MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

FLASH DGSI #90

JANVIER 2023

INGÉRENCE ÉCONOMIQUE

ILLUSTRATION D'UNE PERTE D'UN MARCHÉ À LA SUITE DE DÉMARCHES INTRUSIVES DE CLIENTS ÉTRANGERS

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

ILLUSTRATION D'UNE PERTE D'UN MARCHÉ À LA SUITE DE DÉMARCHES INTRUSIVES DE CLIENTS ÉTRANGERS

La DGSI détecte régulièrement des situations dans lesquelles une relation commerciale établie entre un acteur économique français et un partenaire étranger conduit, au bout de quelques années, à une perte de marché ou de savoir-faire au détriment de la partie française. Certains acteurs étrangers parviennent ainsi à capter des informations sensibles, susceptibles d'être ensuite utilisées dans le cadre d'un projet industriel concurrent en France ou à l'étranger.

Ce flash illustre la manière dont une société française a été écartée d'un marché à la suite de démarches intrusives et déloyales, menées sur plusieurs années, par ses clients étrangers. Ceux-ci ont cherché à tirer profit de la volonté de la société française d'accroître sa présence sur un marché étranger pour obtenir des informations sensibles sur ses méthodes de production, et utiliser abusivement sa dénomination commerciale afin de la remplacer sur le marché visé.

PREMIÈRE PHASE

Une entreprise française spécialisée dans la sous-traitance industrielle au profit de nombreux secteurs a vendu plusieurs exemplaires de ses équipements de haute qualité en France et à l'international. Bénéficiant d'un positionnement reconnu sur son secteur et d'une bonne réputation, l'entreprise française a été démarchée par une société étrangère, se proposant de commercialiser ses produits sur un marché étranger. Dans la perspective de ce partenariat, l'entreprise française lui a ainsi vendu plusieurs équipements.

Toutefois, cet intermédiaire s'est révélé être un sous-traitant industriel cherchant en réalité à assurer son propre développement commercial sur le même marché étranger que l'entreprise française. Usurpant l'identité de l'entreprise française à son insu, le sous-traitant étranger est allé jusqu'à déposer un brevet basé sur la technologie française dans son pays.

En outre, il a exigé à plusieurs reprises, pour le compte de sa propre clientèle locale, des informations sur la technologie de la société française, des envois d'échantillons et des précisions sur les modalités d'installation et de maintenance des équipements.

Face à ces agissements, la société française a mis un terme à toute relation commerciale avec ce client étranger et décidé de ne plus répondre à ses sollicitations.

DEUXIÈME PHASE

Quelques mois plus tard, un second intermédiaire originaire du même pays que le premier a également commandé des équipements à la société française pour le compte d'un groupe industriel étranger. À la suite de la livraison de cette commande, l'intermédiaire est resté plusieurs années en relation avec la société française en lui promettant de futurs contrats aux volumes conséquents, toujours au profit du même groupe industriel.

Au cours de ces échanges, l'intermédiaire a pu accéder à des informations techniques précises sur la composition des équipements de la société française et a également obtenu l'identité de certains sous-traitants clés. Certains éléments demandés par l'intermédiaire laissaient supposer une tentative de rétro-ingénierie sur les équipements de l'entreprise française.

TROISIÈME PHASE

Quelques années après sa première et unique commande, le second intermédiaire a informé la société française que son donneur d'ordre ne procéderait finalement à aucune nouvelle commande, préférant privilégier une entreprise locale à une entreprise française.

Cette décision a suscité l'incompréhension de la société française, notamment compte tenu du fait que l'entreprise locale choisie par l'industriel étranger ne disposait d'aucune notoriété sur le plan international.

La société française a finalement constaté quelques mois plus tard que l'entreprise locale qui lui avait été préférée par le groupe industriel, fournissait des équipements en tous points similaires aux siens, l'excluant de fait, de ce marché étranger.

COMMENTAIRES

Dans le cadre de ses relations commerciales sur ce marché étranger, l'entreprise française semble avoir été instrumentalisée à des fins de captation technologique. En effet, le faible nombre d'équipements commandés et le caractère intrusif des questions techniques posées lors des échanges commerciaux laissent supposer que la rétro-ingénierie était l'objectif premier recherché par son concurrent.

Sous couvert d'une commande, des acteurs économiques étrangers peuvent chercher à développer ou à améliorer une offre concurrente à partir des produits reçus. Ces démarches déloyales peuvent nuire au développement international des sociétés qui en sont victimes. Confrontées ainsi à des pertes de marché, elles peuvent également voir leur réputation affectée en cas de vente de produits similaires, de moindre qualité, commercialisés sous une dénomination commerciale usurpée.

PRÉCONISATIONS DE LA DGSI

EN AMONT D'UNE COMMANDE AVEC TOUT NOUVEAU CLIENT

- **Évaluer l'honorabilité et les intentions du futur client.** En raison des risques de captation technologique par le biais d'un acte de rétro-ingénierie, il est essentiel d'étudier l'honorabilité de tout nouveau client (réputation, existence de litiges passés et identification des partenaires précédents) avant de conclure une vente ou d'envoyer un prototype. Les intermédiaires commerciaux doivent notamment faire l'objet d'une vigilance renforcée, et leurs donneurs d'ordre doivent être préalablement identifiés. Il peut également être utile d'interroger très précisément le futur client sur la destination et l'utilisation exacte des produits commandés, afin d'anticiper toute risque d'utilisation inappropriée pouvant porter préjudice à la société.
- **Déterminer les informations sensibles ne devant pas être communiquées.** Préalablement à toute réponse à des sollicitations émanant d'un client, il est primordial d'identifier l'ensemble des informations essentielles à la préservation du savoir-faire de l'entreprise et de son avance technologique (données techniques d'un produit, identité des sous-traitants, etc.) qu'il conviendra de ne jamais communiquer. Pour tenter de les obtenir, des acteurs mal intentionnés peuvent formuler des promesses de nouveaux contrats sans avoir l'intention de les honorer.
- **Prévoir, dans chaque contrat de vente, des clauses de protection du potentiel technologique, industriel et commercial de la société**, ainsi que des mesures permettant de sanctionner le client en cas d'utilisation abusive du produit commandé. Il convient par ailleurs d'évaluer la possibilité de déposer des brevets et marques, en France et à l'étranger, afin de protéger juridiquement ses droits et sa propriété intellectuelle.

EN CAS DE SOUPÇONS DE CAPTATION TECHNOLOGIQUE OU DE DÉTOURNEMENT D'UNE COMMANDE PAR UN CLIENT

- **Mettre en place une veille permanente sur sa propre marque et ses produits.** Ce type de veille permet de détecter de façon précoce toute utilisation abusive d'une marque ou d'un produit par des acteurs tiers, notamment par des concurrents étrangers, et de réunir des éléments de preuve permettant de caractériser le préjudice subi.
- **S'assurer régulièrement du strict respect de l'ensemble des conditions et des obligations incombant au client dans le contrat de vente.** En cas d'incident survenu à l'étranger, après avoir tenté une résolution à l'amiable avec le client, évaluer la possibilité d'une mise en demeure, voire de poursuites auprès des autorités judiciaires locales.
- **Se désengager de toute relation avec un client déloyal**. Il convient également de sensibiliser ses salariés, voire ses partenaires commerciaux nationaux, à la nécessité de ne plus collaborer avec ce client et ses représentants.
- **Signaler tout soupçon de démarches déloyales de la part de clients étrangers aux services de l'État compétents.** La DGSI dispose d'une adresse électronique dédiée : securite-economique@interieur.gouv.fr

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE
DGSI

FLASH DGSI #91

FÉVRIER 2023

INGÉRENCE ÉCONOMIQUE

LES RISQUES LIÉS AUX VISIOCONFÉRENCES

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

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

FLASH DGSI #91
FÉVRIER 2023

INGÉRENCE ÉCONOMIQUE

LES RISQUES LIÉS AUX VISIOCONFÉRENCES

Depuis la crise sanitaire de 2020, l'utilisation d'outils de travail à distance s'est généralisée. Le développement du télétravail a fortement augmenté le nombre des réunions effectuées à distance. Ces échanges sont l'occasion d'évoquer en interne des sujets souvent sensibles (recherche et développement, projets de de restructuration, etc.) mais également de rencontrer des acteurs étrangers dans le cadre de négociations ou de partenariats.

Dans ce contexte, les acteurs économiques et scientifiques français sont amenés à utiliser davantage de programmes et d'applications non protégés, dont des plateformes de visioconférence, des messageries instantanées et des solutions de partage de documents. Or, plusieurs de ces outils présentent d'importantes failles de sécurité, propices à la fuite, voire à la captation de données personnelles ou d'informations stratégiques. Les entités françaises qui ont recours à ces outils sont par ailleurs davantage exposées aux risques cyber, tels que les escroqueries ou les usurpations d'identité.

PREMIER EXEMPLE

Le comportement suspect d'une salariée étrangère expose son employeur à un risque de captation de ses données sensibles.

L'encadrement d'une salariée étrangère a découvert, peu après l'arrivée de cette dernière dans la société française, qu'elle ne disposait pas des compétences nécessaires pour remplir ses fonctions et a alors adapté ses tâches, sans succès. Profitant de la souplesse de la direction de sa société, cette cadre de l'entreprise a décidé unilatéralement de travailler presque exclusivement en télétravail, malgré des consignes imposant à l'ensemble des salariés un temps de travail effectué à 50 % en présentiel.

Lors de ses réunions de travail auxquelles elle participe en visioconférence, la salariée étrangère désactive systématiquement sa caméra et a, à plusieurs reprises, déclenché l'enregistrement vidéo des réunions portant sur des sujets sensibles comme la stratégie d'innovation. Interrogée par sa hiérarchie sur cette pratique, elle a prétexté enregistrer les réunions pour des collègues qui ne pouvaient pas assister aux réunions. Ce comportement suspect inquiète la société puisque la salariée a accès à distance à des informations stratégiques, dont la captation pourrait bénéficier à un concurrent ou à une puissance étrangère.

DEUXIÈME EXEMPLE

Une entreprise française se voit imposer une réunion en visioconférence suspecte avec des acteurs étrangers dans le cadre d'un projet de création de coentreprise.

Rachetée par un consortium de groupes étrangers, une société française spécialisée dans la conception de dispositifs médicaux a signé un partenariat industriel avec l'un de ses nouveaux actionnaires pour la création d'une coentreprise basée hors du territoire national. Dans le cadre des négociations liées à ce projet, effectuées en visioconférence, la société française a été invitée à s'entretenir avec une autorité étrangère, dont les représentants ne lui avaient pas été présentés par ses partenaires et dont les visages étaient floutés. À cette occasion, les interlocuteurs étrangers ont exigé qu'un salarié de l'entreprise française, récemment arrivé, présente sa pièce d'identité devant la caméra, active la géolocalisation de son téléphone et filme les locaux de la société afin de prouver qu'il se trouvait bien au siège de l'entité française.

La société française rencontre aujourd'hui des tensions dans son partenariat avec ces acteurs étrangers et est confrontée au transfert accéléré de sa technologie à l'étranger. La coentreprise s'est avérée n'être qu'une création juridique sans activité économique, les actionnaires étrangers ayant sous-traité l'assemblage des produits français à d'autres intervenants.

TROISIÈME EXEMPLE

Une structure scientifique française est exposée à une vidéo à caractère terroriste lors d'une visioconférence.

À l'occasion d'une réunion d'information effectuée en visioconférence, un institut de recherche spécialisé dans l'agroalimentaire a été victime d'une intrusion de son système d'information en raison de la faible sécurité du service utilisé. Peu après le début de la réunion, des individus ont en effet pris le contrôle de l'application en s'appropriant les droits d'animateurs, puis ont diffusé une vidéo à caractère terroriste montrant des images de décapitation.

L'inscription à la visioconférence était libre d'accès en ligne et aucun contrôle n'a été effectué. En outre, le niveau de sécurité du mot de passe de l'application était de faible intensité.

COMMENTAIRES

Face à la généralisation du télétravail, l'utilisation de services de visioconférence est devenue systématique alors que les acteurs économiques et scientifiques ont tendance à négliger les risques, numérique et économique, liés à ce type de réunion.

Certaines personnes peuvent tirer profit de ces échanges pour capter des informations. Une vigilance accrue doit donc être portée aux réunions à distance à la fois avec les collaborateurs internes et externes, y compris de confiance. Une attention particulière doit notamment être portée lors des réunions à distance pour lesquelles l'identité des participants n'est pas contrôlée, lorsque des individus n'apparaissent pas à l'écran ou enregistrent des conversations sans prévenir

ou encore lorsque des personnes sont conviées aux réunions au dernier moment sans annonce préalable.

Enfin, les pratiques de bonne conduite en matière de sécurité informatique doivent également être appliquées lors de ces échanges à distance. Des fragilités informatiques peuvent en effet être exploitées et exposer les entités à des risques susceptibles d'affecter la pérennité de leur activité ou leur réputation.

PRÉCONISATIONS DE LA DGSI

BONNES PRATIQUES À APPLIQUER EN MATIÈRE DE SÉCURITÉ INFORMATIQUE ET DE PROTECTION DES INFORMATIONS SENSIBLES

EN MATIÈRE DE PROTECTION ÉCONOMIQUE :

- **Identifier les données sensibles de l'entreprise auxquelles un acteur externe ne doit pas avoir accès et dont la fuite pourrait porter préjudice à la société**. Il est essentiel d'identifier de façon précise toutes les données considérées comme sensibles et vitales pour la préservation du savoir-faire de l'entreprise. Il conviendra ensuite de les classer en fonction de leur niveau de sensibilité et d'assurer un contrôle sur leur accès. Il sera ainsi pertinent de privilégier les réunions en présentiel pour évoquer les sujets les plus stratégiques et sensibles de la société, plutôt que les visioconférences.
- **Les employés doivent être sensibilisés à la nécessité de signaler toute situation inhabituelle menaçant le savoir-faire de la société** : manquement ou comportement déloyal d'un salarié, d'un stagiaire ou d'un prestataire, suspicion de transfert ou de détournement de technologies, etc.
- **En anticipation d'une fuite d'informations sensibles, effectuer une cartographie des risques permettant d'évaluer les conséquences pour la société, ses clients et ses partenaires.** Veiller notamment à la neutralité du cadre du lieu de la réunion et aux informations qui pourraient être visibles des autres participants.

EN MATIÈRE DE SÉCURITÉ INFORMATIQUE :

- **Effectuer de façon régulière et planifiée les mises à jour des systèmes d'exploitation et des programmes informatiques**. Les mises à jour ont vocation à corriger les failles qui facilitent les intrusions informatiques.
- **Utiliser un mot de passe de session pour les visioconférences avec des participants extérieurs, et générer un lien de session différent à chaque réunion.**
- **Inclure les logiciels de visioconférence dans les audits de sécurité informatique** pour une analyse des risques et une correction des vulnérabilités.

- **Impliquer les responsables de la sécurité des systèmes d'information (RSSI) dans l'encadrement de la pratique du télétravail**. Ce dispositif doit prévoir la mise à disposition d'outils adéquats, dont notamment du matériel dédié à l'usage professionnel, des applications et des moyens de connexions sécurisés assurant la confidentialité des échanges. Les collaborateurs doivent être accompagnés et formés à l'utilisation des outils mis à leur disposition. La signature d'une charte de respect des règles de bonne conduite doit également être envisagée. L'agence nationale de la sécurité des systèmes d'informations (Anssi) et la commission nationale de l'informatique et des libertés (Cnil) publient régulièrement des guides de bonnes pratiques et de conseils à respecter afin de réduire les risques cyber dans le cadre du télétravail.
- **Privilégier des solutions de visioconférence comprenant un chiffrement par défaut, idéalement du chiffrement de bout en bout**. L'Anssi recommande par exemple l'application française de visioconférence chiffrée de bout en bout, Tixeo. L'utilisation d'une solution de visioconférence non qualifiée par l'Anssi augmente les possibilités d'ingérence et les risques liés aux réglementations étrangères extraterritoriales portant sur les données numériques.

DANS LE CADRE DE REUNIONS AVEC DES ACTEURS ÉTRANGERS

- **Faire preuve de fermeté en cas d'incident.** Certains membres de délégations étrangères sont susceptibles de fortement insister auprès des structures françaises pour les pousser à déroger aux règles de sécurité. Il peut être pertinent de solliciter les services d'un avocat pour bénéficier de conseils juridiques en cas d'incident.
- **Accorder une attention particulière à la préparation des rencontres avec le partenaire, qu'il soit potentiel ou déjà connu**. En amont de la réunion, il est recommandé de recueillir le maximum d'informations sur les participants à la réunion afin d'évaluer leur stratégie et leurs intentions. Il est important d'avoir la liste complète des participants à la réunion afin d'être capable de les identifier. Enfin, il convient d'exercer une vigilance particulière en cas d'ajout de dernière minute d'un visiteur non identifié. Ces individus sont en effet susceptibles d'être des représentants de sociétés concurrentes, voire des agents des services de renseignement étrangers.
- **Alerter les services de l'État compétents et la DGSI (securite-economique@interieur.gouv.fr)** de tout comportement d'un individu ou d'une entité, en particulier étranger, susceptible de remettre en cause la pérennité de votre activité ou de conduire à des faits de captation d'informations sensibles. La DGSI peut fournir des recommandations en cas d'incident informatique ou impliquant des acteurs étrangers.

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

FLASH DGSI #92

MARS 2023

INGÉRENCE ÉCONOMIQUE

RISQUES D'ESCROQUERIES PAR DES ACTEURS SE PRÉSENTANT COMME DES FONDS D'INVESTISSEMENT

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

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

FLASH DGSI #92
MARS 2023

INGÉRENCE ÉCONOMIQUE

RISQUES D'ESCROQUERIES PAR DES ACTEURS SE PRÉSENTANT COMME DES FONDS D'INVESTISSEMENT

Les sociétés qui rencontrent des difficultés financières ou les start-up qui lèvent des fonds peuvent être sollicitées par des fonds d'investissement étrangers formulant des propositions financières attractives.

Des acteurs se présentent parfois comme des fonds d'investissement étrangers, en utilisant des identités fictives ou en usurpant des identités réelles. Ils exposent les entreprises qu'ils ciblent à d'importants risques financiers et d'atteinte à leur réputation et à leurs savoir-faire.

PREMIER EXEMPLE

Des individus usurpent l'identité d'un fonds d'investissement étranger dans le but d'escroquer une entreprise française.

Une société française a lancé une campagne de levée de fonds en communiquant sur les réseaux sociaux professionnels et la presse spécialisée. Un fonds d'investissement étranger a pris attache avec la société pour lui proposer un prêt sous forme d'obligations convertibles aux conditions très avantageuses, en contrepartie duquel il a uniquement été demandé à la société française la création d'un fonds commun de créance[1] dans le pays d'origine de l'investisseur pour procéder au transfert des fonds.

L'entreprise française s'est étonnée qu'aucune autre demande particulière n'ait été formulée par le fonds avant l'opération, notamment la réalisation d'un audit de la société. Les soupçons de la société ont été renforcés lorsque les représentants du fonds ont refusé de communiquer par visio-conférence.

Souhaitant vérifier l'honorabilité du fonds d'investissement, l'entreprise française a alors constaté qu'un message de prudence apparaissait sur le site internet du fonds indiquant qu'il ne contactait jamais les entreprises directement. La société française a pris conscience qu'elle avait été victime d'une tentative

[1] Special purpose vehicle *en anglais, il s'agit d'un véhicule de financement dont le seul objectif est d'acquérir les créances selon une procédure simplifiée.*

d'escroquerie et que des individus avaient usurpé l'identité du fonds d'investissement en créant des adresses de messagerie électronique dont le libellé était proche de celles du fonds d'investissement.

DEUXIÈME EXEMPLE

Une start-up française placée en redressement judiciaire après avoir été victime d'une escroquerie menée par un fonds d'investissement étranger fictif.

Une start-up française a lancé une levée de fonds de plusieurs millions d'euros. Elle a été contactée par un fonds d'investissement étranger qui, après plusieurs échanges par téléphone et par courrier électronique, a annoncé vouloir participer à la levée de fonds. Le dirigeant de la société française a été invité à se déplacer dans le pays du fonds d'investissement pour signer le contrat de financement.

Une fois sur place et alors que le dirigeant de la start-up devait être reçu par les investisseurs, les représentants du fonds ont prétexté une indisponibilité et ne se sont jamais présentés. Ils ont toutefois invité la société française à s'acquitter de plusieurs types de frais, en espèces et par virement bancaire.

Le fonds d'investissement s'était ensuite engagé à partager une partie de certaines dépenses administratives avant de signaler à la start-up qu'une institution bancaire avait fait opposition à son virement. À la demande du fonds, la société française s'est donc acquittée du restant de ces frais à un agent de recouvrement indiqué par le fonds étranger.

Face à cette multiplication des demandes de versements, la start-up s'est rapprochée des services de l'État qui lui ont indiqué qu'il s'agissait d'une escroquerie élaborée par un fonds d'investissement fictif, établi dans un paradis fiscal avec une domiciliation commune à de nombreuses autres entreprises, et que les individus avaient en parallèle usurpé l'identité d'employés de réelles structures financières étrangères. Ayant subi un préjudice financier de plusieurs dizaines de milliers d'euros et n'ayant pas pu récupérer les sommes versées, la start-up française a été placée en redressement judiciaire.

COMMENTAIRES

Lorsque les entreprises victimes d'escroqueries sont des structures de petite taille, les conséquences de telles démarches sur leur stabilité financière peuvent être importantes, jusqu'à remettre en cause leur pérennité. Les start-up et petites entreprises sont rarement dotées de directions juridiques ou financières à même de les conseiller ou de détecter des indices d'une escroquerie.

Dans certains cas, la combinaison d'usurpations d'identités réelles et de création de fausses structures peut rendre l'identification de l'escroquerie difficile à déceler.

Outre le préjudice financier qui peut être subi par les entreprises victimes d'escroqueries, ces situations peuvent ralentir un processus de levée de fonds, rendre la société vulnérable à propositions financières peu avantageuses ou à des tentatives d'ingérence d'acteurs étrangers intéressés par leurs savoir-faire ou technologies.

Par ailleurs, ce type d'escroqueries peut amener les entreprises à communiquer des données stratégiques, qui pourraient être utilisées au profit de concurrents.

PRÉCONISATIONS DE LA DGSI

BONNES PRATIQUES À ADOPTER POUR SE PRÉMUNIR DES ESCROQUERIES

- **Avoir un usage prudent des réseaux sociaux, même professionnels**. Les réseaux sociaux sont une source d'information pour les individus mal intentionnés. Il est recommandé d'être prudent sur la nature des informations partagées et de faire preuve d'une vigilance renforcée vis-à-vis des approches réalisées exclusivement par le biais des réseaux sociaux.
- **Se renseigner sur l'honorabilité de l'investisseur**. Des vérifications élémentaires peuvent être réalisées par l'entreprise, à commencer par une lecture attentive du site Internet de l'investisseur, une consultation des profils des dirigeants et une vérification de sa domiciliation.
- **Privilégier les rencontres physiques préalablement à tout engagement et, à défaut, exiger au moins un échange en visio-conférence**. Lors d'échanges dématérialisés, une vigilance particulière doit être portée au nom de domaine employé par ses interlocuteurs et à sa bonne concordance avec le nom de l'entreprise qu'ils disent représenter. Un refus des interlocuteurs de toute rencontre ou de se présenter par le biais d'une visio-conférence doit être un élément d'alerte à prendre en compte.
- **Appliquer les procédures de façon stricte, sans dérogation.** Les acteurs malveillants cherchent à tirer profit de la méconnaissance des procédures juridiques et financières internationales de jeunes entreprises pour leur porter atteinte. Il est impératif de se renseigner sur les procédures locales et de ne pas céder à des impératifs d'urgence qui pourraient être avancés par ses interlocuteurs. L'application stricte des procédures permet d'éviter le paiement de frais supplémentaires.
- **Plusieurs services de l'État peuvent être sollicités afin de s'assurer de l'honorabilité d'un interlocuteur financier :** réseau des délégués à l'information stratégique et à la sécurité économiques (DISSE), directions régionales de l'économie, de l'emploi, du travail et des solidarités (DREETS), réseau international de la direction générale du Trésor implanté à l'étranger, etc. La DGSI peut également être sollicitée.

EN CAS D'IDENTIFICATION D'UNE ESCROQUERIE

- **Mettre fin aux échanges avec le partenaire**. Mettre rapidement un terme aux échanges lors d'une tentative d'escroquerie permet de limiter son exposition aux risques de captation de données et d'atteinte à la réputation.
- **Sensibiliser ses salariés**. Sensibiliser en priorité les services chargés de la gestion juridique et financière de l'entreprise, mais aussi l'ensemble des salariés, afin de limiter les risques liés à d'éventuelles approches directes des acteurs malveillants auprès d'autres interlocuteurs dans l'entreprise.
- **Signaler les faits à la DGSI**. Particulièrement lorsqu'elles se manifestent dans le cadre d'une levée de fonds, ces escroqueries peuvent cibler plusieurs entreprises stratégiques sur une même

période de temps. La DGSI pourra sensibiliser en retour ses interlocuteurs aux risques présentés par un acteur identifié comme malveillant.

- **Déposer plainte auprès des services locaux de police ou de gendarmerie.** Même en l'absence de tout préjudice, cette démarche permet de signaler ces agissements, de procéder à des recoupements et d'identifier ainsi leurs auteurs en caractérisant leurs modes opératoires. En cas de préjudice, elle sera le préalable à toute procédure d'indemnisation engagée auprès des banques ou assureurs. Il est conseillé de joindre aux déclarations tous les éléments justificatifs (journaux de connexions, messageries échangées, coordonnées bancaires) permettant de prouver l'escroquerie.

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.

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

FLASH DGSI #94

MAI 2023

INGÉRENCE ÉCONOMIQUE

VOLS DE DONNÉES COMMIS PAR DES SALARIÉS EN FIN DE CONTRAT

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

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

FLASH DGSI #94

MAI 2023

INGÉRENCE ÉCONOMIQUE

VOLS DE DONNÉES COMMIS PAR DES SALARIÉS EN FIN DE CONTRAT

La fin d'une relation de travail, qui peut survenir à la suite d'un licenciement, d'une démission, d'une rupture conventionnelle, d'un départ à la retraite ou d'une fin de contrat, peut induire des vulnérabilités pour l'employeur. Qu'il soit volontaire ou imposé, anticipé ou imprévu, le départ d'un collaborateur peut conduire à des comportements condamnables visant à déstabiliser l'entité, notamment par le vol de données stratégiques.

Des salariés sur le départ peuvent dérober des données de leur ancienne entreprise pour de multiples raisons. Ils peuvent s'emparer d'informations critiques afin de les monétiser, de les utiliser pour le compte de leur nouvel employeur, pour le développement de leur carrière ou pour la création d'une d'entreprise concurrente ou bien par volonté de vengeance voire de dénonciation. D'autres vols s'apparentent à de l'opportunisme, le salarié voulant récupérer des éléments qu'il a produit sans véritable intention de nuire. Les informations ainsi obtenues ne sont plus protégées et sont plus facilement exposées à des risques de détournements par des acteurs malveillants.

PREMIER EXEMPLE :

Captation de données d'une société dans le domaine de la santé par un collaborateur étranger dont le contrat n'a pas été renouvelé. Au cours de la nuit précédant son dernier jour de contrat, un collaborateur de nationalité étrangère d'une société sensible du secteur de la santé a accédé à plusieurs dizaines de fichiers confidentiels depuis son domicile grâce à l'outil de contrôle à distance mis en place pour faciliter le télétravail. Confronté aux faits par sa hiérarchie le lendemain matin, alors qu'il venait rendre son badge d'accès, le salarié a reconnu avoir cherché des dossiers pour les exploiter dans le cadre de son futur emploi. Son contrat n'ayant pas été renouvelé, la société a soupçonné son salarié d'avoir agi par vengeance et a porté plainte pour captation de données.

DEUXIÈME EXEMPLE :

Peu avant son départ, un cadre d'une société française, débauché par un concurrent étranger, a procédé à un vol de données stratégiques. Un cadre de haut niveau, employé depuis 30 ans dans un

grand groupe industriel français, a mis fin à sa collaboration dans le cadre d'une rupture conventionnelle afin de rejoindre l'un de ses principaux concurrents étrangers. Lors de son départ, le salarié a procédé à la suppression de ses messages électroniques professionnels et de ses données hébergées sur son espace de travail, ainsi qu'au transfert de celles-ci vers un support de stockage externe. Propriétés de la société, ces données techniques et commerciales étaient considérées comme extrêmement sensibles et strictement confidentielles. En outre, elles recouvrent le périmètre sur lequel le salarié évolue désormais au sein de la société concurrente.

Le jour de son départ, le salarié a par ailleurs été surpris par un de ses supérieurs en train de charger dans son véhicule un grand nombre de dossiers en format papier comportant des données financières et juridiques. Interrompu dans cette opération, la société a récupéré l'intégralité de ces dossiers. Après avoir envoyé plusieurs courriers à l'ex-salarié et à son nouvel employeur, et avoir fait constater les faits par un huissier, la société française a déposé plainte.

TROISIÈME EXEMPLE :

Un employé en *freelance*, dont le contrat a été résilié prématurément, s'introduit dans le système d'information d'une société du secteur du numérique et télécharge des données sensibles. Un consultant employé en *freelance* depuis quelques mois par un groupe français du numérique a attiré l'attention de sa hiérarchie par des comportements suspects et des manipulations inhabituelles alors qu'il effectuait des missions au sein de la direction des systèmes d'information et bénéficiait de droits d'utilisateur étendus. Sa hiérarchie a alors pris la décision de rompre prématurément son contrat. Après sa résiliation, le salarié ne s'est pas présenté au rendez-vous fixé par son employeur afin de restituer son matériel informatique et son badge d'accès. La nuit suivante, bénéficiant de droits informatiques toujours valides, il a consulté des ressources internes et téléchargé des données particulièrement sensibles de la société. Celle-ci a porté plainte et va renforcer les mesures de protection (procédures d'habilitation, droits informatiques, sensibilisation) à l'égard du personnel temporaire et des sous-traitants.

COMMENTAIRES

Agissant délibérément dans l'illégalité, certains employés sur le départ prennent le risque de voler des informations appartenant à leur employeur. Ces actions sont souvent synonymes de perte de savoir-faire pour les sociétés victimes ainsi que d'importants préjudices financiers et commerciaux.

Généralement découvert tardivement, à un stade où il n'est plus possible de collecter des preuves, le vol de données est particulièrement difficile à caractériser, ne permettant ainsi pas toujours aux actions en justice entreprises d'aboutir.

PRÉCONISATIONS DE LA DGSI

PRÉVENIR LE VOL DE DONNÉES SENSIBLES PAR DES SALARIÉS

- **Identifier les données sensibles à protéger.** Il est essentiel d'identifier de façon précise toutes les données considérées comme sensibles pour la préservation du savoir-faire de l'entreprise, notamment les documents en lien avec la propriété intellectuelle. Il s'agit de les répertorier, de les classer et de les stocker en fonction de leur niveau de sensibilité afin de limiter leur accès.
- **Hiérarchiser les accès informatiques au sein de la société en fonction de chaque profil de salarié.** Il s'agit de strictement limiter l'accès aux données de la société aux besoins précis de chaque salarié.
- **Adopter une politique de sécurité des données informatiques et veiller à son application.** Il est possible de mettre en place des règles strictes de sécurité informatique afin de limiter l'exfiltration de données, comme l'interdiction d'envoyer des informations sensibles à des comptes de messagerie personnels ou d'utiliser des dispositifs de stockage comme les clés USB. Le changement systématique des mots de passe des comptes partagés à chaque départ de collaborateurs est également à privilégier. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) propose sur son site internet un cadre de gouvernance de la sécurité des données.
- **Surveiller le comportement des utilisateurs sur le réseau de l'entreprise en mettant en place des moniteurs de surveillance des bases de données.** La mise en place d'un outil d'audit doté de fonctionnalités de collecte de journaux et de production de rapports est indispensable pour maîtriser l'activité des utilisateurs. Ils aident notamment à identifier les salariés ayant accédé à certains types de données, à déterminer le nombre de fois où un utilisateur spécifique a essayé d'accéder à des dossiers, etc.

LORS DU DÉPART D'UN COLLABORATEUR

- **Le jour du départ, s'assurer que le salarié a restitué l'ensemble de ses clés d'accès et matériels.** La société peut prévoir une liste récapitulant les éléments que le salarié devra rendre lors de son départ afin de s'assurer que ce dernier n'a conservé aucun matériel de l'entreprise. Elle garantit ainsi la désactivation des accès de l'ancien salarié et la protection des données sensibles de la société.

EN CAS DE VOLS DE DONNÉES CONSTATÉS

- **Obtenir des preuves claires en collaboration avec l'équipe dédiée à la sécurité informatique de la société.** Le fait de voler les données de son entreprise est constitutif de plusieurs délits. Afin d'apporter des éléments qui pourront être utiles à l'enquête, des preuves tangibles peuvent être rassemblées notamment par le constat d'un huissier de justice.
- **Déposer plainte auprès des services de police ou de gendarmerie, ou directement auprès du procureur de la République.** En cas de vols de données dans des conditions suspectes, le dépôt

de plainte peut permettre d'établir la matérialité des faits et à la société d'obtenir réparation sous la forme de dommages et intérêts.

- **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
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

FLASH DGSI #95

JUIN 2023

INGÉRENCE ÉCONOMIQUE

LES RISQUES ASSOCIÉS AUX CAPTATIONS DE SAVOIR-FAIRE DANS LA RECHERCHE FONDAMENTALE

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

LES RISQUES ASSOCIÉS AUX CAPTATIONS DE SAVOIR-FAIRE DANS LA RECHERCHE FONDAMENTALE

De nombreux États étrangers, exerçant un contrôle étroit sur les activités de leurs établissements de recherche, ont élaboré des objectifs scientifiques accordant une part essentielle à la recherche fondamentale.

Le caractère théorique et expérimental propre à la recherche fondamentale et l'absence d'application immédiate de ses travaux peuvent être perçus par certains chercheurs comme excluant tout enjeu stratégique en termes de concurrence scientifique ou de protection économique. Reconnue internationalement pour son excellence, la recherche fondamentale française est pourtant ciblée régulièrement par des acteurs étrangers qui cherchent à s'approprier sans contrepartie son savoir-faire afin de combler leur retard scientifique et technologique.

Des universités étrangères peuvent ainsi proposer des échanges et des partenariats en recherche fondamentale plutôt qu'en recherche appliquée afin de dissimuler les applications envisagées, en particulier lorsque celles-ci ont une finalité militaire pour le développement d'armes conventionnelles ou de destruction massive. Elles peuvent également chercher à acquérir le socle de connaissances nécessaires au développement, en toute autonomie, d'applications technologiques civiles dans des secteurs stratégiques et porteurs.

PREMIER EXEMPLE

Multiples tentatives de captation d'équipements de pointe dédiés à la recherche fondamentale et développés par un laboratoire français

Spécialisé dans la recherche fondamentale dans le domaine de la physique, un laboratoire français a développé des équipements qui suscitent depuis plusieurs années l'intérêt d'une université étrangère.

Celle-ci a tenté par divers moyens d'accéder à cette technologie. Elle a tout d'abord envoyé un de ses scientifiques en détachement dans l'une des équipes du laboratoire ayant accès aux équipements concernés. Une fois les liens établis entre les chercheurs français et le scientifique, l'université étrangère a formulé de nombreuses propositions pour obtenir les plans d'installation des équipements.

Face au refus du laboratoire, l'université étrangère a approché un ancien chercheur à la retraite ayant contribué à la mise en place des équipements, en lui proposant des rémunérations avantageuses en échange du transfert de son savoir-faire. Le scientifique ayant refusé, l'université étrangère a alors proposé de conclure un partenariat officiel visant à dupliquer les équipements dans son pays, moyennant d'importantes rétributions.

Au-delà des conséquences d'un transfert de technologie pour l'attractivité du laboratoire français, les applications que le laboratoire étranger aurait été susceptible de développer présentaient également un risque majeur. En effet, celui-ci était spécialisé dans des recherches à caractère dual, présentant un risque élevé que le laboratoire français ne participe, de manière indirecte, au programme militaire d'un pays étranger. Face à ces constats, un avis défavorable au projet de duplication a été émis par le ministère de l'enseignement supérieur et de la recherche.

DEUXIÈME EXEMPLE

Un doctorant étranger installe un logiciel espion dans un ordinateur de son laboratoire pour capter des données de recherche fondamentale.

Un doctorant étranger a installé et utilisé pendant une longue période un logiciel espion dans l'ordinateur centralisant les données sensibles de son unité de recherche, spécialisée dans la recherche fondamentale en chimie. Agissant à l'insu des autres chercheurs, le doctorant a notamment utilisé le logiciel pour transférer un grand nombre de données sur son ordinateur personnel et a régulièrement accédé au laboratoire en dehors des horaires d'accès autorisés.

Interrogé par la direction du laboratoire, le doctorant n'a pas justifié son comportement. Les données extraites disposaient d'applications possibles à court terme dans le domaine de la recherche médicale. Une fois son doctorat obtenu, le chercheur étranger a été recruté par une prestigieuse université étrangère pour travailler sur les applications de son domaine de recherche fondamentale étudié en France.

TROISIÈME EXEMPLE

Une université militaire étrangère initie un partenariat en recherche fondamentale avec une université française avant de développer plusieurs coopérations officieuses en recherche appliquée.

Spécialisée dans une discipline de pointe couvrant la recherche fondamentale et appliquée, un laboratoire français a développé des partenariats avec plusieurs structures étrangères. L'une d'entre elles se démarque en particulier pour sa très forte implication dans le programme militaire de son pays et est défavorablement connue de la DGSI pour le caractère intrusif de ses démarches à l'égard de plusieurs acteurs de la recherche française.

Le laboratoire français a limité le partenariat à la recherche fondamentale afin de prévenir tout accès de l'université étrangère aux données les plus sensibles de la recherche appliquée. Les relations entre les deux parties ont alors pris la forme d'échanges scientifiques ponctuels.

L'université étrangère a cependant tiré profit des liens établis dans la recherche fondamentale pour développer d'autres canaux de coopération avec la structure française en recherche appliquée. Le laboratoire français a accueilli l'année suivante un doctorant de la même université dont les sujets de recherche avaient une forte portée duale. Parallèlement, l'université étrangère a facilité les collaborations scientifiques informelles entre chercheurs sur les mêmes sujets de recherche, sans aucun contrôle du laboratoire français.

COMMENTAIRES

Les risques de captations étrangères en recherche fondamentale sont souvent sous-estimés en comparaison avec la recherche appliquée. Certains domaines de la recherche fondamentale peuvent toutefois trouver des applications à court ou moyen termes et faire l'objet d'une exploitation par des acteurs étrangers.

En outre, l'exploitation du produit de la recherche fondamentale à des fins militaires peut faire peser un risque important sur la réputation et le rayonnement international de structures de recherche françaises, susceptibles d'avoir contribué, à leur insu, au développement de programmes étrangers, même plusieurs années après un partenariat en recherche fondamentale.

Dans certains cas, les propositions de partenariat en recherche fondamentale peuvent être destinées à rassurer le partenaire français sur les intentions de la partie étrangère et constituent un prélude à des coopérations, parfois officieuses, en recherche appliquée.

PRÉCONISATIONS DE LA DGSI

EN AMONT DE TOUT PARTENARIAT

- **Mener une réflexion sur les risques de détournement à des fins militaires des recherches menées.** Pour encadrer le risque de captation des savoirs en cours de développement, il est nécessaire de pouvoir analyser, à chaque étape du processus de recherche, leurs potentiels détournements à des fins militaires, commerciales ou stratégiques.
- **Sensibiliser tout le personnel du laboratoire aux enjeux de protection du potentiel scientifique et technique de la Nation (PPST), quel que soit leur objet d'étude**. À la demande d'établissements ou d'organismes de recherche, la DGSI dispense régulièrement des conférences de sensibilisation dédiées au monde de la recherche qui démontrent, en s'appuyant sur des cas réels, les risques d'ingérence étrangère auxquels peuvent être exposés les chercheurs français.
- **Assurer un niveau de sûreté bâtimentaire et informatique suffisant.** Les captations de données sont souvent facilitées par un faible niveau de sûreté bâtimentaire et informatique. Le contrôle des accès informatiques de tout chercheur étranger, quel que soit son domaine de travail, est essentiel afin de pouvoir prévenir ou détecter toute captation indue de données.
- **Demander une évaluation des risques au regard du dispositif de PPST.** Le ministère de tutelle du laboratoire peut être sollicité pour une évaluation des risques qu'un détournement ou une captation de recherches d'un laboratoire engendrerait. Cette évaluation porte sur l'étude de quatre risques : les atteintes aux intérêts économiques de la Nation, le renforcement des arsenaux militaires étrangers ou l'affaiblissement des capacités de défense de la Nation, la contribution à la prolifération des armes de destruction massive et de leurs vecteurs, l'utilisation à des fins terroristes sur le territoire national.

- **Envisager la création de zones à régime restrictif (ZRR).** À l'issue d'une évaluation, le laboratoire peut demander la création d'une ZRR auprès de son ministère de tutelle. Celle-ci offre une protection administrative et juridique à la zone définie, qui peut concerner tout ou partie du laboratoire, et permet d'exercer un contrôle réglementaire des accès à la ZRR afin d'écarter les profils jugés les plus risqués pour le laboratoire et ses savoir-faire.

DANS LE CADRE D'UN PARTENARIAT

- **Identifier les domaines de recherche appliquée conduite par l'établissement étranger.** Même si le partenariat envisagé ne concerne que des activités de recherche fondamentale, les savoirs acquis peuvent être utilisés dans le cadre de recherches appliquées. En vérifiant les domaines de recherche appliquée de son potentiel partenaire, la structure française peut ainsi veiller à ce que ses recherches ne soient pas détournées au profit d'un programme militaire d'un État étranger.
- **Structurer le partenariat.** Des acteurs étrangers peuvent mobiliser différents canaux de coopération, officiels et officieux, afin d'acquérir de manière plus discrète les savoirs désirés. Structurer le partenariat de manière contractuelle et sensibiliser les chercheurs français à la nature de leurs échanges avec le partenaire étranger est un moyen efficace de se prémunir de toute captation indue de savoir-faire.
- **Signaler tout incident au fonctionnaire de sécurité et de défense de l'établissement, au ministère de rattachement de l'établissement et à la DGSI.** Si un membre du laboratoire enfreint de manière répétée la réglementation interne, signaler son comportement à la DGSI peut permettre de se prémunir contre un détournement des savoirs du laboratoire. De même, si une université étrangère se démarque par une volonté d'entrisme marquée et durable, il est recommandé de le signaler. La DGSI dispose d'une adresse électronique dédiée : securite-economique@interieur.gouv.fr

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

FLASH DGSI #96

SEPTEMBRE 2023

INGÉRENCE ÉCONOMIQUE

UNE SOCIÉTÉ FRANÇAISE INNOVANTE CONFRONTÉE À DES ACTIONS ÉTRANGÈRES DE CAPTATION TECHNOLOGIQUE

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

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

FLASH DGSI #96

SEPTEMBRE 2023

INGÉRENCE ÉCONOMIQUE

UNE SOCIÉTÉ FRANÇAISE INNOVANTE CONFRONTÉE À DES ACTIONS ÉTRANGÈRES DE CAPTATION TECHNOLOGIQUE

Dans les premières années suivant leur création, les sociétés françaises dotées d'un fort potentiel d'innovation sont particulièrement exposées aux marques d'intérêt étrangères. Si certaines approches visent à soutenir le développement de ces sociétés dont la technologie est prometteuse, d'autres ont pour objectif de capter les savoir-faire ou d'entraver le développement des sociétés ciblées.

Ce flash ingérence met en avant plusieurs problèmes auxquels a été confrontée une start-up industrielle française développant des produits de pointe. Plusieurs acteurs étrangers ont en effet cherché, sans se concerter et parfois simultanément, à capter les technologies de l'entreprise à différents stades de son développement.

PREMIER CAS

Peu après sa création, la start-up industrielle française s'est adjoint les services de plusieurs revendeurs mandatés pour remporter de nouveaux contrats. L'un de ces intermédiaires a profité de sa présence dans les locaux de la société pour dérober un prototype de la société française afin de déposer un brevet à son nom sans autorisation.

La start-up a alors engagé une procédure judiciaire en référé afin de mettre un terme aux agissements déloyaux de son revendeur. Ce dernier a alors menacé de divulguer des informations stratégiques de la société et d'utiliser les plans qu'il avait en sa possession pour reproduire les mêmes produits à l'étranger. Il a également initié une campagne de dénigrement auprès des principaux partenaires et clients de la société. À l'origine de l'annulation de plusieurs commandes, cette campagne a engendré des pertes financières importantes pour la start-up.

Après avoir obtenu gain de cause à l'issue des procédures judiciaires, la start-up française a poursuivi son développement à l'international.

DEUXIÈME CAS

Alors qu'elle débutait son activité en France et à l'international, la start-up a rencontré des difficultés dans la vente de ses produits sur un marché étranger, pourtant prometteur, où la concurrence était encore peu développée.

Les appels d'offres locaux imposaient en effet aux sociétés étrangères des exigences, notamment s'agissant de la localisation de la chaîne de production. Ne pouvant remplir l'ensemble des conditions, la start-up a été contrainte de se limiter à des partenariats avec des sociétés locales. Elle a dû en outre s'associer à un revendeur local autorisé, dans le cadre d'un contrat de maintenance conclu entre les deux sociétés, à démonter ses produits.

En parallèle, la start-up a été régulièrement approchée par des fonds d'investissement originaires de ce même pays qui lui promettaient un accès facilité à ce marché en contrepartie d'une prise de participation, leur donnant des droits sur sa propriété intellectuelle.

TROISIÈME CAS

Toujours à la même période, la start-up française s'est vue proposer par une société, située dans un autre pays étranger, d'y distribuer ses produits. Les négociations se sont avérées difficiles en raison du manque de cohérence de ce partenaire potentiel, qui n'a cessé de revoir à la baisse le prix d'achat et la quantité de produits souhaités au fil des discussions.

Face au risque d'échec de ces discussions commerciales, le dirigeant de la société étrangère a finalement proposé d'acquérir, à un prix particulièrement élevé, des parts de la start-up française, voire de la racheter intégralement. Méfiante vis-à-vis de cette offre financière jugée peu crédible, la start-up a décliné cette proposition.

Quelques mois plus tard, un autre représentant de la société étrangère a soumis à la start-up française une nouvelle offre de rachat d'un montant encore plus élevé, conditionnée cette fois à l'obtention d'un échantillon de sa technologie. L'insistance dont ont fait preuve les représentants de la société étrangère a conduit la start-up française à rompre tout contact avec elle.

COMMENTAIRES

Le cas de cette start-up industrielle démontre la diversité d'approches et de situations auxquelles peut être confrontée une jeune société cherchant à se développer à l'international. À plusieurs étapes de son développement, son savoir-faire et sa propriété intellectuelle ont été menacés sous différentes formes : vol de matériel, proposition de prise de participation au capital, rétro-ingénierie, offre de rachat.

Ces tentatives de captation technologique illustrent l'attrait que peuvent susciter les start-up industrielles françaises et le niveau élevé de risques d'ingérences étrangères auxquelles elles peuvent être exposées dès les premières étapes de leur développement, à un stade où ses dirigeants sont souvent peu préparés à de telles actions.

PRÉCONISATIONS DE LA DGSI

RECOMMANDATIONS FACE AU RISQUE DE CAPTATION DE SAVOIR-FAIRE DANS LE CADRE DE PARTENARIATS

- **Évaluer l'honorabilité de ses partenaires potentiels.** Des vérifications approfondies (ou *due diligence*) visant à recueillir tout élément sur le partenaire envisagé permettront d'évaluer ses intentions et d'anticiper une tentative d'ingérence.
- **Accorder une attention particulière à la préparation des rencontres avec le partenaire potentiel.** Dans le cadre de rencontres formelles et informelles, il convient notamment de s'assurer de ne pas fournir prématurément des informations stratégiques. Il faut notamment veiller à instaurer des mesures de protection physique et numérique en cas d'accueil du partenaire dans les locaux de la société.
- **Être vigilant lors de la rédaction des contrats de partenariat et de leur éventuelle révision.** Toute promesse formulée par le partenaire dans le cadre des négociations devra être formalisée dans un document signé entre les deux parties afin de pouvoir s'en prévaloir en cas de non-respect ultérieur de ces engagements. Il s'agira d'être particulièrement attentif aux clauses relatives au transfert de savoir-faire et de technologie.
- **Délimiter clairement les pouvoirs des mandataires à l'occasion de signatures de contrats commerciaux**.

RECOMMANDATIONS FACE À LA CONCURRENCE D'UN ACTEUR ÉTRANGER CIBLANT LE SAVOIR-FAIRE DE LA SOCIÉTÉ

- **Mettre en place une veille stratégique active (technologique, juridique, concurrentielle, etc.) afin d'assurer un suivi de son domaine d'activité**. Une veille active doit permettre de détecter tout changement, présent ou futur, pouvant affecter son environnement économique et pouvant constituer un risque pour la pérennité de son activité.
- **Recenser et classer ses données en fonction de leur niveau de sensibilité afin d'en assurer un meilleur suivi et une meilleure sécurisation**. Il s'agit notamment d'identifier les informations stratégiques auxquelles ont accès les salariés et de détecter les éventuelles vulnérabilités de la société.
- **Déposer plainte auprès des services de police, de gendarmerie ou auprès du procureur de la République**, pour tout vol de données ou de matériels.

RECOMMANDATIONS GÉNÉRALES

- **S'assurer régulièrement du strict respect de l'ensemble des conditions et des obligations imposées au partenaire dans l'exécution du contrat, notamment concernant le respect de la propriété intellectuelle.**
- **Recourir rapidement aux services d'un conseil juridique en cas de litige avéré ou soupçonné avec l'un de ses partenaires.**
- **Alerter les services de l'État de toute tentative de captation d'informations sensibles.** La DGSI dispose d'une adresse électronique dédiée et se tient à la disposition des start-up industrielles

pour les accompagner dans leurs problématiques liées à l'ingérence économique étrangère : securite-economique@interieur.gouv.fr

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

FLASH DGSI #97

OCTOBRE 2023

INGÉRENCE ÉCONOMIQUE

LES SALONS PROFESSIONNELS, SOURCES DE VULNÉRABILITÉS POUR LES ENTREPRISES

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

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

FLASH DGSI #97

OCTOBRE 2023

INGÉRENCE ÉCONOMIQUE

LES SALONS PROFESSIONNELS, SOURCES DE VULNÉRABILITÉS POUR LES ENTREPRISES

Si les salons professionnels, en France et à l'étranger, offrent de nombreuses opportunités commerciales pour les entreprises, ils peuvent également constituer une source de vulnérabilités. La DGSI est régulièrement informée de faits d'ingérence dont ont été victimes des acteurs économiques français lors de ces évènements.

Les salons internationaux sont amenés à accueillir un très grand nombre de visiteurs et représentent une occasion privilégiée pour des acteurs offensifs de cibler des entreprises ou des individus, et de mener des démarches intrusives. Les sociétés participantes sont notamment susceptibles d'être visées par des captations de technologie ou de savoir-faire, des tentatives de débauchage ou de se voir proposer des partenariats déséquilibrés.

PREMIER EXEMPLE

Lors d'un salon professionnel organisé sur le territoire national, un industriel français a été ciblé par une tentative d'espionnage technologique.

Dès la première journée d'un salon professionnel, les représentants d'un industriel français ont identifié la présence inhabituelle devant leur stand d'un groupe de ressortissants étrangers prétendant être journalistes pour un média spécialisé. Ces individus ont notamment tenté de réaliser, à l'insu des représentants de l'industriel, des prises de vue de la technologie présentée sur le stand par l'intermédiaire d'une caméra dissimulée.

Après avoir contrôlé ces individus, la direction sûreté du salon leur a demandé d'effacer l'ensemble des photos prises sur le stand. Informée de cet incident, la DGSI a relevé l'identité des ressortissants étrangers et a veillé à ce que leurs badges d'accès au salon leur soient retirés.

DEUXIÈME EXEMPLE

Une entreprise française participant à un salon international a été victime d'une dégradation de son matériel lors du passage aux douanes étrangères.

Dans le cadre de sa participation à un salon international, une société française a expédié par avion le matériel qu'elle souhaitait exposer.

Lors de la réception du matériel, les représentants de la société ont constaté que l'une des caisses de transport, contrôlée par les douanes étrangères, avait fait l'objet d'une dégradation, laissant soupçonner une tentative d'identification du contenu. Le matériel a toutefois été récupéré sans traces apparentes de dégradation, puis exposé sur le salon.

La direction de la société redoute une tentative d'espionnage technologique par les douanes étrangères.

TROISIÈME EXEMPLE

Une start-up française a été victime du vol de son matériel en raison d'une négligence.

Dans le cadre de leur participation à un salon international, les représentants d'une start-up française ont été invités, le dernier jour du salon, à une réception en soirée organisée par d'autres exposants de nationalité étrangère. Les représentants de la start-up n'ont pas pu entreposer leur matériel dans les espaces protégés dédiés avant de quitter leur stand ; ceux-ci ayant déjà été fermés par l'organisateur. Ils ont alors décidé de le laisser sur place, dissimulé à l'arrière de leur stand, sans autre mesure de protection.

Le lendemain, le matériel avait disparu. Les représentants de la start-up se sont rapprochés de l'organisateur afin que les caméras de vidéosurveillance soient consultées, mais ces dernières avaient été déconnectées. La start-up n'a pas pu récupérer le matériel qui avait été exposé lors du salon et redoute un vol malveillant dans le but de mener une action de rétro-ingénierie.

COMMENTAIRES

Chaque étape de la participation à un salon professionnel doit faire l'objet d'une attention soutenue : le simple fait de disposer d'un stand sur un salon permet déjà à des acteurs étrangers offensifs de procéder au ciblage d'une entité considérée comme stratégique. La technologie présentée sur le salon peut ainsi être captée dès le passage frontière lorsque le salon est situé à l'étranger.

Si la captation de technologie ou de savoir-faire d'entreprises stratégiques est le principal objectif d'acteurs étrangers lors de ces évènements, ceux-ci peuvent également chercher à déstabiliser un concurrent par le biais d'atteintes informatiques ou de tentatives de débauchages de profils qualifiés présents sur le stand.

Les exposants peuvent être approchés par des profils variés (journalistes, étudiants, exposants, concurrents, services de renseignement, etc.) et être la cible de différents actes de malveillance (vols, questions intrusives, connexions non autorisées de clés USB au matériel exposé, etc.).

Dans ce contexte, la participation à un salon professionnel doit faire l'objet d'une préparation minutieuse, couvrant à la fois les aspects liés à la protection physique du stand, à la prévention des vols, à la sécurité informatique et à la sensibilisation de tous les individus présents sur le stand.

PRÉCONISATIONS DE LA DGSI

EN AMONT DU SALON

- **Analyser l'environnement du salon**. Étudier la disposition du stand attribué sur le salon par rapport aux stands environnants et identifie les potentiels concurrents.
- **Préparer des éléments de langage à utiliser en fonction des interlocuteurs**. Définir un ensemble de sujets qui peuvent être abordés, tels que ceux qui sont utiles à l'entreprise d'un point de vue commercial, et ceux qui doivent être évités. Il est utile de concevoir un plan de communication (brochure, documentation technique ou commerciale, etc.) spécifique à ce type d'évènement afin de limiter la diffusion d'informations sensibles. Préparer sur le stand un emplacement permettant d'échanger avec des clients ou prospects en toute discrétion.
- **Assurer la protection des produits stratégiques.** Retirer les éléments sensibles des matériels les plus stratégiques afin de les rendre inutilisables en cas de vol ou de limiter les pertes, technologiques et financières, en cas de dégradation, notamment lors du transit vers le lieu du salon. Envisager l'acquisition de vitrines sécurisées à installer sur place afin de permettre aux clients de visualiser les matériels exposés sans pouvoir les manipuler.
- **Prévoir des appareils numériques nomades dédiés uniquement au salon et aux déplacements (téléphones, ordinateurs, tablettes, clés USB, etc.)**. Ces appareils doivent bénéficier d'une protection informatique (antivirus, *virtual private network* (VPN), chiffrement, etc.) et leur contenu doit se limiter au strict nécessaire. Ne pas connecter les appareils à des clés USB extérieures ou offertes lors du salon, susceptibles de contenir des programmes malveillants.
- **La DGSI propose aux acteurs économiques des conférences de sensibilisation** dédiées à la préparation des grands salons professionnels et dispense à cette occasion des recommandations.

PENDANT LE SALON

- **En matière de sécurité informatique :**
  - Désactiver les fonctions Wi-Fi et *bluetooth* des matériels nomades. Si possible, éviter de se connecter à des réseaux Wi-Fi ouverts sur les lieux du salon ainsi qu'à l'hôtel.
  - Utiliser de préférence des messageries chiffrées pour dialoguer lors du salon.
  - Ne pas préenregistrer les mots de passe dans les navigateurs.
- **Concernant la sécurité du stand** :
  - Ne pas laisser sur le stand les produits et prototypes exposés ainsi que les affaires professionnelles et personnelles sans surveillance. Maintenir si possible une présence continue, y compris lors des pauses déjeuner.
  - Ranger dans un local sécurisé les produits exposés et les documents les plus sensibles en cas d'évacuation inopinée du stand.

- Faire preuve de grande vigilance lors de la dernière journée du salon, journée la plus propice au vol.

- **Face à un interlocuteur trop curieux ou insistant**, rester évasif et utiliser les éléments de langage préparés en amont. Vérifier l'identité d'un interlocuteur avant de répondre à des questions précises et demander systématiquement une carte de visite à tous ceux qui témoignent d'un intérêt pour un produit développé par la société (ces éléments pourront être utiles en cas d'incident).
- **En dehors du salon, notamment à l'hôtel ou lors d'évènements en marge au salon** (dîners, cocktails, conférences, etc.) : conserver les documents et supports sensibles sur soi et ne pas les laisser dans la chambre d'hôtel. Les coffres-forts mis à disposition dans les chambres d'hôtels ne doivent pas être considérés comme des espaces sécurisés.
- **En cas d'incident**, alerter les services de sécurité du salon et rédiger un rapport d'étonnement relatant avec précision les évènements.

À L'ISSUE DU SALON

- **Procéder à un démontage méticuleux du stand** afin de vérifier que l'ensemble des matériels et documents ont bien été récupérés.
- **Demander au service informatique de procéder à une analyse des appareils électroniques** utilisés lors du salon avant de les connecter aux réseaux internes de l'entreprise. Procéder également au changement de tous les mots de passe par précaution.
- **Effectuer une veille active dans la presse et sur Internet** afin d'être en mesure de contrôler les informations susceptibles d'être communiquées en lien avec la participation au salon.
- **En cas de suspicion de captation informationnelle, technologique ou d'approches d'acteurs étrangers intrusifs lors d'un salon professionnel,** contacter la DGSI.

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

FLASH DGSI #98

DÉCEMBRE 2023

INGÉRENCE ÉCONOMIQUE

LES DÉBAUCHAGES, VECTEURS DE DÉSTABILISATION POUR LES ENTREPRISES

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

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

FLASH DGSI #98

DÉCEMBRE 2023

INGÉRENCE ÉCONOMIQUE

LES DÉBAUCHAGES, VECTEURS DE DÉSTABILISATION POUR LES ENTREPRISES

La DGSI identifie régulièrement des cas d'entités françaises déstabilisées à la suite de débauchages conduits par des acteurs étrangers. Ces opérations peuvent aussi bien cibler la majorité du personnel d'une entreprise qu'un seul salarié qui disposerait d'informations stratégiques, d'une expertise ou de compétences rares.

Ce flash illustre les moyens déployés par les acteurs étrangers pour débaucher des salariés dans le but de développer une nouvelle activité, d'acquérir des briques technologiques ou encore de fragiliser un concurrent. Pour la société ciblée, les conséquences peuvent relever de la perte de données stratégiques, de savoir-faire, de clients, ou influer sur son chiffre d'affaires et induire des difficultés de recrutement sur des profils hautement qualifiés.

PREMIER EXEMPLE

Le recours à des démarches déloyales par l'intermédiaire de cabinets de recrutement a permis à un concurrent étranger de débaucher des salariés chez le sous-traitant français d'un secteur stratégique.

Pendant deux ans, une société étrangère a tenté de débaucher, en vain, des salariés de son concurrent français, situé dans la même zone géographique. La société étrangère a eu recours aux services d'un cabinet de recrutement étranger qui a contacté la moitié des salariés de la société française de manière insistante par téléphone, par courrier électronique et sur les réseaux sociaux. Plusieurs salariés ont accepté de passer des entretiens au cours desquels le cabinet de recrutement a dénigré leur employeur actuel et leur a proposé des hausses de salaires supérieures à 20 %. Ils ont également été incités, au moyen d'une prime, à contribuer à des recrutements au sein de leur société.

En l'absence de clause de non-concurrence, plusieurs collaborateurs ont finalement été débauchés. Ces départs ont conduit la société française à arrêter temporairement plusieurs lignes de productions, causant des pertes financières importantes. Une action en justice est envisagée à l'encontre de la société étrangère.

DEUXIÈME EXEMPLE

Après deux refus de rachat par un concurrent étranger, une société française a fait l'objet d'une campagne de débauchages.

Une société française, spécialisée dans un secteur stratégique et disposant de bureaux dans plusieurs pays, a refusé deux propositions de rachat émises par un concurrent étranger. Peu de temps après, deux salariés de la société, reconnus pour leur expertise et n'ayant pas signé de clause de non-concurrence, ont annoncé leur départ au profit de ce concurrent. Alors que les deux anciens salariés avaient conservé leurs matériels informatiques, ils n'ont consenti à les restituer que face à une menace d'une action en justice. Avant leur départ, les deux salariés avaient par ailleurs pris soin de contacter la majorité de leurs clients au sein de la société française afin de les informer de leur changement d'affectation au profit d'un concurrent.

Un troisième salarié, expert technique reconnu dans son domaine, a également été débauché par le même concurrent étranger. Malgré les contraintes liées à la signature d'une clause de non-concurrence, qui ne couvrait qu'une période de six mois, l'expert technique a malgré tout décidé de rejoindre la société étrangère pour un salaire plus attractif.

Le concurrent étranger a également tenté de débaucher cinq autres salariés de la société française, également ciblés pour leurs compétences techniques.

TROISIÈME EXEMPLE

L'implantation en France d'une start-up étrangère à proximité d'acteurs français spécialisés dans le même secteur stratégique facilite les opérations de débauchage.

Des sociétés françaises de pointe, spécialisées dans un secteur stratégique, ont constaté l'implantation récente d'une start-up étrangère à proximité immédiate de leurs sites. La start-up étrangère a rapidement approché des salariés des sociétés françaises en leur promettant des salaires supérieurs de 30 % et des perspectives de mobilité à l'international. Le déménagement de l'une des sociétés françaises dans un autre quartier de la ville, moins accessible et davantage sujet à la délinquance, a également favorisé des débauchages.

Une dizaine de personnes ont été débauchées afin d'occuper des fonctions identiques au sein de la start-up étrangère. Les profils recrutés correspondent à la volonté de la start-up d'internaliser une partie de sa production pour laquelle elle dépend encore des sociétés françaises ciblées.

COMMENTAIRES

Les débauchages de salariés par des concurrents étrangers constituent des facteurs de fragilisation d'une entreprise, en particulier dans des domaines technologiques de pointe où les profils recherchés sont rares.

Les entreprises de petite taille sont particulièrement menacées. Outre des moyens juridiques, informatiques et en ressources humaines généralement limités en comparaison avec

des acteurs économiques de plus grande importance, les conséquences de débauchages au sein de ces structures peuvent être particulièrement préjudiciables, jusqu'à menacer leur pérennité.

Le droit du travail encadre la pratique du débauchage. Certains comportements peuvent engager la responsabilité du nouvel employeur, comme de l'ancien salarié, devant un tribunal. De même, si la justice estime que le nouvel employeur a contribué à la désorganisation de la société ciblée, des condamnations peuvent être prononcées et des réparations demandées.

PRÉCONISATIONS DE LA DGSI

ANTICIPER LES RISQUES DE DÉBAUCHAGES

- **Conduire de façon régulière une cartographie de ses concurrents.** Il peut notamment s'avérer utile d'identifier les concurrents qui procèdent à des acquisitions de compétences dans son secteur d'activité et qui affichent publiquement leurs démarches de recrutement. Il est également nécessaire d'identifier les méthodes de recrutement de ses concurrents, et leurs potentiels intermédiaires à l'image des cabinets de recrutement. Cette cartographie peut notamment se révéler utile en amont de l'ouverture d'un nouveau site ou d'un déménagement.
- **Anticiper les situations à risques telles que les tensions internes entre salariés ou avec leur hiérarchie.** Des situations de conflit en interne dans l'entreprise peuvent précipiter le départ de salariés en les rendant plus réceptifs à une tentative de débauchage. Un concurrent peut aussi chercher à se renseigner sur l'existence de tensions en interne afin de cibler les salariés les plus à même de quitter l'entreprise.
- **Prévenir le vol d'informations sensibles et la perte de clients**. Il convient d'identifier et de répertorier toutes les informations stratégiques de l'entreprise afin d'être en mesure d'en limiter l'accès à un nombre réduit de salariés, en fonction de leurs besoins. Par ailleurs, la consultation de ces données doit pouvoir être retracée numériquement en interne. Les fichiers qui recensent les clients de l'entreprise doivent notamment faire l'objet d'une vigilance renforcée afin qu'ils ne soient pas copiés ou expédiés vers l'extérieur.
- **S'assurer d'une protection juridique suffisante lors de la rédaction des contrats d'embauche**. Différents leviers juridiques permettent de limiter les débauchages. La présence d'une clause de non-concurrence, d'une durée suffisante, est indispensable pour se protéger des débauchages, ou en limiter les conséquences. La clause de non-sollicitation du personnel avec un client, un cabinet de recrutement, ou tout autre co-contractant, est un autre levier possible qui réduit les risques de débauchages. Enfin, la clause de confidentialité permet de se prémunir de fuites de données, voire de pertes de clients.

EN CAS DE TENTATIVE DE DÉBAUCHAGE OU DE CAS AVÉRÉ

- **Solliciter le service juridique de l'entreprise ou un cabinet d'avocat**. Une assistance juridique peut permettre de mettre un terme à une opération de débauchage, avant même le premier recrutement. À défaut, des procédures judiciaires peuvent entraîner une condamnation de

l'entreprise responsable voire du salarié débauché, et impliquer des indemnisations en réparation du préjudice subi. De telles procédures peuvent également s'avérer dissuasives pour d'autres concurrents qui pourraient s'intéresser aux salariés de l'entreprise à l'avenir. Plusieurs arrêts de la Cour de cassation ont été rendus sur des cas de débauchage.

- **S'assurer de la restitution effective de tous les supports numériques et documentaires d'un salarié à son départ.** Il est essentiel de prévoir un document écrit, énumérant tous les documents et supports numériques que le salarié devra remettre à son ancien employeur le jour de son départ. Cela permet de s'assurer que l'ancien salarié ne dispose plus d'informations stratégiques et n'est pas en mesure de les transmettre à un tiers. Ses accès informatiques doivent également être immédiatement désactivés.
- **Obtenir des preuves des agissements commis par les anciens salariés**. Le fait de voler des données de son entreprise est constitutif de plusieurs délits. Toute preuve matérielle ou numérique qui sera rassemblée par l'entreprise pourra être utile dans le cadre de l'enquête.
- **Déposer plainte auprès des services de police ou de gendarmerie, ou auprès du procureur de la République**. En cas de vols de données ou de débauchage dans des conditions déloyales, le dépôt de plainte peut permettre d'établir la matérialité des faits, avant une éventuelle condamnation pouvant mener à des réparations.
- **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.