Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 33 - Mai 2017

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°33 Mai 2017

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.