Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n°17 septembre 2015

Ce « flash » de l'ingérence économique évoque des actions 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.

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash n°17 Septembre 2015

Les salons professionnels, un contexte toujours propice aux captations d'informations

Lors des salons professionnels, les entreprises françaises font régulièrement l'objet d'approches ou de démarches offensives conduites par des sociétés ou des services de renseignement étrangers. Si ces salons sont avant tout des lieux dédiés à la présentation de compétences et de produits, ils offrent aussi aux entreprises participantes l'occasion de réaliser une veille concurrentielle active. Les techniques d'approches directes mises en œuvre par les représentants de sociétés ou de « simples visiteurs » lors de ces évènements sont connues. En revanche, la DGSI souhaite mettre en lumière des techniques plus insidieuses, régulièrement constatées par les exposants et les services de l'Etat.

Vous trouverez ci-après quelques exemples d'opérations visant à capter des informations, en amont, pendant et après la tenue de salons professionnels.

- Avant l'arrivée sur le salon : Utilisation de dispositifs d'écoute dans les moyens de transport. Lors d'un évènement à portée internationale, l'un des leaders mondiaux du secteur a mobilisé la plupart des compagnies privées de transport de la ville durant toute la durée du salon, afin de mettre des véhicules à disposition des participants dans le cadre d'une opération publicitaire. Il est apparu que des dispositifs d'écoute avaient été placés dans ces véhicules ou que des conducteurs, recrutés et sélectionnés en fonction de leurs compétences linguistiques, effectuaient un rapport sur les propos tenus par les personnes transportées. La société organisatrice a ainsi pu avoir accès à toutes les conversations des exposants préparant, pendant leur temps de transport, leurs rendez-vous du jour ou évoquant leurs contacts et rendez-vous de la veille.
- Pendant la durée du salon : Identification du portefeuille de clients d'un concurrent. Afin de cibler au mieux la stratégie commerciale d'un de ses concurrents lors d'un salon international, une entreprise étrangère a pu, grâce à une caméra installée sur un mât télescopique de son stand, filmer les personnes se rendant sur le stand de son concurrent. Deux hôtesses d'accueil entraient ensuite en contact avec les personnes ciblées, sollicitant d'être prises en photo avec elles et tentant d'obtenir l'identité des intéressés.
- Après le salon : Corruption d'un support numérique afin de perpétrer une attaque informatique et un vol de données. Au cours d'un salon professionnel, une clef USB a été connectée sur l'ordinateur portable d'un exposant.

Préalablement sensibilisé au risque de captation d'informations par des logiciels espions, cet exposant ne détenait aucune donnée sensible sur son ordinateur. A l'issue du salon, il s'est néanmoins connecté sur le réseau interne de son entreprise sans prendre de précaution particulière (procédure de « décontamination »), ce qui a permis à un logiciel malveillant transmis par la clef USB de se propager. Plusieurs mois se sont écoulés avant que le malware soit identifié.

Commentaire :

La pratique la plus classique est l'approche directe par un « journaliste », un « étudiant » ou un visiteur, qui cherche à obtenir de son interlocuteur des informations stratégiques sur l'entreprise que celui-ci représente. Ce type d'approche repose sur la collecte préalable d'informations permettant d'identifier les personnes à cibler et les éléments clefs à obtenir lors du salon. La manœuvre finale n'est que la conclusion d'un processus initié en amont du salon. Si les exposants sont familiers de ce mode opératoire, les sociétés les plus offensives se servent également des premiers éléments collectés en vue d'une action d'ingérence économique ultérieure.

Ainsi, l'écoute des briefings, bilans et discussions pendant le transport des exposants permet de connaître les nouveaux projets de R&D d'une société, ainsi que les noms des responsables qui pourront constituer autant de cibles potentielles. De même, la connaissance et l'identification du portefeuille de clients d'une entreprise, si elle donne des indications sur sa stratégie commerciale, permet également d'identifier des accès humains susceptibles de communiquer ultérieurement des informations sensibles ou confidentielles. La corruption d'un équipement relié au réseau interne de l'entreprise permet d'accéder à l'ensemble des informations stockées sur le réseau. Les salons professionnels restent donc des moments privilégiés pour la mise en œuvre d'opérations visant à la captation d'informations stratégiques.

Préconisations de la DGSI :

Il est important de préparer la participation à un salon en intégrant le volet sécurité de l'information. La DGSI vous propose d'accompagner votre démarche par des conférences de sensibilisation adaptées destinées à vos personnels.

Vous trouverez ci-après quelques conseils pratiques visant à se prémunir d'actions offensives régulièrement observées :

- Avant le salon, il est recommandé d'étudier la disposition des stands environnant celui de la société et principalement ceux de ses concurrents. Une sensibilisation des collaborateurs au discours à tenir et aux réponses à apporter aux visiteurs et contacts durant le salon.
- Dans les hôtels, les chambres et les coffres-forts qu'elles contiennent ne doivent pas être considérés comme des zones sécurisées. Il est important de toujours conserver avec soi les documents sensibles. Enfin, l'utilisation des bornes wifi et internet de l'hôtel est à éviter dans toute la mesure du possible. L'utilisation d'une connexion VPN (Virtual Private Network) minimise les risques, sans pour autant garantir une sécurité absolue.
- Pendant le salon, une surveillance physique du stand, des prototypes et du matériel appartenant à la société est fortement recommandée afin d'éviter toute manipulation dommageable par des tiers. Il est recommandé de recueillir tous les éléments relatifs à l'identité et à la fonction de l'interlocuteur, utiles en cas de rédaction de rapports d'étonnement, lesquels ont pour but de relater toutes les situations atypiques survenues lors de l'évènement.
- Après le salon, un démontage méticuleux du stand évitera des « pertes » inopinées de matériels ou de maquettes sensibles. Vérification et décontamination systématique de tous les appareils présents sur le salon augmenteront le niveau de protection du réseau interne de la société.