



MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

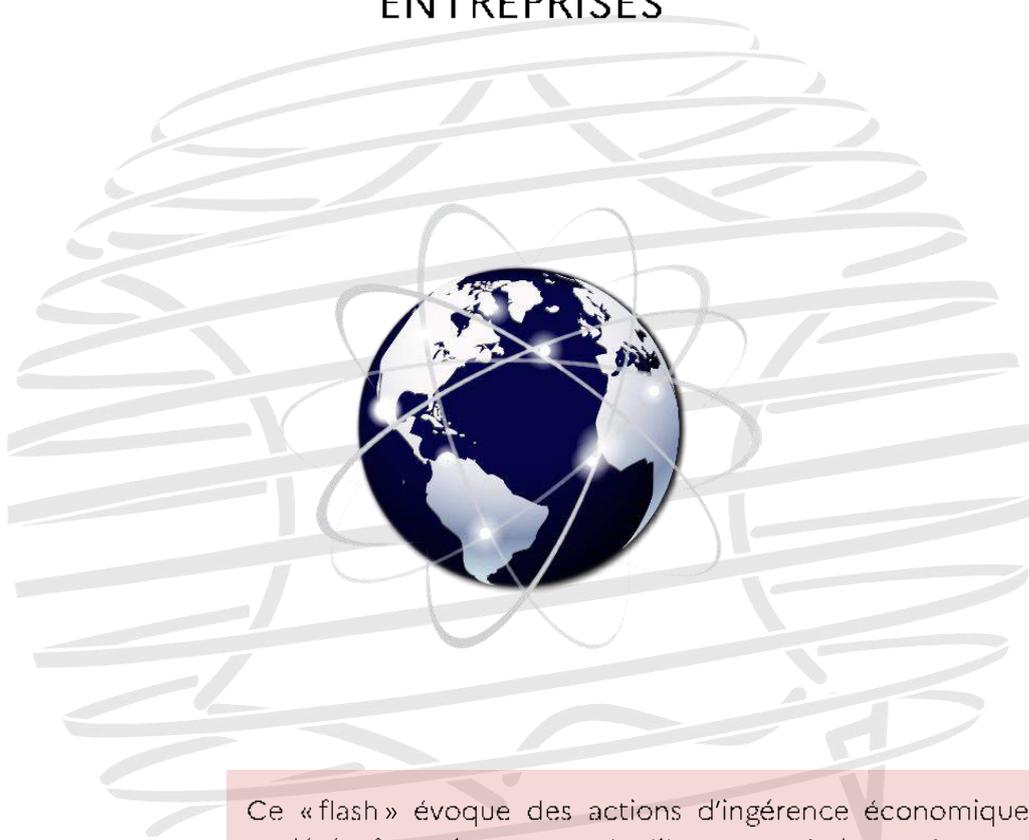


FLASH DGSi #97

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



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 événements.

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 événements, ceux-ci peuvent également chercher à déstabiliser un concurrent par le biais d'attaques 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 DGTI

EN AMONT DU SALON

- **Analyser l'environnement du salon.** Étudier la disposition du stand attribué sur le salon par rapport aux stands environnants et identifier 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 DGTI 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 DGTI.