Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Ces « flashs » évoquent 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

Liste des flashs ingérence économique

- Les risques cyber liés aux prestataires et aux sous-traitants
- Risque généré par le manque d'encadrement des stagiaires au sein des structures publiques et privées
- Déplacements à l'étranger : un risque important de captation d'informations

- Les risques liés à l'hébergement des données dans les data centers/clouds
- Les dangers liés aux objets connectés
- Dangers liés au WiFi public

- Les risques cyber liés aux rançongiciels

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash-ingérence économique

Les risques cyber liés aux prestataires et aux sous-traitants

Les entreprises et administrations, indépendamment de leur taille, mission ou secteur d'activité, sont de plus en plus fréquemment amenées à confier à des tiers tout ou partie de la gestion de leurs systèmes d'information. Ces prestations peuvent induire des risques sur l'intégrité, la disponibilité ou la confidentialité desdits systèmes.

Pour mener à bien ces missions, les prestataires disposent, en particulier, de connexions informatiques aux réseaux de l'entreprise cliente. Ces accès peuvent être internes lorsqu'un sous-traitant est physiquement sur le site, ou à distance, notamment dans le cas d'infogérance ou de supervision des réseaux. Indifféremment de la méthode de connexion au réseau utilisée, l'entreprise est exposée à de nouvelles vulnérabilités.

Dans le cadre de ses missions de sécurité économique et de protection du patrimoine, la DGSI a traité plusieurs cas d'atteintes à des systèmes d'information perpétrés par un prestataire, au cours ou à l'issue de sa mission. D'autres cas relèvent d'intrusions dans les systèmes d'information du prestataire en vue d'atteindre l'entreprise ou l'administration ayant sollicité le sous-traitant.

1er exemple : les problèmes liés à un sous-traitant durant une prestation

Une administration a accueilli dans ses locaux les employés du sous-traitant pour un projet de refonte de son système d'information. Les accès informatiques nécessaires pour mener à bien la mission leur ont été octroyés. Après avoir constaté des irrégularités dans le système d'information, l'équipe de sécurité de l'administration cliente a découvert que l'un de ces employés ne respectait pas la charte informatique et utilisait du matériel informatique personnel non déclaré.

Après enquête, il s'est avéré que ce prestataire exfiltrait de l'information sensible et menait des actions informatiques au sein de l'administration elle-même, afin d'augmenter ses privilèges au sein du système d'information de celle-ci.

2ème exemple : malveillance d'un sous-traitant à l'issue d'un contrat de prestation non renouvelé

Une entreprise a subi des attaques provoquant l'indisponibilité de son système d'information, ainsi que la perte de données sauvegardées. Après investigations techniques, il a été démontré que le dysfonctionnement provenait d'un compte administrateur mis à disposition de prestataires.

Il est apparu que l'ancien sous-traitant, dont le contrat était arrivé à terme et n'avait pas été renouvelé, disposait toujours des droits d'accès au réseau du client et au compte administrateur.

Animé par un esprit de vengeance, ce prestataire a exfiltré des données sensibles et mené des actions de sabotage (suppression de données).

3ème exemple : Ingérence à l'encontre d'un prestataire pour compromettre le système d'information de l'entreprise cliente

Une entreprise ayant fait appel à un prestataire pour mener à bien des projets d'ingénierie, a interconnecté une partie de son réseau avec celui du sous-traitant afin de permettre des opérations à distance. Quelques mois après, l'entreprise a été victime d'une compromission importante de son système d'information.
Après enquête, il s'est avéré que le prestataire avait fait l'objet d'une compromission de son système d'information, dont l'objectif était d'accéder au système d'information du client final afin d'en exfiltrer des données sensibles.

Préconisations de la DGSI

Afin de réduire les risques d'atteintes aux systèmes d'information, dont ceux de captation et d'exfiltration de données sensibles, la DGSI recommande d'appliquer les bonnes pratiques suivantes :

En amont d'une prestation :

Bien définir le périmètre et les modalités d'interconnexion :

- Cloisonner au maximum le réseau informatique accueillant les prestataires
- Créer des comptes utilisateurs temporaires pour les prestataires et ne leur octroyer que les droits strictement nécessaires aux missions confiées ;

Bien définir les modalités contractuelles de la prestation :

- Prévoir contractuellement et de manière précise les missions et obligations des prestataires ;
- Inclure une clause de confidentialité dans les contrats de prestation, couvrant toutes les informations et données relatives à l'entreprise, dont le prestataire pourrait être amené à prendre connaissance ;
- Privilégier le recours à des entreprises européennes (siège social dans l'UE) afin de ne pas s'exposer à des législations étrangères défavorables et à portée extraterritoriale ;
- Assurer le suivi des informations et données détenues par le prestataire ; s'assurer, le cas échéant, que ces dernières sont stockées sur des serveurs situés dans l'Union Européenne ;

- Procéder à toute vérification qui paraîtrait utile pour vérifier le respect de la clause de confidentialité prévue par le contrat.
- Exiger un niveau de sécurité informatique minimal du prestataire (dispose-t-il d'une politique de sécurité des systèmes d'information ? réalise-t-il des audits de ses systèmes informatiques régulièrement ? Ses salariés sont-ils sensibilisés à la sécurité informatique ?)

Durant la prestation :

- Superviser la sécurité, le maintien en condition opérationnelle et de sécurité des équipements utilisés par le prestataire ;

- Surveiller l'ensemble des activités du prestataire (accès, changement de personnels, journaux d'évènements réseau) ;
- Nommer un référent pour assurer le bon déroulement du projet et veiller à ce que les règles informatiques et contractuelles soient appliquées ;

Après la prestation :

- Couper l'ensemble des flux réseaux et interconnexions avec le prestataire ;
- Suspendre l'ensemble des accès et comptes utilisateurs utilisés par les sous-traitants avant de les supprimer, le cas échéant.
- Superviser les équipements du réseau ayant été utilisés par le prestataire afin d'exclure toute malveillance potentielle.
- Rapporter aux responsables de l'entreprise et de l'administration et, le cas échéant, aux autorités, les incidents constatés.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash-ingérence économique

Risques générés par le manque d'encadrement des stagiaires au sein des structures publiques et privées

Les entreprises et laboratoires ont tous recours à des personnels temporaires étudiants (stagiaires ou alternants), présents dans leurs locaux pour une durée s'étalant parfois sur plusieurs mois.

Ce phénomène est accentué par l'internationalisation des échanges économiques et des savoirs, notamment par le biais d'échanges universitaires, favorisant l'accueil de stagiaires étrangers dans les structures publiques et privées françaises. Certains pays incitent d'ailleurs fortement leurs étudiants à favoriser un cursus universitaires à l'étranger, par le biais d'autorisations spécifiques et de soutiens officiels, notamment financiers. Ces étudiants se retrouvent ainsi dans des programmes de formations français qui requièrent d'effectuer un stage d'application.

Ces missions de stages sont réalisées notamment dans entreprises ou laboratoires de secteurs stratégiques ou innovants (industrie de pointe, recherche, start up innovantes). Les stagiaires, alors totalement intégrés aux équipes, peuvent avoir accès à des informations sensibles ou stratégiques de l'entreprise, constitutif d'une potentielle vulnérabilité si jamais le périmètre d'accès de la personne n'a pas été bien défini en amont.

1er exemple

Un employé binational du secteur des fusions-acquisitions, a copié des données sensibles d'un serveur chiffré grâce notamment à une carte d'identification et des codes d'accès appartenant à un stagiaire présent dans l'entreprise à ce moment-là. Après avoir récupéré les documents sur un serveur non-sécurisé, l'employé les a envoyés sur sa messagerie personnelle. Parmi les pièces copiées, figuraient des documents concernant des contrats de vente sensibles, co-traités avec une entreprise tierce pour qui cette captation frauduleuse est également dommageable. Ces documents étaient tous strictement confidentiels.

Bien que les accès informatiques dans l'entreprise aient fait l'objet de cloisonnement, l'employé de l'établissement a pu avoir accès au serveur chiffré via les identifiants du stagiaire car il était d'usage que ces derniers les laissent à disposition des autres employés pour des raisons pratiques de connexions à certaines applications. Cette négligence concernant les droits informatiques a ainsi créé une vulnérabilité pour l'entreprise.

2ème exemple

Un élève ingénieur étranger, employé en tant qu'apprenti sur un site industriel de matières premières sur le territoire national, a quitté son lieu d'emploi en omettant de restituer le fichier informatique contenant le « plan de sécurisation » de l'unité pour laquelle il travaillait. Ce document intégrait les analyses des équipements et définissait leurs défaillances et points de vulnérabilités. Malgré les tentatives de récupération de la part de l'entreprise, l'ex stagiaire, qui n'a pu être contacté immédiatement, n'a restitué les documents que 4 mois après son départ, prétextant penser les avoir rendu en partant. Il a par ailleurs précisé être retourné dans son pays d'origine.

L'incident a fait prendre conscience au responsable sûreté du site des lacunes dans le suivi et l'encadrement des stagiaires concernant les supports informatiques dont ils sont détenteurs le temps de leurs contrats.

3ème exemple

Une unité mixte de recherche médicale française, travaillant sur des sujets sensibles dans des domaines de pointe a accueilli en son sein un stagiaire d'origine étrangère dans le cadre d'un programme universitaire d'échange. Son encadrement a rapidement identifié un décalage entre son curriculum vitae et son niveau de compétence réel, jugé faible. L'attitude de l'étudiant a en outre attiré l'attention du personnel du laboratoire. Ce dernier s'est en effet montré particulièrement intéressé par des domaines n'intéressant pas ses travaux, et a été surpris prenant des clichés photographiques de certaines zones du laboratoire. Il s'est également intéressé aux disques durs de sauvegarde du laboratoire et a tenté de filmer une expérience résumant toutes les manipulations d'un personnel du labo.

Après recherche il est apparu que le stagiaire avait des intérêts dans plusieurs sociétés ou laboratoires concurrents de l'établissement français.

4ème exemple

Une entreprise française spécialisée dans la R&D pour la machinerie industrielle, travaille à un projet de joint-venture avec un intermédiaire étranger pour l'obtention d'un marché dans ce pays. Dans le cadre de ce projet, le PDG de l'entreprise étrangère a fortement « suggéré » de former de manière régulière deux ou trois étudiants originaires de son pays sur les sites hexagonaux de l'entreprise française afin de les former et les embaucher à termes dans la joint-venture. Le directeur de l'entreprise française s'est montré hostile à cette proposition, une salarié de son entreprise ayant surpris les stagiaires dans des parties de l'établissement qui leur était interdites, notamment les bureaux de R&D. Les stagiaires sont en outre apparus peu qualifié pour les tâches qui leur étaient demandées.

5eme exemple

Un stagiaire effectuant sa mission dans le Service SSI d'une administration et travaillant sur l'architecture dudit établissement a sollicité l'aide d'un de ses enseignants afin de trouver la solution à un problème. Pour ce faire, il a envoyé à son professeur une copie de l'architecture concernée afin qu'il puisse l'aider dans sa recherche exposant ainsi des données stratégiques pour l'établissement.

Commentaires

La présence de stagiaires au sein d'entités françaises est inévitable et constitue une richesse pour le rayonnement de l'établissement.

Cependant, au regard des exemples cités, même s'il n'est pas toujours prouvé que la démarche des stagiaires ait été frauduleuse ou malveillante, leur présence n'en constitue pas moins une potentielle source de vulnérabilité pour le patrimoine d'une entreprise ou le potentiel scientifique technique national.

En outre, il est à noter que certains concurrents ou pays tiers n'hésitent pas à « placer » des stagiaires dans le but de capter des informations ou de les faire bénéficier de formations à bon compte sur des technologies non maîtrisées.

Les manquements aux règlements de l'entreprise ou l'accès à des données confidentielles, sont souvent favorisés par une politique d'accueil des stagiaires floue de la part des établissements. Le traitement de ces personnels temporaires est trop fréquemment négligé alors qu'ils devraient être informés et soumis aux mêmes obligations que l'ensemble du personnel de l'entreprise (signature de charte informatique, accord de confidentialité…). Leurs accès physiques et informatiques doivent également être précisément déterminés et restreints aux seuls travaux qui les intéressent. Par ailleurs, il est important de sensibiliser les référents de stage à la nécessité de remonter tout comportement anormal aux personnes en charge de la sécurité.

Ajoutons qu'en cas de vol ou de fuite de données, **le Règlement général sur la protection des données[1] exposera les entreprises et administrations qui n'auront pas mis en œuvre toutes mesures techniques et organisationnelles appropriées pour s'assurer de la protection des**

[1] Le Règlement général sur la protection des données est un règlement européen qui entrera en vigueur le 25 mai 2018.

données à caractère personnel à de substantielles amendes (de 2% à 4% du chiffre d'affaires annuel mondial pour les grands groupes, et 10 à 20 millions d'euros pour les autres entreprises).

Préconisations de la DGSI

Compte de la présence de plus en plus fréquente de stagiaires étrangers dans les entreprises, la DGSI émet les préconisations suivantes :

- Identifier précisément le périmètre d'accès physique du stagiaire. Limiter si possible son accès à l'entreprise aux heures ouvrables afin d'éviter qu'il se retrouve seul dans l'établissement
- Limiter les accès informatiques, notamment concernant des données sensibles ou stratégiques
- Faire signer au stagiaire la charte informatique de l'établissement (non partage des codes d'accès, identifiants etc.)
- Faire signer un engagement de sécurité/confidentialité et avertir les stagiaires des sanctions en cas de non-respect des consignes interne à l'entreprise
- Sensibiliser le maître de stage/référent sur les risques potentiels afin que reste vigilant quant à l'encadrement du stage et fasse remonter tout comportement suspect. Dans la même optique, sensibiliser les personnels de l'équipe afin qu'ils veillent à respecter la politique de confidentialité des données

Les déplacements à l'étranger, un risque important de captations d'informations

Un agent travaillant sur des questions de défense et de sécurité au sin d'une administration a récemment fait l'objet d'un contrôle intrusif en zone internationale de l'aéroport de Roissy-Charles de Gaulle, alors qu'il s'apprêtait à partir en congés dans un pays étranger en compagnie d'une relation.

Au moment de l'enregistrement des bagages, deux agents se réclamant de la compagnie aérienne concernée les ont séparés et interrogés de façon concomitante. Outre les questions habituelles de sécurité (motif et adresse du séjour dans le pays de destination, voyages antérieurs, situation maritale, etc.), l'agent a posé à l'intéressé un certain nombre de questions précises sur sa profession et son employeur. Ce dernier a précisé la qualité de son employeur, sans pour autant révéler la nature réelle de ses fonctions. A la fin de l'interrogatoire, l'agent a signalé au fonctionnaire qu'il ferait l'objet d'un deuxième contrôle en zone internationale, après le passage en douane.

Arrivé à la salle d'embarquement, le fonctionnaire français a été interpellé par un autre agent de la compagnie aérienne qui lui a demandé de le suivre pour procéder, comme convenu, aux formalités de contrôle. L'intéressé a été conduit dans une salle sécurisée de l'aéroport, où les mêmes questions sur son environnement personnel et professionnel lui ont été posées. Le contenu de son bagage à main a par ailleurs été entièrement contrôlé et l'agent a également examiné pendant quelques instants son téléphone portable. Le fonctionnaire n'a pas pu constater les actions effectuées sur son téléphone, l'intervenant opérant dos tourné. En tout état de cause, le téléphone était verrouillé et le code d'accès n'a pas été sollicité.

De retour dans la salle d'embarquement, le fonctionnaire a reçu la consigne de rester à proximité de l'agent qui l'avait interrogé la première fois, jusqu'à sa montée dans l'avion.

Arrivé dans le pays de destination, le téléphone de l'intéressé n'a pas fonctionné pendant trois jours, aucun appel ne pouvant être émis depuis l'appareil. Passé ce délai, le téléphone n'a plus présenté de dysfonctionnements. Par ailleurs, aucun problème n'a été constaté par le fonctionnaire pendant son séjour.

Commentaires

Cette situation pourrait s'avérer anecdotique si l'environnement professionnel de l'intéressé et le contenu de son téléphone ne présentait pas un caractère sensible. Il travaille en effet dans un service qui traite de questions liées à la sécurité de certaines informations stratégiques et son téléphone contenait les noms et coordonnées téléphoniques professionnelles de ses collègues. De plus, sa messagerie professionnelle pouvait être consultée depuis internet, donc depuis son téléphone, ce dernier pouvant conserver l'historique des messages échangés.

Dans le cas d'espèce, rien ne prouve que des informations sensibles ont été récupérées par l'agent ayant procédé à l'interrogatoire, dans la mesure où le téléphone était protégé par un code de verrouillage, ce qui rend l'accès au contenu de ce dernier plus difficile à mettre en œuvre. Néanmoins, le risque de captation d'informations dans ce type de situation peut s'avérer bien réel, avec pour conséquences potentielles une captation de données se rapportant à des dossiers sensibles.

Sous couvert de lutte contre le terrorisme, les contrôles opérés par certains états dans les aéroports, bien que légitimes dans leur principe au vu des enjeux sécuritaires actuels, peuvent cependant donner lieu à des actions relevant de l'ingérence. Des agents appartenant à des services de renseignement étrangers peuvent agir dans les zones internationales des aéroports et profiter des vérifications de sécurité sur des passagers pour récupérer données et informations. Des cadres d'entreprises ont déjà fait l'expérience de ce type contrôles intrusifs, y compris au moment du passage en douane une fois arrivés à destination (exigence de remise de smartphones ou d'ordinateurs portables par les autorités aux fins de « vérifications », la détention des appareils pouvant durer de longues minutes).

Préconisations de la DGSI

Les déplacements à l'étranger impliquent une préparation avant le départ. Dans le cadre de ses missions de sécurité économique, et de contre-ingérence, la DGSI émet les préconisations suivantes (liste non-exhaustive) :

Avant le départ :

- Se renseigner sur la situation politique et sécuritaire du pays de destination, ainsi que sur les législations locales en termes de contrôle aux frontières. Cette préparation permet d'assurer la sécurité de la mission et d'anticiper les difficultés que pourraient poser des contrôles intrusifs opérés par/dans certains pays.

Privilégier l'utilisation de matériel nomades dédiés exclusivement à la mission. Cette pratique permet de limiter le stockage d'informations et de documents sensibles/stratégiques aux seuls besoins de la

mission. Les ordinateurs portables et smartphones doivent être expurgés de toute donnée sensible et l'accès à leur contenu doit être protégé par des mots de passe forts, personnels et secrets.

Pendant le déplacement

- Dès l'arrivée dans le pays, signaler sa présence aux autorités officielles françaises (ambassade ou consulat

- Conserver sur soi, pendant toute la durée du déplacement, tous les appareils électroniques et ne pas les laisser dans les coffres forts des hôtels. Le personnel des hôtels peut être amené à visiter votre chambre en cotre absence et à ouvrir le coffre à l'aide d'un double de la clef ou d'un mot de passe « maître » pour se livrer à un vol d'informations. Si vous êtes contraint de vous séparer, par exemple, de votre smartphone, retirer et conserver sur vous la carte SIM, ainsi que la batterie dans la mesure du possible

- Eviter de connecter ses appareils électroniques à des postes ou périphériques informatiques qui ne sont pas de confiance. Si vous avez besoin d'échanger des documents, privilégier l'utilisation d'une clé USB et effacer ensuite le contenu avec un logiciel d'effacement sécurisé

- Apposer un filtre de confidentialité sur son écran d'ordinateur pour empêcher les regards indiscrets. A défaut, si vous travaillez dans les transports en commun, votre voisin peut jeter des regards sur votre écran d'ordinateur à votre insu

- En cas de perte ou de vol de matériels, ou de contrôle par les autorités locales, informer immédiatement son responsable hiérarchique et demander conseil aux autorités officielles françaises (ambassade ou consulat) avant toute démarche auprès des autorités locales

- Se méfier des rencontres professionnelles ou amicales « spontanées ». Ces rencontres peuvent aspirer à sympathiser avec vous pour vous faire parler.

Au retour :

- Rédiger un rapport d'étonnement à l'attention de son responsable hiérarchique et de son référent sûreté pour tout problème de sécurité et signaler tout comportement qui aurait pu retenir l'attention. La DGSI pourra au besoin être alertée par les personnes référentes au sein de l'entité

- Analyser ou faire analyser tout particulièrement les appareils électroniques ayant échappé à votre surveillance à un moment ou à un autre.

A toutes fins utiles, vous trouverez diverses informations utiles à la préparation d'un voyage sur les sites internet suivants :

Site du Service à l'information stratégique et à la sécurité économiques (SISSE) www.entreprises.gouv.fr/information-stratégique-sisse

Site de l'Agence nationale de sécurité des systèmes d'information (ANSSI) www.ssi.gouv.fr

Site du ministère de l'Europe et des Affaires étrangères (MEAE) www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs.html

Site du Club des directeurs de Sécurités des entreprises (CDSE) www.cdse.fr

Les risques liés à l'hébergement des données dans les *data centers* / le *cloud*

L'augmentation constante de la masse des données hébergées à l'aide des techniques d'informatique en nuage[2] représente un enjeu majeur pour la sécurité des informations sensibles des entreprises.

En effet, les données hébergées dans le nuage sont traitées au sein de centres de données[3] dont la maîtrise par le client est limitée et essentiellement d'ordre contractuel. En particulier, la connaissance de la localisation exacte des données est difficile, celles-ci étant réparties entre plusieurs centres géographiquement distincts (pour des questions de résilience notamment) et faisant l'objet de transferts à des fins de rationalisation et d'optimisation des flux de données.

Ces services permettent aux entreprises de bénéficier de solutions d'hébergement ou de traitement de données souples, évolutives, faciles d'emploi et accessibles en tout point du globe.

Cette forme avancée de sous-traitance de la gestion des systèmes d'information **induit en contrepartie d'importants risques pour la sécurité des données des entreprises, françaises en l'espèce.** Ces données sont en effet susceptibles de faire l'objet d'interceptions ou de captations, à tout moment de leur cycle de vie (au cours de leur acheminement sur Internet, durant leur stockage sur des serveurs à distance, lors du transfert au sein d'un autre centre de données, etc.).

Or, les serveurs situés à l'étranger et notamment ceux des centres de données, sont soumis à la réglementation des États qui les hébergent. Les législations de la plupart des pays prévoient ainsi la possibilité, pour les services de police et de sécurité, d'accéder aux données hébergées sur leur territoire. Par ailleurs, certaines autorités peuvent parfois invoquer un motif de sécurité nationale, ou d'autres impératifs d'ordre public, pour justifier l'accès aux données des clients des prestataires. En effet, certains États, grâce à un cadre juridique adapté et à une définition large des enjeux relevant de la sécurité nationale, peuvent enjoindre les prestataires de leur nationalité, même localisés dans un autre pays, de transmettre des données concernant des clients étrangers.

1er exemple

Un prestataire extra-européen d'hébergement de données a refusé de transmettre à son gouvernement des courriels hébergés sur ses serveurs situés à l'étranger. Si une décision de justice lui a donné raison,

[2] L'information en nuage ou *cloud computing* se définit comme un « *mode de traitement des données d'un client, dont l'exploitation s'effectue par l'Internet, sous la forme de services fournis par un prestataire* », même si des solutions de *cloud* privé, au sein desquels les données ne transitent qu'à travers le réseau d'un opérateur de télécommunication, peuvent être mises en œuvre.

[3] Un centre de données ou *data center* est un centre d'hébergement et de traitement de données à distance pour les entreprises et les administrations, abritant un nombre important de serveurs et d'équipements informatiques tout en fournissant une sécurité physique et une continuité d'activité.

cette jurisprudence demeure fragile et d'autres prestataires ont pu se voir contraints de transmettre à leurs autorités des emails stockés en dehors de leur territoire national.

Ainsi, certains pays, qui ont fait de l'économie un enjeu majeur pour leur sécurité nationale, utilisent ces instruments légaux pour collecter des informations relevant de cette sphère d'activité.

2ème exemple

Une société française spécialisée dans la pharmaceutique vétérinaire a choisi d'externaliser le stockage de ses données vers une solution de *cloud* gratuite d'un prestataire étranger.

Il a alors été constaté que l'hébergeur de données étranger était soumis à une législation différente, plus souple en matière de collecte de renseignements. Cette entreprise française comptant par ailleurs parmi ses concurrents plusieurs groupes de la nationalité de l'hébergeur, la société tricolore s'expose ainsi à un risque accru d'espionnage économique de ses données stratégiques.

Commentaires

Les risques de l'hébergement de type *cloud* dans des centres de données restent encore **largement sous-estimés.**

Nombreuses sont les sociétés persuadées que les interceptions/captations de données par des puissances étatiques s'inscrivent exclusivement dans le cadre de la lutte contre le terrorisme ou la criminalité organisée. Elles ne se considèrent ainsi pas menacées par le risque de captation de leurs données stratégiques hébergées dans le *cloud*.

Par ailleurs, les solutions de stockage ou de traitement des données à l'étranger sont parfois considérées comme offrant un plus haut niveau de sécurité et des services plus performants que les solutions nationales. Certains prestataires étrangers proposent à cet égard des fonctionnalités avancées, très prisées des entreprises qui se développent à l'international, et à un moindre coût.

En outre, pour rassurer leurs clients face à la **portée extraterritoriale de certaines législations**, et plus largement aux risques d'interception de leurs données par des gouvernements étrangers, certains prestataires extra-européens ont décidé de confier la gestion de leurs centres de données à des groupes européens. Cette solution apparaît toutefois insuffisante pour garantir la protection des données hébergées. En effet, même si les centres de données sont exploités par des opérateurs européens, des entreprises non-européennes conservent régulièrement la maîtrise de l'architecture matérielle et logicielle des installations.

Préconisations de la DGSI

Face au risque d'interception et aux pratiques de certains prestataires, la DGSI émet les préconisations suivantes pour tenter de limiter les risques de captation du patrimoine informationnel des entreprises utilisant les *datas centers* / le *cloud* :

- S'agissant des centres de données localisés sur le territoire national, veiller à accorder une attention particulière aux conditions générales de vente et d'utilisation. Il convient, pour les entreprises, de s'assurer que le contrat ne permet pas le transfert des données hébergées en France vers un pays tiers.

- Préférer des prestataires français, ou à défaut européens, dont les serveurs sont situés dans l'Hexagone ou dans un pays membre de l'Union européenne.

- Bannir l'utilisation des services, gratuits ou non, d'hébergement dans le *cloud*, autorisant l'accès aux données hébergées à des fins publicitaires.

- Distinguer le traitement des données non sensibles, stockables dans le *cloud*, des informations à forte valeur ajoutée économique, stratégique ou financière, à conserver dans des infrastructures internes à l'entreprise.

- Procéder systématiquement au **chiffrement** de l'ensemble des données transférées sur un service d'hébergement à distance. Ce chiffrement doit être effectué par l'entreprise elle-même et non par ses prestataires, ou via les outils de ces derniers.

- Limiter les droits des utilisateurs des services dans le nuage, ne pas utiliser de compte administrateur pour les tâches quotidiennes, surveiller les logs de connexion et assurer une gestion rigoureuse des droits d'accès pour éviter toute usurpation d'identité.

- Procéder à un audit des infrastructures techniques hébergeant les données de l'entreprise et s'assurer du respect des stipulations contractuelles.

- Contacter la DGSI en cas de découverte ou de suspicion d'un cas d'ingérence ou d'interception de données.

Les dangers liés aux objets connectés

L'engouement massif pour les objets connectés ne se limite pas seulement au grand public. Le phénomène concerne également de plus en plus les entreprises.
Qu'il s'agisse d'équipements personnels (bracelets, montres, cigarettes électroniques, etc.) apportés et utilisés au sein des locaux de l'entreprise par les salariés / visiteurs ou de matériels acquis et déployés par l'entreprise, la présence de ces objets connectés se multiplie dans le monde professionnel.

Les objets connectés sont également de plus en plus utilisés pour des applications industrielles (afin d'optimiser la traçabilité des marchandises et la logistique, par exemple). On parle désormais d' « Industrie 4.0 » avec des usines connectées et « intelligentes » pour gagner en compétitivité. Mais ces équipements présentent des vulnérabilités intrinsèques et des risques liés aux nouveaux usages rendus possibles grâce à une connectivité quasi continue à Internet.

Voici deux exemples représentatifs de ces nouveaux scénarii de menaces :

1er exemple : Augmentation de la surface d'attaque des entreprises

De plus en plus d'entreprises françaises s'équipent avec du matériel « connecté » dédié à la sécurité physique (alarme, détecteur de fumée, serrure, caméra de vidéo-protection, etc.). Ces systèmes sensibles sont reliés aux réseaux informatiques de l'entreprise voire accessibles depuis Internet. Ces équipements de sécurité présentent également des failles de sécurité (identifiant et mot de passe par défaut, protocoles de communication non chiffrés, interface d'administration exposée à Internet, etc.) les exposent à des attaques informatiques. Ces dernières peuvent être exploitées dans le but de désactiver l'équipement mais également pour servir de point d'entrée pour réaliser une intrusion plus classique dans les réseaux informatiques de l'entreprise.

Le risque est d'autant plus grand qu'identifier des objets connectés vulnérables est facilité par des sites Internet comme *Shodan.io* ou *Censys.io*, des moteurs de recherche spécialisés qui référencent tout type d'équipement connecté à Internet.

2ème exemple : Piratage d'une montre connectée

Des chercheurs en sécurité informatique ont montré qu'il était possible de compromettre à distance des montres connectées afin de prendre le contrôle de leurs capteurs (microphone, mesure du

rythme cardiaque, etc.) ou d'accéder aux données échangées entre la montre et le smartphone auquel elle est reliée.

Commentaires

Le nombre d'objets connectés en circulation à travers le monde explose depuis quelques années. Estimé à 15 milliards aujourd'hui, ce chiffre pourrait atteindre les 80 milliards en 2020.
Ces objets connectés collectent et génèrent un nombre très important de données à caractère personnel qu'il est difficile de maîtriser et de sécuriser. Conçus généralement sans intégrer de façon native de mécanismes de sécurité (chiffrement par exemple), ils présentent également des vulnérabilités intrinsèques qui sont autant de portes d'entrée dans les réseaux informatiques des entreprises.

Si l'utilisation d'objets connectés dans un contexte professionnel peut permettre d'améliorer la compétitivité de l'entreprise, des mesures doivent être prises pour anticiper et prévenir les nouveaux risques qu'un usage non maîtrisé peut entraîner.

Préconisations de la DGSI

Afin de réduire les risques liés à l'utilisation d'objets connectés en milieu professionnel, la DGSI recommande d'appliquer les bonnes pratiques suivantes :

- Recenser et réaliser une veille sur les vulnérabilités des objets connectés en activité dans l'entreprise ;
- Interroger les fournisseurs d'objets connectés sur les mesures de sécurité implémentées dans leurs produits :

➢ Si c'est possible, il est recommandé de réaliser ou de faire réaliser un comparatif de différents modèles d'objets connectés en intégrant une évaluation technique de son niveau de sécurité.

- Encadrer l'usage des objets connectés personnels dans une charte de bonnes pratiques ou dans la politique de sécurité des systèmes d'information (PSSI) ;
- Réaliser une analyse de risque avant d'autoriser et de déployer des objets connectés sur les systèmes d'information de l'entreprise ;
- Créer des réseaux Wi-Fi ou filaires dédiés et cloisonnés à l'utilisation des objets connectés.
- Désactiver l'interface d'administration sur Internet, si elle est proposée par le fournisseur du produit :

➢ Changer les mots de passe par défaut, le cas échéant.

- Déployer régulièrement les mises à jour des produits, quand celles-ci sont proposées par le fournisseur ;
- Sensibiliser les utilisateurs aux vulnérabilités qui sont liées aux objets connectés et notamment sur les données à caractère personnel qu'ils collectent, génèrent et transfèrent sur des services Cloud.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash-ingérence économique

Les dangers liés aux Wi-Fi publics

Depuis plusieurs années, la DGSI a connaissance de compromissions informatiques, conséquences d'une utilisation imprudente de Wi-Fi publics.

Voici deux exemples représentatifs des risques liés au faible niveau de sécurité de ce type d'équipement :

1er exemple

Le directeur commercial d'une PME française a vu sa messagerie électronique compromise, alors qu'il se rendait à une conférence internationale à l'étranger. A l'arrivée dans le pays de destination, il avait en effet activé la fonction Wi-Fi de son smartphone pour consulter ses courriels professionnels.
Quelques heures plus tard, il recevait des courriels de plusieurs collègues lui signalant qu'il leur avait envoyé des messages inhabituels, écrits en anglais, les invitant à cliquer sur un lien suspect. Il constatait également qu'une partie de sa boîte de réception avait été effacée.

2ème exemple

« DarkHotel » est un groupe de pirates informatiques, identifié fin 2014 par un éditeur de sécurité informatique, spécialisé dans le piégeage des réseaux Wi-Fi d'hôtels asiatiques dans lesquels séjournent de nombreux cadres d'entreprises en voyage d'affaires.

Le mode opératoire des attaquants consiste notamment à pirater les portails d'identification au réseau Wi-Fi des hôtels. En se connectant, les victimes sont incitées à télécharger des fausses mises à jour pour des logiciels comme Adobe Flash ou des barres d'outils Google.
Il s'agit en réalité de maliciels qui vont permettre aux pirates informatiques de prendre le contrôle de la machine de la victime pour exfiltrer de l'information sensible.

Commentaires

Aujourd'hui, la plupart des lieux publics (restaurants, cafés, aéroports, hôtels, centres commerciaux, gares, etc.) en France et à l'étranger, proposent à leurs clients ou aux simples visiteurs un accès gratuit à Internet via des réseaux Wi-Fi.
Dans le cadre de déplacements professionnels mais également personnels, il est alors tentant d'y connecter son smartphone, sa tablette ou son ordinateur portable afin d'accéder à diverses ressources

informatiques (messageries électroniques, compte bancaire, réseaux sociaux, extranet, espace de stockage en ligne, etc.).
Malheureusement, ces accès publics sont généralement vulnérables, en raison d'un faible niveau de sécurité.

Des utilisateurs malveillants peuvent notamment exploiter ces failles pour intercepter les communications (identifiants de connexion à des messageries électroniques, mots de passe, numéro de carte bancaire, historique de navigation Internet, etc.) transitant par ces points d'accès Wi-Fi. Il est également très facile pour des pirates informatiques de créer de vrais-faux réseaux Wi-Fi usurpant le nom d'une enseigne reconnue, accessibles gratuitement et sans mot de passe. Cette manoeuvre leur permet de récupérer des informations techniques sur les systèmes ainsi que de nombreuses données personnelles et sensibles facilitant de nouvelles intrusions informatiques.

Préconisations de la DGSI

Afin de réduire les risques de vol de données sensibles d'une connexion à un Wi-Fi public, la DGSI recommande d'appliquer les bonnes pratiques suivantes :

- Privilégier des connexions cellulaires en 3G/4G, en France et à l'étranger, pour des usages professionnels ;
- Utiliser obligatoirement un VPN en cas d'utilisation d'un point d'accès Wi-Fi public ;
- Désactiver le mode Wi-Fi quand il n'est pas utilisé ;
- Mettre à jour régulièrement le système d'exploitation, le navigateur Internet (et ses extensions), son antivirus et les logiciels comme Adobe Reader et Flash ;
- Privilégier les sites Internet sécurisés utilisant du HTTPS (une extension à installer sur les navigateurs Internet telle que HTTPSANYWHERE permet également d'automatiser le passage de certains sites Internet en HTTPS).

En cas de doute après avoir été connecté à un Wi-Fi public :

- Changer rapidement les mots de passe des applications (messageries électroniques, réseaux sociaux, comptes bancaires, espace de stockage en ligne, etc.) que vous utilisez le plus souvent.

Les risques cyber liés aux rançongiciels

Un rançongiciel est une forme d'attaque informatique visant à extorquer une somme d'argent à un utilisateur *via* l'infection de son périphérique. L'outil malveillant bloque le matériel ou chiffre les données afin de rendre impossible tout travail sur ce dernier. Une rançon est demandée en contrepartie du rétablissement de l'accès au périphérique ou de la fourniture d'une clé de déchiffrement. En pratique, le périphérique touché affichera le plus souvent une fenêtre *pop-up* avec les instructions permettant le déverrouillage. La pression psychologique de l'attaque sur l'utilisateur peut être renforcée par la présence d'un chronomètre qui affiche le temps restant jusqu'à l'augmentation de la rançon, la destruction des données ou leur diffusion en clair sur les réseaux.

Le paiement de la rançon est régulièrement demandé en crypto-monnaie – *Bitcoin* la plupart du temps – ce qui permet de masquer l'identité de l'attaquant et d'entraver les actions de suivi (pas de trace liée à l'existence d'un compte bancaire nominatif, pas de rencontre physique pour paiement en liquide, etc.). Les rançongiciels sont le plus souvent utilisés par le milieu cybercriminel, mais la facilité d'accès à de tels outils sur le *Dark Web* les rendent utilisables par des attaquants disposant d'un plus faible niveau de technicité.

Si les modes de propagation sont variés, la diffusion de pièces jointes par courrier électronique reste le mode d'infection le plus courant avec la mise à disposition d'un lien vers un site Internet ayant une apparence authentique. Le facteur humain est déterminant dans la réussite d'une tentative d'infection, celle-ci dépendant fortement de l'inattention de l'utilisateur.

1er exemple : *WannaCry*, plus de 250 000 victimes dans le monde en mai 2017

WannaCry est un rançongiciel tirant profit d'une vulnérabilité de certains systèmes d'exploitation Windows, dévoilée par une entité connue sous le nom de *ShadowBrokers*, qui l'attribue à la NSA. L'outil malveillant a permis d'infecter des cibles telles que *Téléfonica* en Espagne, le *National Health Service* au Royaume-Uni ou encore certaines usines de Renault en France. L'impossibilité d'accéder aux postes touchés a obligé l'arrêt de la production au sein de certaines entreprises, impliquant des pertes financières non négligeables.

2ème exemple : *Locky*, plus d'un million de victimes en 2016

Découvert pour la première fois en février 2016, *Locky* a touché des cibles dans la plupart des pays. Une pièce jointe malveillante prenant la forme d'une facture reste le principal mode de propagation

de ce rançongiciel. L'utilisateur ayant ouvert le fichier Word et activé les macros voit l'intégralité de ses fichiers chiffrés. Une fenêtre *pop-up* explique le fonctionnement et guide l'utilisateur jusqu'au paiement de la rançon, allant de 200 à 1000€. *Locky* a connu plusieurs versions. Il serait l'œuvre d'un groupe ayant déjà conçu un rançongiciel du nom de *Dridex* en 2015.

Préconisations de la DGSI

La DGSI recommande quelques actions visant à se prémunir au mieux des risques inhérents aux rançongiciels :

En amont de l'infection :

- Sensibiliser son personnel : l'infection s'effectue souvent par une pièce jointe frauduleuse reçue par courriel électronique sous une forme légitime (facture, bon de livraison, etc.). L'ouverture d'une seule de ces pièces jointes peut suffire à propager l'infection sur l'ensemble des systèmes d'information de l'entreprise. Il est donc essentiel de sensibiliser son personnel quant aux risques inhérents à l'ouverture des documents provenant d'émetteurs inconnus et/ou douteux ;

- Utiliser un outil de filtrage de courriers électroniques en plus d'une solution anti-virus efficace ;

- Effectuer fréquemment les mises à jour des systèmes d'exploitation et programmes ;

- Avoir une politique de sauvegarde de ses données afin de pouvoir les restaurer en cas de problème.

Pendant l'infection :

- Éviter de payer la rançon afin de limiter l'attrait de ces pratiques et de ne pas risquer une nouvelle attaque. Le paiement de la rançon ne garantit pas la récupération des données ou le déverrouillage des postes touchés ;

- Prendre les mesures nécessaires pour circonscrire l'infection sur les systèmes d'information placés sous votre responsabilité et, le cas échant, conserver les preuves relatives à l'attaque ;

- Informer le correspondant de la DGSI ;

- Consulter le site CERT-FR afin de vérifier l'existence d'un bulletin d'alerte, d'une campagne en cours ou de moyens de remédiation contre le rançongiciel qui vous a ciblé.

Après l'infection :

- Déposer plainte auprès des services de police (OCLTIC ou BEFTI) ou de gendarmerie compétents ;

- Effectuer un retour d'expérience sur la gestion de la crise afin de limiter les impacts d'une éventuelle future cyberattaque ;

- Evaluer les solutions de cybersécurité disponibles dans l'hypothèse où l'entreprise ne dispose pas au moment de l'incident des outils d'entrave nécessaires;

- Restaurer le système à l'aide de sauvegardes ou à défaut reformater le disque.

Nota : Il est parfois utile de conserver les supports de stockage infectés, des chercheurs en cybersécurité mettant régulièrement en ligne quelques jours plus tard des méthodes ou des outils de déchiffrement.