INGERENCE ECONOMIQUE

Flash n° 63 – 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°63 avril 2020

Les risques cyber liés au télétravail des salariés confinés dans le cadre de la lutte contre le Covid-19

Dans le contexte de la crise sanitaire mondiale et de la lutte contre le Covid-19 qui a conduit les autorités à mettre en place des mesures de confinement, le télétravail est apparu comme une solution indispensable afin d'assurer la continuité d'activité des entreprises et des administrations ainsi que la sécurité sanitaire des employés. Cette pratique s'accompagne toutefois de risques cyber accrus.

Confinés, les salariés utilisent davantage des programmes et des applications non-sécurisés, notamment des plateformes de visioconférence, des messageries instantanées et des solutions de partage de documents. Plusieurs de ces outils présentent d'importantes failles de sécurité, propices à la fuite, voire à la captation, de données personnelles ou d'informations confidentielles ou stratégiques relatives à l'activité de l'entreprise ou de l'institution.

En outre, la pratique du télétravail s'accompagne souvent de l'utilisation de réseaux non-sécurisés, voire d'ordinateurs ou de téléphones personnels. Cette situation dégradée accentue les risques cyber, notamment les usurpations d'identité ou encore les fraudes au président ou aux faux ordres de virements.

PREMIER EXEMPLE

Plusieurs applications, gratuites ou payantes, permettant le partage de documents ou l'organisation de visioconférences, sont devenues particulièrement populaires. L'essor du télétravail en France, renforcé par les mesures de confinement décidées pour lutter contre le Covid-19, s'est accompagné d'un recours croissant à ces solutions qui présentent toutefois de sérieuses vulnérabilités et failles de sécurité, à l'instar de l'application américaine Zoom[1].

Si le nombre d'utilisateurs quotidiens de l'application a été multiplié par 20 en trois mois, passant de 10 à 200 millions dans le monde, les critiques visant Zoom sont de plus en plus nombreuses. Plusieurs entreprises et administrations en ont d'ailleurs interdit l'usage à leurs collaborateurs après avoir identifié plusieurs risques : transmission des données, à l'insu des utilisateurs, à

[1] *Zoom Video Communications est une société américaine de services de téléconférence basée en Californie.*

Facebook ; transfert de clés de chiffrement, au moins partiellement, vers des serveurs hébergés en Chine, permettant ainsi aux autorités chinoises d'accéder aux données ; absence de chiffrement de bout en bout malgré les allégations de la société américaine ; vol de mots de passe Windows ; données stockées sans protection ; etc.

Le faible niveau de sécurité de l'outil a également permis à des individus de s'introduire dans des visioconférences auxquelles ils n'étaient pas conviés, diffusant des images à caractère pornographique ou des messages de haine.

DEUXIEME EXEMPLE

Les sociétés sont également confrontées à la difficulté croissante de s'assurer que leurs collaborateurs, en télétravail depuis le début du confinement, n'utilisent que les outils mis à leur disposition par l'entreprise et respectent effectivement les consignes et les règles d'hygiène informatique, mêmes les plus simples et élémentaires, afin de garantir la sécurité des systèmes d'information.

La direction d'un grand groupe industriel français reconnait que cette situation doit faire l'objet d'autant plus d'attention que les solutions informatiques, préexistantes à la crise sanitaire actuelle, sont rarement conçues pour être sollicitées par autant d'utilisateurs en même temps, lesquels parfois n'ont pas été pleinement formés à leur utilisation.

Face aux dysfonctionnements et autres lenteurs de connexion, les salariés sont tentés de se diriger vers des solutions qu'ils jugent plus efficaces pour répondre à leurs besoins immédiats malgré de nombreux risques. Ainsi des échanges de documents et des réunions sur des sujets sensibles ont lieu *via* des canaux non-sécurisés.

TROISIEME EXEMPLE

Profitant de la généralisation du télétravail pour tous les salariés au sein d'un établissement français, un cybercriminel a réussi à usurper l'identité d'un membre du service informatique et a lancé une campagne de *phishing*, ou hameçonnage, à destination des employés confinés à domicile. Son objectif était de récupérer leurs mots de passe et leurs identifiants afin de pouvoir accéder au réseau de l'entité. Le service informatique de l'établissement, informé de l'attaque, est parvenu à contacter rapidement tous les employés pour les mettre en garde contre cette menace, leur rappeler les bonnes pratiques et les encourager à faire preuve de la plus grande vigilance.

Commentaire

En cas de recours à des outils (accès à distance, applications de visioconférence, applications de partage de documents, etc.) peu ou pas sécurisés, les données peuvent être détournées, copiées ou encore supprimées. De même, le risque d'être victime d'une escroquerie est augmenté.

Ainsi, la pratique du télétravail doit être encadrée par les responsables de la sécurité des systèmes d'information (RSSI) des entreprises et des administrations. Les collaborateurs doivent être accompagnés et formés à l'utilisation des outils mis à leur disposition et les bonnes pratiques doivent être régulièrement rappelées.

PRECONISATIONS DE LA DGSI

Face aux risques cyber induits par la pratique du télétravail, la DGSI émet les préconisations suivantes :

→ Le RSSI doit mettre en place une politique stricte encadrant le télétravail, notamment la mise à disposition d'outils adéquats (ordinateurs portables professionnels, applications sécurisées, etc.) et la signature d'une charte engageant le collaborateur à respecter des règles de bonne conduite édictées par l'entreprise ou l'administration.

→ Outre des matériels dédiés uniquement à l'usage professionnel (ordinateur, téléphone, etc.), des moyens de connexion protégés ou chiffrés, notamment *via* un *virtual private network (VPN)*, couplés à des applications assurant la confidentialité des échanges doivent être mis en place pour permettre aux différents collaborateurs de travailler dans un environnement de télétravail sécurisé.

→ L'Agence nationale de la sécurité des systèmes d'informations (ANSSI) et la Commission nationale de l'informatique 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. L'ANSSI recommande par exemple l'application française de visioconférence Tixeo. La CNIL, quant à elle, invite à la plus grande vigilance concernant la collecte des données personnelles, les applications de visioconférence sont par exemple tenues d'informer les utilisateurs de l'usage fait de leurs données.