MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH INGÉRENCE ÉCONOMIQUE DGSI #111

Mars 2025

RISQUES ASSOCIÉS À L'UTILISATION D'OUTILS NUMÉRIQUES PERSONNELS À DES FINS PROFESSIONNELLES

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**

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**

RISQUES ASSOCIÉS À L'UTILISATION D'OUTILS NUMÉRIQUES PERSONNELS À DES FINS PROFESSIONNELLES

Depuis plusieurs années, l'utilisation d'outils numériques personnels (téléphones, ordinateurs, tablettes, clés USB, disques durs, etc.) à des fins professionnelles s'est accrue, notamment avec l'évolution des modes de travail, permettant de combiner des journées de travail dans les locaux de l'entreprise, et du travail à distance ou à domicile.

Cette pratique peut être encouragée par des entreprises ou des laboratoires de recherche, souvent par souci d'économie et de recherche de flexibilité, qui vont parfois jusqu'à inciter leurs salariés à utiliser leurs appareils personnels dans le cadre professionnel selon la politique du « bring your own device »[1]. Certains salariés préfèrent également utiliser leurs propres appareils dès lors que ceux mis à disposition par leur employeur ne leur conviennent pas.

Cette pratique accroît particulièrement les risques cyber, matériels et humains, qui peuvent avoir des conséquences pour la structure concernée, comme le vol de données sensibles, la compromission du système d'information ou encore une atteinte à la réputation.

1 L'INFECTION DE L'ORDINATEUR PERSONNEL D'UN SALARIÉ A PERMIS D'ACCÉDER À PLUSIEURS CENTAINES DE MILLIERS DE FICHIERS CLIENTS

Un salarié a utilisé à de multiples reprises son ordinateur personnel pour se connecter à la plateforme commerciale de son entreprise, sans dispositif d'anonymisation, ni de chiffrement des échanges. Or, cet ordinateur, régulièrement utilisé par un membre de la famille du salarié, a eu un fonctionnement inhabituel sur une très courte période sans que cela ait pu être expliqué.

Plusieurs mois après cet évènement, le responsable de la sécurité des systèmes d'information de la société a détecté la présence de l'identifiant professionnel et du mot de passe du salarié sur le dark web. La société n'ayant pas mis en place de mécanisme d'authentification forte pour sa plateforme commerciale, ces informations de connexion ont permis des accès non autorisés à l'intégralité de sa base de données clients.

L'entreprise a corrigé ces vulnérabilités techniques et initié une campagne de communication à destination de ses clients pour les informer de l'existence de cette attaque informatique et des risques d'exfiltration de données personnelles.

[1] Cette expression signifie littéralement « apportez votre propre équipement numérique ».

2 LE TÉLÉPHONE D'UN SALARIÉ, UTILISÉ À DES FINS PERSONNELLES ET PROFESSIONNELLES, A ÉTÉ CONTROLÉ PAR DES AUTORITÉS ETRANGÈRES

Après avoir atterri dans un pays étranger, le salarié d'une société française a fait l'objet d'un contrôle aux frontières et s'est vu saisir le téléphone, qu'il utilise aussi bien à titre personnel que professionnel. Les autorités du pays d'accueil lui ont alors demandé de déverrouiller son téléphone avant de l'emporter dans une autre pièce.

Alertée de ce contrôle aéroportuaire intrusif par son salarié, la société française n'a toutefois pas été en mesure de déterminer si le téléphone avait été manipulé et si les données sensibles s'y trouvant avaient été compromises.

En effet, encourageant la pratique du « bring your own device » auprès de ses salariés, la société n'a pas rédigé de politique claire encadrant le recours à des appareils personnels. Par ailleurs, elle ne possédait pas de système de gestion des appareils mobiles à distance qui aurait permis d'exercer une surveillance sur la flotte de téléphones utilisés au sein de la société.

3 LE VOL DE L'ORDINATEUR D'UN CONSULTANT EXTÉRIEUR FAIT PESER DES RISQUES DE PERTES DE DONNÉES SUR UNE SOCIÉTÉ SENSIBLE

Une société exerçant son activité dans un domaine sensible et particulièrement concurrentiel sur le plan international, a régulièrement recours à des prestataires externes, spécialisés en informatique.

Or, l'un des consultants d'un prestataire informatique de la société a été victime du vol de son ordinateur personnel à son domicile. Avant le vol de l'appareil, le consultant y avait transféré des données appartenant à la société depuis son poste de travail professionnel, dont certaines portaient sur un projet particulièrement sensible de la société. Ces données étaient stockées sans protection particulière, sur un ordinateur qui ne contenait qu'une simple protection par mot de passe.

La société a interrompu sa collaboration avec ce prestataire qui ne l'avait pas avisée du transfert de ces fichiers. Elle a également initié une politique de communication interne auprès de ses salariés et prestataires externes pour éviter que ce type d'incident ne se reproduise.

Commentaires

Lorsqu'il ne peut être évité, le recours à des appareils personnels dans le cadre professionnel doit impérativement être limité aux usages les moins sensibles pour l'entreprise. En effet, les usagers sont souvent moins vigilants aux pratiques élémentaires d'hygiène numérique lorsqu'ils utilisent leurs appareils personnels, et négligent certaines mesures de sécurité. Par ailleurs, un appareil personnel est par définition moins bien protégé et plus vulnérable aux vols, car davantage susceptible d'être déplacé, notamment dans un cadre personnel.

Cette pratique, si elle n'est pas encadrée, expose les entreprises qui y ont recours à des risques importants pour la sécurité de leurs données. Les appareils numériques utilisés à des fins personnelles sont en effet souvent moins protégés contre les attaques d'acteurs malveillants qui chercheraient à cibler une société.

La sensibilisation des salariés sur les comportements à adopter lors de l'usage d'un appareil personnel à des fins professionnelles est donc essentielle et doit impérativement accompagner la politique du « bring your own device » lorsqu'elle est pratiquée. Des outils de cloisonnement de chaque environnement numérique de travail doivent également être déployés.

Sensibiliser son personnel aux bonnes pratiques à adopter dans l'usage mixte de leurs appareils numériques

- **Sensibiliser les utilisateurs aux enjeux de sécurité propres à leur secteur d'activité.**

  Tous les salariés de l'entité doivent être régulièrement sensibilisés aux enjeux propres à leur secteur d'activité afin qu'ils prennent la mesure des approches ou des tentatives d'ingérences dont ils pourraient faire l'objet. Ces sensibilisations doivent les inviter à la prudence dans leurs comportements quotidiens, et particulièrement dans la gestion de leurs outils numériques.

- **Émettre des recommandations sur l'emploi des appareils personnels hors du lieu de travail.**

  À l'extérieur du lieu de travail, et particulièrement dans les lieux publics, il est recommandé de ne travailler que sur des données peu sensibles, de ne jamais laisser ses appareils sans surveillance, de ne jamais confier ses appareils à des tiers et de ne pas se connecter à des réseaux Wifi ou à des ports USB inconnus.

- **Veiller à diffuser aux salariés les règles de bonne pratique à adopter en matière d'hygiène numérique.**

  Les utilisateurs doivent appliquer les règles élémentaires de sécurité informatique, par exemple en s'appuyant sur les recommandations de l'Agence nationale de la sécurité des systèmes d'information (Anssi). Il est notamment recommandé de maintenir à jour ses appareils et ses applications, de ne pas installer d'applications comportant des vulnérabilités, de limiter les autorisations données à chaque application au strict nécessaire ou encore d'utiliser des mots de passe différents pour chaque usage numérique.

- **Recommander vivement aux salariés de cloisonner leurs usages personnels et professionnels sur leurs appareils numériques partagés.**

  Le cloisonnement des usages personnels et professionnels est essentiel. Il est notamment conseillé d'utiliser des sessions différentes et protégées pour chaque usage, de prohiber les transferts d'informations entre messageries personnelles et professionnelles et de ne stocker aucune donnée sur l'appareil qui ne soit pas nécessaire aux missions effectuées.

Adapter la sécurité informatique de la société aux vulnérabilités des appareils personnels

- **Encadrer le recours aux outils numériques personnels dans une charte présentée à tous les salariés dès leur recrutement.**

  La politique interne de sécurité informatique, formalisée par exemple sous forme de charte, doit intégrer des dispositions relatives aux usages d'appareil personnel à des fins professionnelles, particulièrement en cas de politique de « bring your own device ». Elle doit notamment prévoir et limiter les tâches qui peuvent être effectuées avec ces appareils et les droits d'accès aux données internes. Des rappels réguliers doivent être transmis à tous les salariés. La politique interne de sécurité informatique doit prévoir également la conduite à tenir en cas de perte ou de vol des appareils mais aussi en cas de rétention des outils par une autorité étrangère (lors d'un passage frontière par exemple).

- **Veiller à encadrer étroitement les changements de fonction des salariés au sein de l'entreprise et les départs des collaborateurs.**

  Le changement de fonction d'un salarié doit s'accompagner de la vérification par le service chargé de la sécurité des systèmes d'information que ce dernier a conservé les accès strictement nécessaires à l'exercice de ses nouvelles fonctions. De même, lors du départ des collaborateurs, il est essentiel de s'assurer qu'ils n'ont conservé aucune donnée ou accès professionnels sur leurs appareils personnels.

En cas d'incident lié à un appareil personnel utilisé à des fins professionnelles

- **En cas d'incident avéré ou suspecté sur l'appareil.**

  Il est impératif d'en informer le responsable de la sécurité des systèmes d'information de la structure dès que possible, afin qu'il puisse prendre des mesures pour protéger les données et le réseau de la société.

- **En cas de vol d'un matériel personnel utilisé à des fins professionnelles.**

  Signaler la disparition du matériel auprès du responsable de la sécurité des systèmes d'information et déposer rapidement plainte auprès des services de police ou de gendarmerie compétents en veillant bien à signaler que l'appareil était utilisé à des fins personnelles et professionnelles.

- **En cas de suspicion de compromission de son appareil personnel.**

  Confier l'appareil au responsable de la sécurité des systèmes d'information pour qu'il évalue son intégrité numérique. En fonction du contexte de l'incident, ne pas hésiter à le signaler à la DGSI, à l'adresse : **securite-economique@interieur.gouv.fr**

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité