MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE
DGSI

FLASH DGSI #91

FÉVRIER 2023

INGÉRENCE ÉCONOMIQUE

LES RISQUES LIÉS AUX VISIOCONFÉRENCES

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 #91
FÉVRIER 2023

INGÉRENCE ÉCONOMIQUE

LES RISQUES LIÉS AUX VISIOCONFÉRENCES

Depuis la crise sanitaire de 2020, l'utilisation d'outils de travail à distance s'est généralisée. Le développement du télétravail a fortement augmenté le nombre des réunions effectuées à distance. Ces échanges sont l'occasion d'évoquer en interne des sujets souvent sensibles (recherche et développement, projets de de restructuration, etc.) mais également de rencontrer des acteurs étrangers dans le cadre de négociations ou de partenariats.

Dans ce contexte, les acteurs économiques et scientifiques français sont amenés à utiliser davantage de programmes et d'applications non protégés, dont des plateformes de visioconférence, des messageries instantanées et des solutions de partage de documents. Or, plusieurs de ces outils présentent d'importantes failles de sécurité, propices à la fuite, voire à la captation de données personnelles ou d'informations stratégiques. Les entités françaises qui ont recours à ces outils sont par ailleurs davantage exposées aux risques cyber, tels que les escroqueries ou les usurpations d'identité.

PREMIER EXEMPLE

Le comportement suspect d'une salariée étrangère expose son employeur à un risque de captation de ses données sensibles.

L'encadrement d'une salariée étrangère a découvert, peu après l'arrivée de cette dernière dans la société française, qu'elle ne disposait pas des compétences nécessaires pour remplir ses fonctions et a alors adapté ses tâches, sans succès. Profitant de la souplesse de la direction de sa société, cette cadre de l'entreprise a décidé unilatéralement de travailler presque exclusivement en télétravail, malgré des consignes imposant à l'ensemble des salariés un temps de travail effectué à 50 % en présentiel.

Lors de ses réunions de travail auxquelles elle participe en visioconférence, la salariée étrangère désactive systématiquement sa caméra et a, à plusieurs reprises, déclenché l'enregistrement vidéo des réunions portant sur des sujets sensibles comme la stratégie d'innovation. Interrogée par sa hiérarchie sur cette pratique, elle a prétexté enregistrer les réunions pour des collègues qui ne pouvaient pas assister aux réunions. Ce comportement suspect inquiète la société puisque la salariée a accès à distance à des informations stratégiques, dont la captation pourrait bénéficier à un concurrent ou à une puissance étrangère.

DEUXIÈME EXEMPLE

Une entreprise française se voit imposer une réunion en visioconférence suspecte avec des acteurs étrangers dans le cadre d'un projet de création de coentreprise.

Rachetée par un consortium de groupes étrangers, une société française spécialisée dans la conception de dispositifs médicaux a signé un partenariat industriel avec l'un de ses nouveaux actionnaires pour la création d'une coentreprise basée hors du territoire national. Dans le cadre des négociations liées à ce projet, effectuées en visioconférence, la société française a été invitée à s'entretenir avec une autorité étrangère, dont les représentants ne lui avaient pas été présentés par ses partenaires et dont les visages étaient floutés. À cette occasion, les interlocuteurs étrangers ont exigé qu'un salarié de l'entreprise française, récemment arrivé, présente sa pièce d'identité devant la caméra, active la géolocalisation de son téléphone et filme les locaux de la société afin de prouver qu'il se trouvait bien au siège de l'entité française.

La société française rencontre aujourd'hui des tensions dans son partenariat avec ces acteurs étrangers et est confrontée au transfert accéléré de sa technologie à l'étranger. La coentreprise s'est avérée n'être qu'une création juridique sans activité économique, les actionnaires étrangers ayant sous-traité l'assemblage des produits français à d'autres intervenants.

TROISIÈME EXEMPLE

Une structure scientifique française est exposée à une vidéo à caractère terroriste lors d'une visioconférence.

À l'occasion d'une réunion d'information effectuée en visioconférence, un institut de recherche spécialisé dans l'agroalimentaire a été victime d'une intrusion de son système d'information en raison de la faible sécurité du service utilisé. Peu après le début de la réunion, des individus ont en effet pris le contrôle de l'application en s'appropriant les droits d'animateurs, puis ont diffusé une vidéo à caractère terroriste montrant des images de décapitation.

L'inscription à la visioconférence était libre d'accès en ligne et aucun contrôle n'a été effectué. En outre, le niveau de sécurité du mot de passe de l'application était de faible intensité.

COMMENTAIRES

Face à la généralisation du télétravail, l'utilisation de services de visioconférence est devenue systématique alors que les acteurs économiques et scientifiques ont tendance à négliger les risques, numérique et économique, liés à ce type de réunion.

Certaines personnes peuvent tirer profit de ces échanges pour capter des informations. Une vigilance accrue doit donc être portée aux réunions à distance à la fois avec les collaborateurs internes et externes, y compris de confiance. Une attention particulière doit notamment être portée lors des réunions à distance pour lesquelles l'identité des participants n'est pas contrôlée, lorsque des individus n'apparaissent pas à l'écran ou enregistrent des conversations sans prévenir

ou encore lorsque des personnes sont conviées aux réunions au dernier moment sans annonce préalable.

Enfin, les pratiques de bonne conduite en matière de sécurité informatique doivent également être appliquées lors de ces échanges à distance. Des fragilités informatiques peuvent en effet être exploitées et exposer les entités à des risques susceptibles d'affecter la pérennité de leur activité ou leur réputation.

PRÉCONISATIONS DE LA DGSI

BONNES PRATIQUES À APPLIQUER EN MATIÈRE DE SÉCURITÉ INFORMATIQUE ET DE PROTECTION DES INFORMATIONS SENSIBLES

EN MATIÈRE DE PROTECTION ÉCONOMIQUE :

- **Identifier les données sensibles de l'entreprise auxquelles un acteur externe ne doit pas avoir accès et dont la fuite pourrait porter préjudice à la société**. Il est essentiel d'identifier de façon précise toutes les données considérées comme sensibles et vitales pour la préservation du savoir-faire de l'entreprise. Il conviendra ensuite de les classer en fonction de leur niveau de sensibilité et d'assurer un contrôle sur leur accès. Il sera ainsi pertinent de privilégier les réunions en présentiel pour évoquer les sujets les plus stratégiques et sensibles de la société, plutôt que les visioconférences.
- **Les employés doivent être sensibilisés à la nécessité de signaler toute situation inhabituelle menaçant le savoir-faire de la société** : manquement ou comportement déloyal d'un salarié, d'un stagiaire ou d'un prestataire, suspicion de transfert ou de détournement de technologies, etc.
- **En anticipation d'une fuite d'informations sensibles, effectuer une cartographie des risques permettant d'évaluer les conséquences pour la société, ses clients et ses partenaires.** Veiller notamment à la neutralité du cadre du lieu de la réunion et aux informations qui pourraient être visibles des autres participants.

EN MATIÈRE DE SÉCURITÉ INFORMATIQUE :

- **Effectuer de façon régulière et planifiée les mises à jour des systèmes d'exploitation et des programmes informatiques**. Les mises à jour ont vocation à corriger les failles qui facilitent les intrusions informatiques.
- **Utiliser un mot de passe de session pour les visioconférences avec des participants extérieurs, et générer un lien de session différent à chaque réunion.**
- **Inclure les logiciels de visioconférence dans les audits de sécurité informatique** pour une analyse des risques et une correction des vulnérabilités.

- **Impliquer les responsables de la sécurité des systèmes d'information (RSSI) dans l'encadrement de la pratique du télétravail**. Ce dispositif doit prévoir la mise à disposition d'outils adéquats, dont notamment du matériel dédié à l'usage professionnel, des applications et des moyens de connexions sécurisés assurant la confidentialité des échanges. Les collaborateurs doivent être accompagnés et formés à l'utilisation des outils mis à leur disposition. La signature d'une charte de respect des règles de bonne conduite doit également être envisagée. L'agence nationale de la sécurité des systèmes d'informations (Anssi) et la commission nationale de l'informatique et des libertés (Cnil) publient régulièrement des guides de bonnes pratiques et de conseils à respecter afin de réduire les risques cyber dans le cadre du télétravail.
- **Privilégier des solutions de visioconférence comprenant un chiffrement par défaut, idéalement du chiffrement de bout en bout**. L'Anssi recommande par exemple l'application française de visioconférence chiffrée de bout en bout, Tixeo. L'utilisation d'une solution de visioconférence non qualifiée par l'Anssi augmente les possibilités d'ingérence et les risques liés aux réglementations étrangères extraterritoriales portant sur les données numériques.

DANS LE CADRE DE REUNIONS AVEC DES ACTEURS ÉTRANGERS

- **Faire preuve de fermeté en cas d'incident.** Certains membres de délégations étrangères sont susceptibles de fortement insister auprès des structures françaises pour les pousser à déroger aux règles de sécurité. Il peut être pertinent de solliciter les services d'un avocat pour bénéficier de conseils juridiques en cas d'incident.
- **Accorder une attention particulière à la préparation des rencontres avec le partenaire, qu'il soit potentiel ou déjà connu**. En amont de la réunion, il est recommandé de recueillir le maximum d'informations sur les participants à la réunion afin d'évaluer leur stratégie et leurs intentions. Il est important d'avoir la liste complète des participants à la réunion afin d'être capable de les identifier. Enfin, il convient d'exercer une vigilance particulière en cas d'ajout de dernière minute d'un visiteur non identifié. Ces individus sont en effet susceptibles d'être des représentants de sociétés concurrentes, voire des agents des services de renseignement étrangers.
- **Alerter les services de l'État compétents et la DGSI (securite-economique@interieur.gouv.fr)** de tout comportement d'un individu ou d'une entité, en particulier étranger, susceptible de remettre en cause la pérennité de votre activité ou de conduire à des faits de captation d'informations sensibles. La DGSI peut fournir des recommandations en cas d'incident informatique ou impliquant des acteurs étrangers.