MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH INGÉRENCE ÉCONOMIQUE DGSI #112

Avril 2025

LE FACTEUR HUMAIN, PRINCIPAL VECTEUR DE COMPROMISSION DES SYSTÈMES D'INFORMATION

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**

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

LE FACTEUR HUMAIN, PRINCIPAL VECTEUR DE COMPROMISSION DES SYSTÈMES D'INFORMATION

Les systèmes d'information occupent une place centrale dans le fonctionnement quotidien des structures privées et publiques, économiques comme académiques. Toutes ces données, parfois sensibles ou stratégiques, transitent par ces systèmes d'information accessibles à de nombreux salariés.

En dépit d'une protection assurée par l'adoption de solutions anti-virus ou de pare-feu par exemple, les failles d'origine humaine constituent un vecteur majeur de compromission. En effet, d'après le *World Economic Forum*, 95 % des violations de données ont pour origine une faille d'origine humaine.

Tout type de structure peut ainsi être visé par ce type d'attaque dès lors que les précautions nécessaires n'ont pas été prises pour les éviter.

1 LA MAUVAISE UTILISATION D'UNE MESSAGERIE PROFESSIONNELLE PERMET L'EXPLOITATION D'UNE FAILLE DE TYPE *ZERO-DAY*

Un salarié d'une société hébergeant des données sensibles a accédé à sa messagerie professionnelle à partir d'outils personnels, alors même que cette pratique était formellement interdite par la charte informatique de son employeur.

Cette utilisation de la messagerie professionnelle, hors du cadre protégé des outils informatiques professionnels, a permis à un groupe d'attaquants de pénétrer le système d'information de la société. Ce groupe a ensuite exploité une vulnérabilité du système d'exploitation de type *zero-day*, pour laquelle il n'existait pas à ce moment de mise à jour corrective. La réaction rapide des équipes de sécurité informatique a permis de limiter les conséquences de l'attaque.

Si la particularité de la faille *zero-day* implique que celle-ci n'aurait pu être anticipée, le respect de la charte informatique et l'utilisation de la messagerie professionnelle sur un outil approprié aurait permis d'éviter l'intrusion.

2 L'UTILISATION D'UNE CLÉ USB INFECTÉE PERMET LA CAPTATION DE DONNÉES PROFESSIONNELLES D'UNE SOCIÉTÉ

Un salarié d'un prestataire d'un grand groupe industriel a installé sur une clé USB personnelle un logiciel de type *keylogger* permettant d'enregistrer toutes les frappes effectuées sur le clavier de l'ordinateur. Il l'a ensuite mise à disposition de ses collègues qui ont utilisé cette clé USB comme un support de stockage professionnel, la connectant à leurs ordinateurs respectifs.

Peu après, le salarié a récupéré sa clé USB contenant l'ensemble des identifiants des personnes qui s'étaient connectées à leurs ordinateurs.

Le prestataire a rapidement détecté l'intrusion de la clé USB personnelle et identifié le salarié en cause, limitant les conséquences. Cet incident a été l'occasion de renforcer les règles de sécurité informatique et de rappeler à l'ensemble des salariés les bonnes pratiques.

3 L'OUVERTURE D'UNE PIÈCE-JOINTE PAR UN SALARIÉ SUR SON ORDINATEUR PROFESSIONNEL PERMET LE PIRATAGE DES SERVEURS DE SA SOCIÉTÉ

Un salarié d'une entreprise opérant dans un secteur sensible a été approché via un réseau social professionnel par un individu se présentant comme chargé de recrutement au sein d'un grand groupe étranger. Après quelques échanges, le prétendu recruteur a invité le salarié à ouvrir une pièce-jointe contenue dans l'un des courriels reçus.

Le salarié s'est exécuté et a ouvert la pièce-jointe sur son ordinateur professionnel. Contenant en réalité un virus, la pièce-jointe a infecté l'ordinateur du salarié, permettant l'extraction de plusieurs centaines de fichiers professionnels sensibles. Des fichiers appartenant à son ancien employeur, que le salarié avait indûment conservés sur son ordinateur professionnel, ont également été exfiltrés.

À la suite de l'incident, le salarié a fait l'objet d'un rappel à l'ordre formel.

Commentaires

Si certaines attaques informatiques se démarquent par leur complexité, les rendant difficiles à contrer, la faille humaine reste le principal vecteur de compromission des systèmes d'information. De nombreuses attaques informatiques pourraient être évitées si les consignes étaient appliquées et respectées.

Qu'elles résultent d'inattention, d'une méconnaissance des règles ou d'une volonté évidente de passer outre, les failles humaines doivent faire l'objet d'une attention accrue des équipes de sécurité informatique.

Il est ainsi essentiel que la politique de sécurité informatique d'une entité repose à la fois sur un pan technologique avec une architecture de protection robuste et sur un pan humain par la formation, la sensibilisation et la responsabilisation de tous les collaborateurs.

Renforcer la protection des systèmes d'information par l'adoption de solutions informatiques robustes

- **Effectuer un audit de sécurité informatique.**
  Réalisé auprès d'un prestataire spécialisé et de confiance, un audit permet la détection des vulnérabilités existantes et l'identification des risques qu'elles représentent, pour ensuite convenir de solutions adaptées à une meilleure protection.

- **Effectuer les mises à jour nécessaires des systèmes informatiques.**
  Il est essentiel de veiller à ce que les mises à jour soient faites de façon régulière, et dès leur publication, afin de corriger les failles susceptibles de favoriser les compromissions des systèmes informatiques.

- **Adopter des mesures de sécurité spécifiques pour les connexions aux ports informatiques.**
  Afin de limiter la propagation d'une attaque à la suite d'un branchement d'un support externe de type clé USB, il peut être utile d'établir des stations de décontamination afin d'analyser puis de nettoyer ces supports amovibles. Il est également possible de n'autoriser la reconnaissance que d'un nombre limité et encadré de supports amovibles.

- **Porter une attention particulière aux différents niveaux de sensibilité des données.**
  Pour limiter les exfiltrations de données en cas d'attaque, celles-ci peuvent être stockées sur des serveurs dédiés, non connectés au réseau local de travail, ou hébergées dans un *cloud* sécurisé de confiance. Il est également important de veiller à classer les données par niveau de sensibilité et d'accorder le plus haut niveau de protection aux données les plus importantes.

- **Se tenir informé auprès de sites Internet dédiés.**
  L'Agence nationale de la sécurité des systèmes d'information (Anssi) publie de façon régulière des recommandations sur son site (**www.ssi.gouv.fr**). Le site internet **www.cybermalveillance.gouv.fr** recense également de nombreux conseils et propose une assistance aux victimes d'actes malveillants.

Renforcer la protection des systèmes d'information par la diffusion d'une culture de sécurité informatique

- **Adopter une politique interne de sécurité informatique.**
  La politique interne de sécurité informatique doit dicter les bons usages à observer et peut être matérialisée par l'édiction d'une charte informatique signée par tous les collaborateurs de l'entité. Des sanctions peuvent également être prévues en cas de non-respect.

- **Former l'ensemble du personnel à l'hygiène numérique.**
  Il est conseillé d'instaurer une politique de formation, de sensibilisation et de responsabilisation à destination de l'ensemble des collaborateurs, indépendamment du service de rattachement et de la position hiérarchique.

- **Cloisonner les accès informatiques du personnel.**
  Donner seulement accès aux données nécessaires pour l'accomplissement des tâches confiées permet d'agir à titre préventif en limitant les risques de fuite de données intentionnelles, mais également en cas d'attaque en restreignant les parties exposées du système informatique.

- **Instaurer un COS (centre opérationnel de sécurité).**
  Composé d'experts en cybersécurité, le COS permet d'assurer une surveillance constante au sein des systèmes informatiques et donc de repérer une éventuelle activité anormale qui pourrait être synonyme d'une attaque.

- **Réévaluer ses liens avec des sous-traitants ou des prestataires.**
  Les sous-traitants ou les prestataires peuvent, volontairement ou non, être à l'origine d'une attaque informatique. Il peut être pertinent d'évaluer leur rôle précis et l'accès qu'ils peuvent avoir aux données de l'entité afin de limiter les conséquences d'une attaque par ce vecteur.

Réagir en cas d'incident informatique

- **Couper les accès de la personne suspectée d'être le point d'entrée de l'attaque.**
  La mesure permet d'isoler l'origine de l'incident le temps de sa résolution mais également de parer à une fuite de données plus importante si l'attaque est d'origine intentionnelle.
- **Déposer plainte auprès des services de police ou de gendarmerie compétents.**
  Il est également conseillé de conserver des preuves de l'attaque pour compléter le dépôt de plainte.
- **Prendre attache avec la Commission nationale de l'informatique et des libertés (Cnil).**
  L'incident doit être communiqué dans les 72 heures à la Cnil si l'attaque informatique a permis la consultation, la modification ou la destruction de données personnelles.
- **Contacter la DGSI afin de signaler tout incident.**
  La DGSI comprend un service proposant un accompagnement et une assistance administrative aux victimes d'incidents. Elle dispose d'une adresse électronique dédiée aux sujets de protection économique : securite-economique@interieur.gouv.fr.

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité