MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH INGÉRENCE ÉCONOMIQUE DGSI #124

Novembre 2026

ENJEUX LIÉS À LA PROTECTION DES INFRASTRUCTURES CRITIQUES



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

ENJEUX LIÉS À LA PROTECTION DES INFRASTRUCTURES CRITIQUES

L'invasion de l'Ukraine par la Russie a profondément déstabilisé le paysage géopolitique mondial. Si le conflit a entraîné la perturbation des chaînes logistiques, des marchés de l'énergie et des approvisionnements, il a également généré des menaces inédites pour les entités dites « critiques ». La découverte d'un drone explosif à l'aéroport de Leipzig (Allemagne) début août 2026, attribué à la Russie, et la multiplication d'attaques cyber visant des infrastructures sensibles en Europe appellent aujourd'hui à la plus grande vigilance. Si le contexte international venait à s'aggraver, les actions déstabilisatrices et offensives à l'encontre des intérêts français pourraient ainsi se multiplier.

Parce qu'elles concourent à la production et à la distribution de biens ou services indispensables au fonctionnement de l'économie, et donc à la continuité de la vie de la Nation, les infrastructures critiques sont susceptibles d'être particulièrement ciblées par des actions clandestines, orchestrées sous le seuil d'un conflit militaire ouvert et visant directement à punir les alliés de l'Ukraine.

Pour les entreprises, la menace se traduit par des risques concrets de sabotages physiques de leurs installations ou de leurs réseaux, d'attaques cybernétiques paralysantes, et d'un espionnage industriel agressif.

Ce flash ingérence met en lumière plusieurs types d'atteintes ayant ciblé des infrastructures critiques en France, illustrant le niveau élevé de la menace, et la nécessité, pour les entreprises, de renforcer la sûreté et la sécurité de leurs installations.

1 LES TENTATIVES DE CARTOGRAPHIE DES INFRASTRUCTURES CRITIQUES

EXEMPLE

À plusieurs reprises, en pleine nuit, un drone a été détecté visuellement au-dessus d'infrastructures stratégiques par le service sûreté du site concerné. Le drone, équipé de capteurs optiques, répétait les mêmes mouvements, puis opérait un positionnement stationnaire pendant plusieurs minutes, avant de s'éloigner à vitesse rapide. Le système de détection des drones, présent sur le site, n'a pas fonctionné et son pilote n'a pas pu être appréhendé.

COMMENTAIRE

De telles actions de survols de drones peuvent paraître anodines ou décorrélées du contexte international. Néanmoins, elles peuvent aussi être destinées à cartographier les infrastructures stratégiques, évaluer leurs dispositifs de sécurité, de réaction et de décision, ou encore intimider les personnels en présence.

RECOMMANDATIONS

Prévenir les actions de repérage

- Adapter le dispositif de sécurité du site à la sensibilité des matériels et données qu'il héberge. 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, afin de développer une culture commune de vigilance.

En cas d'incident

- Recueillir et consigner tous les éléments relatifs à l'incident, notamment auprès des témoins de l'incident. Dans le cadre des survols de drones, consigner la date, la durée et l'heure du survol, et chercher à identifier l'appareil ou à le photographier à des fins d'identification ultérieure du modèle ;
- 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

2 LES SABOTAGES

EXEMPLE 1

Une entreprise stratégique a subi plusieurs actes de malveillance. Après un départ de feu d'origine criminelle à proximité de son atelier de production, deux inondations, issues de sabotages, ont été constatées dans le même périmètre, quelques jours plus tard. Ces évènements étaient accompagnés de lettres anonymes menaçant certains salariés.

EXEMPLE 2

Une entreprise évoluant dans un secteur particulièrement stratégique et hautement concurrentiel a constaté trois sabotages de produits qu'elle commercialise à l'étranger, dans un court intervalle de temps. En amont de leur livraison au client, plusieurs composants électriques avaient été sectionnés et dissimulés dans les produits, empêchant ainsi leur bon fonctionnement.

COMMENTAIRE

Les sabotages ont pour objectif de déstabiliser des entités opérant dans des secteurs stratégiques, en portant atteinte à leurs capacités de production et à leurs installations. Dans la sphère civile, les entreprises menant des activités duales et celles considérées comme essentielles à la continuité de la vie de la Nation sont particulièrement exposées aux sabotages, notamment dans un contexte géopolitique tendu.

