n'a alors survolé que les abords du site veillant ainsi à demeurer dans l'espace public. Aucun signalement n'a été réalisé, puisqu'il n'a pas été établi que le drone avait effectivement visé la société.

Le deuxième survol a eu lieu quatre jours plus tard, en début d'après-midi, lors d'une période de vacances scolaires. Le même drone s'est positionné dans l'enceinte de la société et a pris, pendant une minute, une série de clichés de l'intérieur de l'un des hangars. Dans celui-ci, se trouvaient plusieurs machines en cours d'assemblage et destinées à des clients industriels sensibles. Deux jours plus tard, le drone a effectué un nouveau survol de l'ensemble du site.

Ces incidents pouvaient aussi bien s'apparenter à de l'espionnage industriel qu'à une opération de repérage annonçant des vols de matériaux, par ailleurs fréquents dans la zone d'implantation de la société.

DEUXIEME EXEMPLE

Des individus s'introduisent dans les locaux d'un grand groupe industriel afin de repérer les lieux en contournant les dispositifs de sécurité.

Le siège d'une grande entreprise industrielle, régulièrement ciblée par des associations de défense de l'environnement, a enregistré en quelques semaines trois incidents assimilables à des opérations de repérage, qui ont notamment mis en évidence plusieurs failles de sécurité.

Lors de l'un de ces incidents, un individu, qui s'est présenté plus tard comme membre d'une organisation non gouvernementale, est parvenu à pénétrer dans les locaux durant la pause méridienne sans se signaler à l'accueil qui délivre habituellement un badge à tous les visiteurs. L'individu a pu prendre l'ascenseur, dont l'accès n'est possible qu'avec un badge, en profitant des allers et venues de salariés du site, et a ainsi été en mesure de visiter plusieurs étages, accédant notamment au département le plus sensible de l'entité.

L'individu a finalement été intercepté par un salarié, qui l'a raccompagné à l'accueil afin qu'il soit prise en charge par le service de sécurité. Le chef du site l'a toutefois laissé partir sans lui demander son identité, ni obtenir d'explications sur les raisons de sa présence.

Les deux autres incidents, qui se sont déroulés quelques semaines plus tard, ont impliqué de multiples prises de photographies et de vidéos des moyens d'accès à l'entité. Dans l'un des cas, une autre personne est entrée dans le hall et a pris des photos des différents accès pendant une dizaine de minutes. Elle a pu repartir sans avoir été interrogée par un agent de sécurité.

TROISIEME EXEMPLE

Un individu effectue des prises de vue depuis son véhicule aux abords d'un site produisant des équipements numériques sensibles.

Durant l'été, à une période où l'activité est plutôt réduite, un individu à bord d'un véhicule s'est garé à proximité immédiate de l'entrée d'une société spécialisée dans la fabrication d'équipements numériques sensibles. Durant plusieurs minutes, l'individu a pu prendre des photographies et des vidéos de l'entrée du site et de ses abords immédiats, avant de repartir en voiture.

L'officier de sécurité du site a été averti seulement deux jours après l'incident par un salarié qui sortait du site au moment des faits mais qui ne les avait pas immédiatement signalés. En consultant les caméras de sécurité qui entourent le site, l'officier de sécurité a été en mesure de recueillir quelques indications générales concernant le véhicule. Toutefois, la faible résolution des images n'a pas permis d'identifier l'individu ou de lire la plaque d'immatriculation. La société n'a pas souhaité déposer plainte.

COMMENTAIRES

Les opérations de repérage comportent souvent plusieurs étapes, qui peuvent être menées par plusieurs individus et par le biais de différents vecteurs : un piéton, un véhicule stationné à proximité du site, le survol d'un drone. Elles sont souvent réalisées à des moments où la vigilance est réduite : lors de périodes de congés (juillet et août en particulier), la nuit, ou lors de la pause méridienne plus propice aux nombreux déplacements des salariés.

