INGERENCE ECONOMIQUE

Flash n° 64 – Avril 2020

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.

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°64 avril 2020

L'exposition médiatique, facteur de vulnérabilité dans le cadre de la crise sanitaire

Dans le contexte de la crise sanitaire mondiale et de la lutte contre le Covid-19, plusieurs entreprises et entités susceptibles de contribuer à la résolution de la crise font l'objet d'une exposition médiatique, parfois soudaine.

Or, cette visibilité inattendue peut attirer l'attention d'individus malveillants. La publicité gratuite pour les entreprises, qui voient leur savoir-faire ou leurs innovations être mis en valeur, est une véritable aubaine pour un grand nombre d'entre elles, mais peut avoir des conséquences néfastes pour les sociétés les plus fragiles et les moins préparées, notamment s'agissant de la protection de leurs systèmes d'information.

Par ailleurs, la couverture médiatique dont les entreprises font l'objet offre aux individus mal intentionnés de nombreuses informations qu'ils peuvent utiliser afin de mettre en place des escroqueries, notamment aux faux ordres de virement, ou pour se livrer à de la contrefaçon.

PREMIER EXEMPLE

Quelques jours après la parution d'un article de presse à son sujet, une PME, spécialisée dans la production de matériel sanitaire, a dû porter plainte après avoir été la victime d'une attaque informatique. Un cybercriminel a réussi à pirater l'adresse électronique officielle de l'entreprise pour contacter des sociétés. Profitant de la notoriété de sa victime, le cybercriminel a proposé à ses cibles un approvisionnement en matériel sanitaire. Le préjudice est double, à la fois pour l'entreprise dont la réputation est atteinte, et pour la société qui a été victime de l'escroquerie en pensant, en toute bonne foi, être le nouveau client d'une entreprise connue.

DEUXIÈME EXEMPLE

Une entreprise française, spécialisée dans la fabrication de matériel de protection et faisant l'objet d'articles réguliers dans la presse depuis le début de la crise sanitaire, a récemment été contactée par une entreprise étrangère, laquelle souhaitait vérifier l'origine de masques de protection FFP2 qui venaient de lui être proposés à la vente par un grossiste étranger. La société française a

confirmé que le matériel, labellisé à son nom, était une contrefaçon. L'entreprise tricolore est déterminée à déposer plainte pour se prémunir légalement de toute contestation concernant la qualité de son matériel.

TROISIEME EXEMPLE

Une institution, médiatisée pour son implication dans la gestion de la crise sanitaire, a constaté que des cybercriminels avaient créé une adresse électronique quasiment identique à la sienne pour tenter d'escroquer les établissements de santé et les entreprises. Ces cybercriminels ont envoyé un courriel aux entités ciblées pour leur proposer de commander, par téléphone ou par messagerie informatique, du matériel de protection (gants ou masques). Les structures ciblées, qui pensent avoir affaire à une institution officielle, régulièrement mise en avant dans cette période de crise, sont invitées à régler la facture avant la soi-disant réception du matériel.

Commentaire :

Une exposition médiatique soudaine peut exposer les entreprises à des risques majeurs. Ainsi, certaines PME, peu habituées à gérer leur image et à répondre à de nombreuses sollicitations, sont confrontées à la multiplication de marques d'intérêt, notamment étrangères, qui doivent appeler à la plus grande vigilance. De nombreuses approches peuvent ainsi s'avérer malveillantes.

PRECONISATIONS DE LA DGSI

Face aux risques liés à une médiatisation soudaine, la DGSI émet les préconisations suivantes :

→ Avant toute prise de parole et d'affichage médiatique, les entreprises doivent se préparer aux risques liés à une visibilité accrue, qui suscitera de nombreuses marques d'intérêt. Dans ce contexte, il est pertinent de procéder au renforcement de la sécurité des systèmes d'informations de la société. Il s'agit également de veiller à assurer la protection juridique appliquée aux savoir-faire et aux innovations.

→ Avant de procéder à tout paiement, il est important d'évaluer l'honorabilité d'un vendeur en se rapprochant de différentes entités : banques, autorités de santé (ministère, agence régionale de santé, hôpitaux), services de protection économique (ministère de l'intérieur, ministère de l'économie et des finances), etc.

→ En cas d'escroquerie avérée, porter plainte immédiatement auprès des services de police ou de gendarmerie. Conserver tous les éléments (e-mails, noms, etc.) pouvant contribuer à l'enquête. Des plateformes de signalements mises en place par les pouvoirs publics permettent également de dénoncer ces tentatives frauduleuses. Nous vous orientons plus particulièrement vers le site web du ministère de l'intérieur : www.internet-signalement.gouv.fr