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

FLASH DGSI #89

DÉCEMBRE 2022

INGÉRENCE ÉCONOMIQUE

RISQUES D'ACCÈS AUX APPAREILS ÉLECTRONIQUES LORS DE CONTRÔLES AÉROPORTUAIRES

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 #89

DÉCEMBRE 2022

INGÉRENCE ÉCONOMIQUE

RISQUES D'ACCÈS AUX APPAREILS ÉLECTRONIQUES LORS DE CONTRÔLES AÉROPORTUAIRES

Cadres d'entreprise, experts ou encore chercheurs sont amenés à se rendre régulièrement à l'étranger pour rencontrer des partenaires commerciaux, prospecter de nouveaux marchés ou assister à des salons professionnels, des colloques et des congrès.

Dans la majorité des cas, ces déplacements impliquent le transport de supports numériques (ordinateurs portables, tablettes et téléphones portables). Ces appareils peuvent contenir des données sensibles ou confidentielles comme des informations financières, commerciales ou encore les résultats de travaux de recherche.

La DGSI a constaté une recrudescence tendancielle de démarches intrusives menées à l'égard de dirigeants ou de salariés d'entités stratégiques françaises lors de leurs voyages, plus particulièrement à l'occasion des contrôles aéroportuaires. Justifiés par des motifs d'ordre sécuritaire, ces contrôles peuvent être détournés et exploités à des fins de captation de données ou de piégeage informatique.

PREMIER EXEMPLE

Un chercheur d'une école d'ingénieurs française renommée a été invité à participer à une conférence internationale durant laquelle il devait présenter le résultat de ses travaux.

Arrivé à l'aéroport du pays de destination, le chercheur français a été longuement interrogé par les douanes. Un agent en civil lui a posé quelques questions générales puis, au motif d'une vérification, lui a retiré son téléphone portable et sa tablette qui contenaient ses travaux de recherche et étaient utilisés à la fois à titre personnel et professionnel.

Le chercheur a ensuite été escorté dans un bureau de l'aéroport afin de procéder à un entretien de plusieurs heures, mêlant questions professionnelles et personnelles. Au terme de cet interrogatoire, le chercheur s'est vu restituer ses documents d'identité, son téléphone et sa tablette, ainsi qu'un document officiel lui précisant que la saisie de ses appareils était autorisée dans le cadre de ce contrôle frontalier.

DEUXIEME EXEMPLE

Un cadre d'une grande entreprise française s'est rendu à l'étranger pour motif familial en emportant son ordinateur portable professionnel. À l'aéroport du pays étranger pour son vol retour, ses effets personnels ont fait l'objet d'un contrôle renforcé à l'occasion des vérifications de sécurité habituelles des bagages à main.

L'agent de sécurité a notamment retiré la batterie de son ordinateur professionnel puis a effectué à plusieurs reprises un contrôle de l'appareil avec un scanner. Les agents de l'aéroport ont alors procédé durant plusieurs heures à un interrogatoire particulièrement intrusif portant notamment sur l'activité professionnelle du cadre, l'identité de ses clients ou encore le type de produits proposées par son entreprise.

S'il a finalement été autorisé à voyager, le cadre n'a pas pu emporter son ordinateur avec lui à bord de l'avion. Le service de sécurité a en effet décidé de retenir son appareil sous prétexte d'un problème de sécurité. Ce dernier lui a été restitué le lendemain par courrier par la compagnie aérienne.

TROISIEME EXEMPLE

Alors qu'il se rendait à un salon professionnel à l'étranger, un cadre d'entreprise attendait l'ouverture des guichets devant le comptoir de la compagnie aérienne étrangère pour effectuer son enregistrement lorsqu'un individu, sans lien apparent avec la compagnie aérienne, s'est présenté à lui.

Le cadre a été interrogé sur les motifs de son déplacement, le déroulement de sa journée avant d'arriver à l'aéroport et le contenu de son bagage. Il a ensuite été invité à suivre l'agent étranger dans un local sécurisé à proximité des comptoirs d'enregistrement de la compagnie aérienne.

L'agent étranger a alors expliqué qu'il allait procéder à l'inspection de ses bagages et effectuer une analyse de son ordinateur et que, durant ce contrôle, il était nécessaire que le cadre français patiente en dehors du local. Sensibilisé aux risques associés aux contrôles des appareils numériques, le cadre de la société française a refusé de se séparer de ses bagages et de son ordinateur. Si l'ordinateur portable n'a finalement pas été allumé, l'agent étranger a examiné très méticuleusement les affaires personnelles du cadre français en sa présence, recourant à de nombreuses reprises à un détecteur de particules sur ses terminaux numériques. Le cadre français a finalement pu retourner au comptoir d'enregistrement et poursuivre son voyage.

COMMENTAIRES

Lors d'un déplacement à l'étranger, le transport d'appareils électroniques doit faire l'objet d'une vigilance continue tout au long du trajet et du séjour. Même lors d'un déplacement dans un cadre privé, les appareils électroniques peuvent faire l'objet d'un contrôle ciblé ou d'opportunité.

Ces contrôles, qui peuvent se dérouler aussi bien sur le territoire national qu'à l'étranger, peuvent être détournés à des fins de collecte d'information et aller jusqu'à la copie des données d'appareils électroniques, effectuée à l'insu de son propriétaire. Les agents chargés des contrôles aéroportuaires peuvent également exiger les mots de passe ou les clés de chiffrement pour débloquer les appareils électroniques et ainsi avoir accès aux données qu'ils contiennent.

Certains États n'hésitent pas à mener des actions ciblées auprès de cadres d'entreprises, d'experts ou de chercheurs français à l'occasion de déplacements préalablement identifiés comme stratégiques. Certains profils peuvent également être ciblés en amont afin qu'un contrôle soit réalisé lors d'un déplacement privé, où la vigilance vis-à-vis de la protection des informations professionnelles peut parfois être moins soutenue.

PRÉCONISATIONS DE LA DGSI

RECOMMANDATIONS EN AMONT D'UN VOYAGE À L'ÉTRANGER

- **Prendre connaissance des règles de sécurité mises en place par son entreprise ou son centre de recherches dans le cadre des déplacements à l'étranger**. Il peut être utile de se rapprocher de son responsable de la sécurité des systèmes d'information (RSSI) afin de prendre connaissance des règles élémentaires d'hygiène numérique et se voir notamment rappeler, le cas échéant, l'existence d'ordinateurs nomades dédiés à ce type de déplacements.
- **Réaliser une sauvegarde de ses données avant le départ et la stocker en lieu sûr**. Cela permet de récupérer de manière intacte ses données en cas d'incident lors d'un déplacement. Il est conseillé d'effectuer des sauvegardes régulières sur un support hors réseau.
- **Limiter les informations stockées sur les appareils électroniques aux seuls besoins de la mission**. Afin de réduire le risque de perte, vol ou captation de données, il convient de limiter le transport de données aux besoins exclusifs de la mission visée par le déplacement.
- **Chiffrer les données sensibles sur ses dispositifs numériques grâce à des solutions sécurisées et diversifier ses mots de passes**. Lorsque les dispositifs numériques et applications le permettent, privilégier l'authentification forte. Il est également conseillé de créer un mot de passe différent pour chaque appareil et application. Vérifier cependant que l'utilisation de ces moyens de chiffrement ne nécessite pas une autorisation préalable à leur introduction sur le territoire étranger dont le défaut constituerait le motif à un contrôle renforcé. Certaines pratiques sont en effet légales en France mais interdites à l'étranger.
- **Consulter le « Passeport de sécurité numérique de l'Agence nationale de la sécurité des systèmes d'information » (www.ssi.gouv.fr) relatif aux bonnes pratiques à l'usage des professionnels en déplacement.**

CONSEILS LORS D'UN PASSAGE A L'AEROPORT

- **Ne pas laisser ses appareils électroniques sans surveillance**. Les garder prioritairement avec soi en bagage à main. S'ils doivent être mis en soute, il peut être utile de les placer dans une enveloppe sécurisée inviolable bien identifiée afin de les protéger et d'être en mesure de vérifier si quelqu'un a cherché à y accéder.

- **Ne pas recharger ses appareils sur les bornes de recharge USB en libre-service**. Toujours utiliser son propre matériel de recharge et le brancher sur des prises murales.
- **Éviter de se connecter aux réseaux Wi-Fi publics des aéroports**. Le cas échéant, il est important d'utiliser les outils professionnels sécurisés fournis par son organisme d'origine, ou un réseau privé virtuel (VPN). Après avoir eu recours à un réseau Wi-Fi public, il est préférable de modifier les mots de passe des applications utilisées régulièrement sur ses appareils.
- **Faire preuve de discrétion**. Limiter l'utilisation des dispositifs numériques contenant des données sensibles en public et équiper les appareils électroniques de filtres de confidentialité.
- **En cas de contrôle, ne pas chercher à s'y opposer mais à l'accompagner : demander à son interlocuteur de préciser son identité ou de justifier sa fonction avant de répondre à des questions jugées intrusives**. Dans la mesure du possible, essayer de garder son matériel électronique avec soi ou demander à être présent lors du contrôle des appareils.
- **À l'issue du contrôle, être attentif au comportement de ses appareils :** icônes déplacés, consommations excessives ou rechargement injustifié des batteries.
- **Informer sans délai le service informatique de son employeur en cas de problème avec ses appareils électroniques à l'issue d'un déplacement**. Des mesures pourront ainsi être mises en œuvre pour limiter la perte de données et protéger l'entité, notamment en cas de perte, de vol ou de fonctionnement anormal des équipements.

BONNES PRATIQUES A METTRE EN ŒUVRE LORS DU RETOUR EN FRANCE

- **Renouveler les mots de passe de tous les appareils électroniques et des applications utilisés lors du déplacement.**
- **Faire analyser les appareils électroniques par son service informatique une fois de retour de mission, et avant de les connecter aux réseaux internes de son organisation**. Cette étape est essentielle pour éviter une possible contamination du système informatique de son organisation et afin de détecter si des données ont été captées, volées ou détruites par un acteur tiers.
- **En cas de découverte ou de suspicion de captation informationnelle ou technologique, d'approches inhabituelles d'acteurs étrangers ou d'incidents survenus lors de contrôles aéroportuaires, contacter la DGSI à** securite-economique@interieur.gouv.fr