Dans certains cas, les premières étapes d'une opération de repérage peuvent sembler anodines, à l'image d'un individu qui s'arrêterait devant un bâtiment pour le photographier. Toutefois, la vigilance des services de sécurité face à ces situations est essentielle afin d'être en mesure de retracer, sur une période donnée, la totalité des événements susceptibles de constituer une opération plus large. Ces faits peuvent constituer les actes préparatoires d'un vol simple, d'un vol avec effraction, d'une atteinte à la réputation, d'une démarche d'espionnage ou encore d'une captation de savoir-faire.

Quel que soit le motif du repérage, il constitue une vulnérabilité pour l'entité ciblée et chaque suspicion d'incident doit retenir l'attention, notamment en cas de réitération, et documentée de façon précise.

PRÉCONISATIONS DE LA DGSI

EN AMONT D'UNE OPERATION DE REPERAGE

- **Adapter le dispositif de sécurité du site à la sensibilité des matériels et données qu'il héberge.** La sécurité des locaux passe tout d'abord par la présence d'un service d'accueil ou de sécurité afin d'être en mesure de contrôler les entrées et les sorties, quelle que soit la sensibilité du site. Une atteinte à la réputation peut cibler n'importe quelle entité. En revanche, pour les sites hébergeant des données, matériels ou savoir-faire sensibles, un dispositif de surveillance vidéo doit non seulement permettre de détecter des incidents mais aussi de collecter des éléments de preuve dans la perspective d'une enquête interne ou d'un dépôt de plainte.
- **Sensibiliser régulièrement tous les salariés aux intrusions et aux opérations de repérage.** Bien souvent une intrusion est favorisée par un manque de vigilance, sinon par la complaisance des personnes travaillant dans la société qui peuvent hésiter ou simplement tarder à signaler des situations anormales. Une sensibilisation régulière de tous les salariés est essentielle afin de développer une culture commune de vigilance.
- **Créer ou formaliser une chaîne de sûreté au sein du personnel.** Procéder à l'expression de vos besoins au terme d'une analyse de risque permettant d'identifier les cibles et les valeurs à protéger. Communiquer les moyens de contacts de référents sûreté distinctement identifiés parmi vos salariés et dont les rôles et missions auront été préalablement définis. Formaliser une remontée d'information à ces référents par une procédure facile à mettre en place (courriel, appel, main-courante). Enfin, organiser la prise en charge des visiteurs, de l'annonce de leur

venue, à leur arrivée et prévoir de les faire accompagner par un de vos salariés lors de leur présence dans les locaux.

EN CAS D'INTRUSION SUR LE SITE OU DE REPERAGE A L'EXTERIEUR DU SITE

- **Recueillir et consigner tous les éléments relatifs à l'incident**. Les opérations de repérage sont rarement des cas isolés. Il est donc essentiel de consigner de façon précise et détaillée tous les éléments de contexte relatifs à l'incident et de recueillir une description précise des faits auprès des témoins de l'incident. Dans le cadre des survols de drones, il faudra veiller à consigner la date, la durée et l'heure du survol et chercher à identifier l'appareil ou à le photographier aux fins d'identification ultérieure du modèle, notamment en cas de survols multiples.
- **Intercepter l'individu et recueillir son identité.** Tout individu présent dans des locaux sans motif légitime doit être intercepté et accompagné jusqu'à l'accueil ou le poste de sécurité afin que son identité puisse être relevée et que lui soit signifiée l'interdiction de pénétrer à nouveau sur le site sans autorisation.
- **Signaler l'incident aux autorités.** Même si les faits relevés peuvent sembler anodins, ils peuvent constituer un préalable à une opération de plus grande ampleur. Signaler ces faits aux autorités locales et à la DGSI permet de mieux se prémunir contre une éventuelle tentative de vol ou d'espionnage industriel. La DGSI dispose d'une adresse électronique dédiée : securite-economique@interieur.gouv.fr
- **Un dépôt de plainte** auprès des services de police ou de gendarmerie doit être systématiquement envisagé.