MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH DGSI #84

mai 2022

INGÉRENCE ÉCONOMIQUE

LA SÉCURITÉ INFORMATIQUE COMME IMPÉRATIF DE PROTECTION ÉCONOMIQUE

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

LA SÉCURITÉ INFORMATIQUE COMME IMPÉRATIF DE PROTECTION ÉCONOMIQUE

Les attaques informatiques ne cessent de se diversifier et s'adaptent rapidement aux évolutions des usages et des technologies. Qu'il s'agisse de piratages, de rançongiciels, d'actions d'ingénierie sociale ou encore de modification de sites Internet, ces actions malveillantes peuvent avoir d'importantes répercussions sur une société ou une institution et affecter à la fois son activité économique ou industrielle, son savoir-faire et sa réputation.

La prise en compte de ces risques par la mise en place de mesures préventives adaptées, l'identification et la correction des failles existantes et la diffusion d'une culture d'hygiène informatique au quotidien doivent désormais compter parmi les impératifs de protection économique des entreprises et des acteurs académiques.

PREMIER EXEMPLE

Vol de données d'une entreprise à la suite d'une imprudence d'un salarié. Un groupe français, sous-traitant pour plusieurs secteurs industriels, a été victime d'une attaque de type rançongiciel (ou *ransomware*). Ce type de logiciel malveillant chiffre les données d'un utilisateur puis impose à la victime le paiement d'une rançon en échange du déchiffrement de ses données.

L'intrusion du rançongiciel a été rendue possible par l'imprudence d'un salarié du groupe qui, après avoir ouvert un courrier électronique provenant d'une personne de confiance sur son ordinateur portable, a téléchargé la pièce jointe du courrier électronique puis a connecté son ordinateur au réseau de l'entreprise. L'identité de son interlocuteur avait été usurpée et l'absence de précaution particulière dans l'ouverture de la pièce jointe a conduit à la propagation du logiciel malveillant dans le système d'information de l'entreprise.

Grâce à cette intrusion, les cybercriminels ont pu chiffrer la quasi-totalité des serveurs du groupe, paralysant ainsi ses activités logistiques, de vente et d'achat pendant plusieurs jours. Un nombre important de données a été exfiltré des serveurs de l'entreprise, sans que la direction du groupe ne soit en mesure de déterminer leur nature et leur sensibilité. Le groupe a mis environ quatre mois à désinfecter l'ensemble de ses systèmes d'information et a pu restaurer la majorité de ses données grâce à des sauvegardes, sans payer la rançon demandée.

DEUXIÈME EXEMPLE

Atteinte à la réputation en raison d'une négligence en matière de sécurité informatique. Une société a été victime d'un rançongiciel provoquant une importante paralysie de ses activités et affectant notamment sa base de données, ses espaces de travail collaboratifs et son site Internet. L'attaque a été facilitée par l'existence de failles de sécurité dans les systèmes d'information de l'entreprise, qu'elle avait identifiées à l'occasion de précédentes tentatives d'intrusion, mais qu'elle n'avait pas corrigées.

Lors de la propagation du rançongiciel, les cybercriminels ont exploité ces failles pour infiltrer les réseaux de la société et ont notamment désactivé l'antivirus de l'exploitant et installé des programmes malveillants permettant d'extraire des données. Outre les dommages financiers, la société a été affectée par la diffusion des faits dans la presse et sur les réseaux sociaux, dénonçant son manque d'anticipation des risques informatiques.

TROISIÈME EXEMPLE

Faille de sécurité informatique causée par le comportement inapproprié d'un chercheur. Un chercheur d'un centre français de recherche a utilisé son ordinateur professionnel pour « miner » des crypto-monnaies (le minage consiste à effectuer un calcul informatique complexe qui permet de créer des actifs numériques).

Le centre de recherche, qui n'a pas détecté spontanément cette utilisation inappropriée d'un ordinateur professionnel, a mis plus d'un an pour constater une dégradation de la rapidité de son réseau, qui s'expliquait par la lourdeur des opérations de calcul nécessaires au minage de crypto-monnaies. Le centre de recherche n'est pas en mesure de déterminer dans quelle mesure son réseau a été endommagé durant cette période.

COMMENTAIRES

Si, dans la plupart des cas, l'origine des attaques informatiques est externe, les atteintes sont souvent facilitées par des imprudences internes.

Au-delà des attaques à but purement lucratif, les atteintes informatiques peuvent s'insérer dans une stratégie visant à affecter la compétitivité d'une entreprise, à capter ses données ou à la déstabiliser. Elles peuvent être commanditées par des États, notamment à des fins d'espionnage.

Les risques d'attaques informatiques sont souvent négligés par certains acteurs qui découvrent à l'issue d'un incident de sécurité qu'ils sont insuffisamment préparés aux conséquences de ces évènements. Ces risques peuvent pourtant être considérablement réduits par l'application de mesures de sécurité informatique adéquates et la prise en compte par tous les salariés d'un certain nombre de règles de bonne conduite informatique.

PRÉCONISATIONS DE LA DGSI

MESURES D'HYGIÈNE ET DE SÉCURITÉ INFORMATIQUE

- **Sensibiliser régulièrement l'ensemble des collaborateurs aux risques informatiques et à l'importance de la mise en œuvre de bonnes pratiques en matière de sécurité informatique**. La compromission d'un ou plusieurs systèmes d'information se produit souvent à la suite d'une négligence humaine (ouverture d'une pièce jointe frauduleuse, absence de sécurisation du mot de passe, etc.).
- **Renforcer la perception des risques informatiques auprès de ses collaborateurs,** par exemple en conduisant des campagnes de tests destinées à évaluer leurs réactions face à divers scénarios d'attaque informatique.
- **Faire preuve d'une vigilance constante dans la gestion des courriers électroniques.** Lorsqu'il s'agit d'un message dont l'expéditeur n'est pas connu, ne pas ouvrir le courriel en l'absence de vérification préalable, ne pas procéder au téléchargement des pièces jointes et ne pas activer les liens hypertextes. Dans le cadre d'échanges avec un interlocuteur connu et considéré comme de confiance, ne pas sous-estimer les risques d'usurpation d'identité et prêter une attention particulière à la pertinence du message, à la cohérence des propos, aux changements inhabituels dans le style d'écriture ou la police de caractères.
- **Réaliser une analyse de risques de son système d'information**. Il convient de prendre en compte les interconnexions informatiques avec ses prestataires : le risque d'attaque contre la chaîne logistique (*supply chain attack*) s'est accru depuis quelques années.
- **Effectuer un audit de sécurité informatique** en privilégiant un prestataire de service de confiance afin d'identifier et de corriger les vulnérabilités de son système d'information.
- **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.

PROTECTION DES DONNÉES SENSIBLES

- **Classer les données en fonction de leur niveau de sensibilité afin d'en assurer un meilleur suivi et une meilleure protection**. Il convient de différencier les données non sensibles, stockables sur Internet ou sur un service de *cloud*, des informations stratégiques et sensibles, à conserver dans des infrastructures protégées et internes à l'entreprise. Les données personnelles doivent faire l'objet du même traitement que les données sensibles.
- **Sauvegarder régulièrement ses données** afin de pouvoir restaurer les systèmes d'information en cas d'attaque informatique. Il est préférable de stocker ses données sur un support externe, non connecté au réseau local. En effet, les sauvegardes stockées en ligne peuvent également être ciblées par des attaques. Tester régulièrement les procédures de restauration des sauvegardes est également indispensable pour garantir une reprise d'activité rapide, en particulier dans un contexte de gestion de crise.

- **Activer la journalisation des évènements sur les équipements sensibles**, afin de pouvoir identifier et enquêter sur les dysfonctionnements ou les incidents de cybersécurité.

GESTION DES ATTAQUES

- **En cas d'attaque informatique**, débrancher la ou les machines compromises d'Internet et du réseau local afin de limiter la propagation de virus. Alerter immédiatement le service ou le prestataire informatique afin qu'il puisse intervenir le plus rapidement possible. **Tenir un registre des évènements et conserver les preuves relatives à l'attaque** : messages reçus, machines infectées, journaux de connexion, etc.
- **Informer le correspondant local de la DGSI pour bénéficier d'un accompagnement et d'une assistance administrative dans la gestion de la cyberattaque**.
- **Face à une attaque de type rançongiciel**, ne jamais payer la rançon imposée par les cybercriminels. Le paiement de la rançon ne garantit ni la récupération des données ni le déverrouillage des postes touchés et contribue à alimenter un écosystème cybercriminel. Par ailleurs, les données chiffrées ne doivent pas être supprimées : la clé de déchiffrement peut être obtenue ultérieurement et ainsi permettre la récupération des données.
- **Déposer plainte auprès des services de police ou de gendarmerie de proximité.**

Contacts :

- **L'Agence nationale de la sécurité des systèmes d'information (ANSSI)** publie régulièrement des recommandations qu'il convient de consulter et d'appliquer, disponibles sur le site Internet de l'agence : **www.ssi.gouv.fr**.
- **Le site www.cybermalveillance.gouv.fr** est un dispositif national dédié à la sensibilisation, la prévention et l'assistance aux victimes d'actes malveillants. Sur cette plateforme, des professionnels en cybersécurité sont notamment à disposition des particuliers, entreprises et collectivités territoriales pour les conseiller en matière de sécurité informatique.