Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 52 – Avril 2019

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°52 Avril 2019

Utilisation des attaques informatiques aux fins de déstabilisation d'une entreprise

Au-delà des enjeux liés à l'espionnage, au sabotage ou au terrorisme, une attaque informatique peut être une composante d'une opération plus complexe ou de plus grande ampleur, comme une manœuvre de déstabilisation ou une tentative d'ingérence économique. Ainsi, une exfiltration de données peut renseigner une entreprise sur l'état de santé d'un concurrent ou sur les vulnérabilités d'un cadre dirigeant, tandis qu'un déni de service peut entraver le bon fonctionnement d'une entreprise, notamment en période de forte activité.

L'attaquant ou son commanditaire pourra ainsi obtenir plus facilement une position déterminante pour mettre en œuvre son projet (acquisition, délivrance d'une sanction financière, abandon d'un marché, affaiblissement d'un concurrent, etc.). La DGSI a en effet observé dans certains cas une concomitance entre des attaques informatiques et des faits plus traditionnels de déstabilisation (mouvement de personnel, participation à un marché gouvernemental, prise de capital, etc.).

Ces attaques multi-vectorielles sont d'autant plus difficiles à déceler que l'entreprise est peu préparée ou n'est pas organisée pour disposer d'une approche transversale des risques.

PREMIER EXEMPLE

Une entreprise française proposant des objets numériques à destination du grand public a été victime d'une attaque informatique ciblée. Les attaquants ont en effet visé le poste de travail du chef de projet du produit phare de la société.

L'attaque est intervenue quelques semaines avant Noël, période de grande activité durant laquelle l'entreprise réalise l'essentiel de son chiffre d'affaires. Les équipes étaient par conséquent peu disponibles pour traiter l'incident et leur faible maturité en matière de sécurité, notamment informatique, n'a pas permis aux employés présents de recueillir et d'analyser les éléments permettant de définir précisément quels types de données avaient été exfiltrées.

Plusieurs mois plus tard, un concurrent étranger a commercialisé un nouveau produit dont les caractéristiques étaient visiblement inspirées du modèle conçu par l'entreprise française et proposé à un prix largement inférieur.

À ce jour, il apparait que la société française a perdu sa position de leader sur le marché et connait des difficultés financières importantes.

DEUXIEME EXEMPLE

Une entreprise du secteur industriel dispose d'un établissement en France dédié à la R&D de son produit ainsi qu'à sa commercialisation et d'une zone de production située dans une usine en Asie.

Lors d'une vérification de routine du cycle de production sur le site de l'usine asiatique, un ingénieur a introduit une clé USB pour récupérer des données liées à la production afin de les traiter dans son environnement de développement et de test au sein de l'établissement français, qui dispose d'un réseau distinct, séparé du réseau bureautique.

Quelques jours après que la clé ait été connectée sur un ordinateur du réseau bureautique, le centre de supervision a détecté une requête envoyée de manière irrégulière à un serveur externe depuis différents postes de travail. Une investigation interne a permis de découvrir un code malicieux sur plusieurs postes de travail du réseau bureautique ainsi qu'au sein de l'environnement de test. Le code malicieux disposait d'une porte dérobée (« *backdoor* ») activable à distance et susceptible d'être utilisée pour exfiltrer des données de l'entreprise.

Une enquête ultérieure a démontré que l'usine située en Asie proposait également ses services à un concurrent de l'entreprise.

COMMENTAIRES

Afin de limiter les risques d'ingérence, une attention toute particulière doit être portée à la protection des systèmes d'information, notamment lorsque une entreprise fait face à des événements impactant son fonctionnement et son développement (acquisitions, négociations salariales, réalisation d'audits de conformité [1], bilan annuel, renégociation contractuelle, mouvement de grève, perte d'un collaborateur stratégique [DSI, RSSI, etc.],...).

Il est donc essentiel de se préparer à la gestion d'une crise cyber en amont afin d'être apte à résoudre les incidents qui interviendraient lors de ces moments de vulnérabilité temporaire.

[1] *En particulier dans le cas d'une démarche de mise en conformité soutenue par des cabinets de conseil et des sociétés d'investigation numérique étrangers.*

Par ailleurs, les entreprises doivent prendre conscience des risques de captation d'informations liés à un positionnement sur des marchés stratégiques. Les entités concurrentes peuvent en effet adopter un comportement ingérant, notamment par le biais d'attaques informatiques, pour collecter des informations stratégiques sur leur concurrent, augmenter ses coûts d'acquisition de la clientèle, déstabiliser celui-ci ou se garantir un avantage concurrentiel.

PRECONISATIONS DE LA DGSI

Afin de réduire ces risques, la DGSI recommande d'appliquer les bonnes pratiques suivantes :

→ Le cas échéant, veiller, au sein de l'organisation interne de l'entreprise, à la création ou au renforcement d'une structure en charge de l'identification des menaces et de la détection des opérations sensibles susceptibles d'induire des vulnérabilités supplémentaires.

→ Adopter une approche transversale des risques permettant d'appréhender de manière globale les risques techniques, organisationnels et humains liés à l'activité de l'entreprise.

→ Inclure les fournisseurs dans la gestion des risques cyber.

→ Renforcer la cyber-sécurité des réseaux et installations en amont et pendant les opérations sensibles.

→ Limiter en amont et pendant les opérations sensibles les nouveaux facteurs de risques (nouveau sous-traitant, nouveaux stagiaires, intégration d'un nouveau système d'information, etc.).

→ Procéder à une campagne de sensibilisation ciblée en amont de chaque opération sensible.

→ Mettre en place les dispositifs organisationnels et techniques qui permettront de détecter les attaques informatiques et d'y remédier (sondes de détections, contrats de prestations de réponse à incident, etc.).

→ Limiter les conséquences des actes malveillants : restriction des droits des utilisateurs des services dans le *cloud*, 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.