RECOMMANDATIONS

Prévenir les atteintes aux biens :

- Effectuer un audit de sûreté bâtimentaire. La DGSI peut proposer ce type de prestations visant à émettre des recommandations sur la mise en œuvre de mesures de sûreté cohérentes avec la configuration des locaux ;
- Mettre en place des mesures élémentaires d'ordre organisationnel visant à contrôler les accès aux différents espaces ;
- Envisager d'installer un système de détection d'intrusion pour protéger l'intérieur des locaux ;
- Réévaluer périodiquement les processus de sécurité ;
- En cas de risques identifiés, s'informer sur le dispositif d'Opération tranquillité entreprises et commerce (OTEC), qui permet à l'entité de bénéficier d'un suivi renforcé par les forces de police ou de gendarmerie.

Prévenir les atteintes aux personnes :

- Sensibiliser les personnels aux menaces et à leur détection. Encourager la réduction de l'exposition d'informations personnelles sur Internet et les réseaux sociaux ;
- Si la fonction n'existe pas, désigner un responsable sûreté et formaliser une procédure de traitement des signalements émanant des personnels ;
- Encadrer le déplacement des personnels les plus exposés aux risques.

En cas de menace ou d'incident :

- Déposer plainte auprès des services de police ou de gendarmerie. Le dépôt de plainte permet d'initier des investigations judiciaires ; la victime peut se prévaloir de ce statut auprès des services de l'État et bénéficier d'un accompagnement adapté ;
- Mettre en place un dispositif d'accompagnement des victimes ;
- Contacter la DGSI afin de signaler l'incident à l'adresse securite-economique@interieur.gouv.fr

3 LES INTRUSIONS

EXEMPLE 1

Trois personnes se sont introduites dans un site protégé après avoir découpé une partie du grillage du portillon d'entrée. Elles ont escaladé l'un des bâtiments, testé l'ouverture de plusieurs portes et pris des photographies à différents endroits. Elles ont quitté le site peu avant l'arrivée d'un prestataire, semblant indiquer qu'elles avaient connaissance des horaires habituels des différentes personnels dans l'entreprise.

EXEMPLE 2

Un prestataire effectuant des missions de sous-traitance est intervenu sur le site d'une entité stratégique pour installer des équipements informatiques. Il a été retrouvé par un agent de sécurité, seul, sur une partie sensible du site, téléphone en main, après l'heure de départ autorisée. Le lendemain matin, alors qu'il n'était pas censé revenir, il s'est à nouveau présenté au poste de sécurité et a demandé avec insistance à entrer sur le site, sans succès.

COMMENTAIRE

Les intrusions sur site peuvent parfois sembler anodines ou sans aucun lien avec les tensions internationales ou l'actualité géopolitique. Toutefois, il est essentiel de ne pas les sous-estimer, d'y prêter une attention soutenue et de prendre des mesures afin de prévenir toute récidive. Si les infrastructures stratégiques (réseaux d'énergie, de transport, de télécommunications, opérateurs vitaux, etc.) sont des objectifs aisément identifiés, la DGSI constate que le champ des cibles potentielles s'étend à une multitude d'entités à l'image de laboratoires, de sous-traitants d'entités sensibles, de sites industriels ou encore de sites logistiques. Ces différentes entités, souvent moins protégées ou acculturées à ces enjeux sécuritaires, peuvent présenter un ratio risque/avantage intéressant pour la conduite d'actions d'ingérence.

RECOMMANDATIONS

À titre préventif :

- Effectuer des tests d'intrusion physique pour évaluer le dispositif de sûreté et, au besoin, renforcer les protections extérieures du site ;
- Identifier les éléments, matériels et installations à protéger prioritairement et renforcer la protection de leurs accès ;
- Formaliser une remontée d'information aux référents sûreté ;
- Organiser la prise en charge des visiteurs et intervenants extérieurs, de l'annonce de leur venue à leur arrivée physique sur site, puis, lors de leurs déplacements au sein des locaux, en prévoyant de les faire accompagner par des membres du personnel.

En cas d'incident :

- Intercepter les auteurs des intrusions et recueillir leur identité. Tout individu présent dans des locaux sans motif légitime doit être interpellé 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 ;
- Un dépôt de plainte auprès des services de police ou de gendarmerie doit être systématiquement effectué. Même si les faits relevés peuvent sembler anodins, ils peuvent constituer un préalable à une opération de plus grande ampleur ;
- Signaler l'incident à la DGSI à l'adresse securite-economique@interieur.gouv.fr

4 LES ATTEINTES AUX SYSTÈMES D'INFORMATION

EXEMPLE 1

Un établissement d'enseignement supérieur et de recherche a été victime d'une intrusion informatique pendant la période estivale. Le responsable de la sécurité des systèmes d'information a déterminé que la cyberattaque avait permis la compromission et l'extraction du contenu de plusieurs centaines de messageries des personnels de l'établissement. Or, cet établissement héberge des laboratoires qui comportent plusieurs zones à régime restrictif (ZRR) encadrées par le dispositif de protection du potentiel scientifique et technique de la nation (PPST).

EXEMPLE 2

Plusieurs infrastructures stratégiques ont fait l'objet de cyberattaques simultanées. Leurs auteurs ont pu prendre le contrôle des infrastructures à distance, mettant en danger la sécurité des personnels présents sur les sites. Si tous les personnels ont pu être mis en sécurité, ces attaques ont provoqué des dégâts matériels et ont ralenti la production durant toute la durée de leur commission.

COMMENTAIRE

Aujourd'hui, les acteurs de l'ingérence sont particulièrement présents dans le cyberespace. Ils disposent d'importants moyens et leur savoir-faire est éprouvé. Leurs attaques sont destinées à déstabiliser les infrastructures et entreprises stratégiques par divers moyens : en leur extorquant de l'argent, en paralysant leur activité, en provoquant des destructions matérielles, en nuisant à leur réputation ou encore en utilisant les données exfiltrées à des fins de ciblage pour la mise en œuvre d'autres modes opératoires.

La DGSI constate régulièrement des lacunes dans la sécurité des systèmes d'information de nombreuses structures, non seulement pour des raisons financières mais aussi par défaut de prise en compte des risques cybernétiques et de leur impact potentiel sur la vie économique de leur structure. Cette vulnérabilité des réseaux informatiques accroît le risque de ciblage d'opportunité par des cyberattaquants.

Face à ces menaces, la DGSI, en lien avec ses partenaires nationaux, notamment l'Agence nationale de la sécurité des systèmes d'information (Anssi), propose d'accompagner les jeunes entreprises à travers une prestation de conseil en sécurité des systèmes d'information.

RECOMMANDATIONS

Prévenir les risques cybernétiques

- Identifier les évènements les plus critiques pour la sécurité du système d'information et activer la journalisation de ceux-ci sur les équipements et applications sensibles, afin de pouvoir identifier et investiguer les dysfonctionnements ou/et les incidents de cybersécurité ;
- Nommer un référent sécurité des systèmes d'information (RSSI) qui aura pour mission d'être l'interlocuteur privilégié sur les questions liées à la sécurité du système, de sensibiliser les utilisateurs et d'effectuer ponctuellement des contrôles sur l'application des bonnes pratiques SSI ;
- Formaliser dans un document écrit les bonnes pratiques relatives à la sécurité des systèmes d'information qui devront être mises en œuvre par les personnels. Celui-ci pourra servir de base à l'établissement d'une politique de sécurité des systèmes d'information ;
- Définir une politique d'application des mises à jour des composants du système d'information, des procédures associées mais également de sauvegarde des composants et données les plus critiques afin de pouvoir restaurer le service en cas d'attaque informatique ;
- Renforcer la perception des risques informatiques auprès de l'ensemble des personnels, par exemple en conduisant des campagnes de tests de type « tentative d'hameçonnage », « ingénierie sociale » et « tests d'intrusion red team », destinées à évaluer leurs réactions face à divers scénarios d'attaques informatiques ;
- Effectuer un audit de sécurité informatique (ex : « audit de configuration », « test d'intrusion ») en privilégiant un prestataire de service de confiance, afin d'identifier et corriger les vulnérabilités de son système d'information.

En cas de cyberattaque

- Contacter immédiatement le service chargé de la sécurité des systèmes d'information ;
- Isoler le ou les systèmes victimes de l'attaque, pour limiter la propagation ;
- Identifier l'origine de l'attaque et son étendue, afin de pouvoir effectuer des corrections ;
- Déposer plainte auprès des services de police ou de gendarmerie compétents. Il est également conseillé de conserver des preuves de l'attaque pour compléter le dépôt de plainte ;
- Prendre attache avec la Commission nationale de l'informatique et des libertés (Cnil), si l'attaque informatique a permis la consultation, la modification ou la destruction de données personnelles ;
- Contacter la DGSI afin de signaler tout incident à l'adresse securite-economique@interieur.gouv.fr

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité