DECLARATION PREALABLE CSEC DES 10 ET 11 AVRIL 2024

UNE NOUVELLE FOIS, LE SYSTEME D'INFORMATION DE FRANCE TRAVAIL DEVOILE SES FAILLES ! LA DIRECTION DE LA DSI ET DONC LA DIRECTION GENERALE EN SONT RESPONSABLES

La CGT DSI avait demandé, par écrit en date du 14 mars, la tenue d'une réunion de CSE extraordinaire considérant la gravité de la situation concernant la fuite de données importante du SI de France Travail. Lors du CSE de la DSI du 4 avril, la direction a confirmé la fuite de données sans précédent dont a été victime notre système d'information. **Pour la CGT de la DSI, cette attaque résulte du choix assumé de la Direction de la DSI de ne pas mettre en place les préconisations sécuritaires nécessaires à l'ouverture de notre SI aux partenaires de France Travail.**

La CGT DSI avait pourtant alerté maintes fois sur des situations où la sécurité du SI n'était pas respectée ou insuffisante, car il s'agit bien d'une cyberattaque, et non d'une simple usurpation d'identité comme vous l'avez communiqué le 18 mars à l'ensemble des salariés de la DSI, et ce, afin de minimiser la responsabilité de la Direction de la DSI ou de la Direction Générale.

Une cyberattaque peut démarrer par un ciblage de salariés d'une entreprise, à travers des réseaux sociaux, qui constituent une source inimaginable et importante d'informations sur l'entreprise ou les données de ses salariés. Ensuite, le profilage permet d'identifier les failles (techniques ou autres) pour attaquer un système. **C'est ce qui s'est passé et nous avons bien subi une Cyberattaque.** Devant l'ampleur de la violation, la présidente de la CNIL a décidé de mener très rapidement des investigations afin de déterminer notamment si les mesures de sécurité mises en œuvre préalablement à l'incident et en réaction à celui-ci étaient appropriées au regard des obligations du Règlement Général sur la Protection des Données (RGPD).

Dans le cadre de nouveaux projets, la DSI réalise, avec des salariés professionnels internes reconnus sur le domaine de sécurité, un document "intégration de la sécurité dans les projets" (ISP) qui décline les analyses de risques et les préconisations. Lors du projet de connexion du partenaire Cap emploi en 2022, une analyse de risque a bien été réalisée en interne. Dans ce rapport il a été identifié, entre autres, le risque suivant : *« Un attaquant usurpe l'identité d'un agent Cap emploi et accède aux données du SI Pôle emploi via la machine virtuelle »* avec un indice d'alerte 4 (maximum). Le rapport préconisait de *« Renforcer l'authentification à la machine virtuelle avec un deuxième facteur d'authentification (2FA) »* conformément aux exigences de l'ANSSI, mais il n'a jamais été mis en place. **Pourquoi la Direction, suite aux préconisations, n'a pas validé et mis en place rapidement cette sécurité de base ? Il aura fallu une attaque d'ampleur jamais vue pour la mettre en place pour les salariés de Cap emploi en seulement 1 à 2 semaines !**

Le rapport alerte aussi sur le « principe du moindre privilège », qui est un concept de sécurité informatique consistant à octroyer aux utilisateurs des droits d'accès limités en fonction des tâches qu'ils doivent réaliser dans le cadre de leur travail. En vertu de ce principe, seuls les utilisateurs autorisés, dont l'identité a été vérifiée, disposent des autorisations nécessaires pour effectuer des tâches dans certains systèmes et applications ou pour accéder à certaines données ou ressources. Or les salariés de CAP emploi ont des autorisations d'accès non restreintes. Par ailleurs, ce principe n'est pas appliqué à l'ensemble de nos partenaires, entre autres les prestataires qui travaillent pour la DSI (ex-situ ou in-situ). Ceux-ci disposent des droits à l'identique des internes, que ce soit dans l'environnement de qualification ou de production du SI.

Cela fait la 4ème fois que notre SI est mis à mal au point de vue sécurité informatique :

- La 1ère fois, une société d'Intérim qui travaillait avec Pôle emploi s'est faite dérober des données et les malfaisants ont utilisé les données des DE pour appeler le support des demandeurs d'emploi de Pôle emploi le 3949 et demandaient de changer le RIB de leur banque et ainsi détourner les indemnités des DE. La somme s'élevait à plusieurs centaines de milliers d'Euros.

- ⇨ La 2ème concernait une extraction importante de données de DE faite par un salarié de Pôle emploi dans le cadre de son activité, données qui se sont retrouvées sur le Darknet : ce salarié a été licencié.
- ⇨ La 3ème en juillet 2023 concernait une cyberattaque au sein de la société de prestation MAJOREL de Pôle emploi. Les noms, prénoms, le statut actuel ou ancien de demandeurs d'emploi ainsi que leur numéro de Sécurité Sociale ont été divulgués.
- ⇨ La 4ème concerne la cyberattaque du mois de février 2024 impactant 43 millions d'inscrits potentiellement

Régulièrement, et plus précisément à chaque évènement d'attaque sécuritaire, notre syndicat CGT DSI a alerté sur les niveaux de sécurité insuffisants au sein de notre SI, mais la Direction minimise nos interventions et ne les prend pas en compte. La CGT réaffirme que la Direction est principalement responsable de cette situation, du fait de ne pas avoir mis en place toutes les préconisations concernant la sécurité (surtout la double authentification).

La CGT réitère ses demandes et fait les préconisations suivantes :

- ➢ **Mise en place de la méthode « multi facteur d'authentification »** pour tous les partenaires et salariés qui se connectent sur notre SI (salariés internes et externes, les missions locales, les conseils départementaux, les métropoles, les mairies, par exemple)
- ➢ **Révision de la politique d'attribution des activités de sécurité à la prestation de service**.
- ➢ **Application stricte du « principe de moindre privilège »** (la gestion des habilitations), et particulièrement pour les salariés externes, partenaires ou prestataires de service qui disposent des mêmes droits que les internes.
- ➢ **Révision de la politique d'ouverture des accès pour les salariés externes** qui peuvent se connecter 24h/24, 7j/7 et 365j /365 sur le SI.
- ➢ **Présentation au CSE de la DSI et au CSEC des mesures de sécurité qui seront mise en place pour tout nouveau projet** qui nécessiterait une connexion sur notre SI.

En accord avec la CGT DSI, les élus et RS CGT du CSEC préconisent d'identifier et de sanctuariser les domaines qui doivent être réalisés uniquement par des internes et non par de la prestation de services, et ce afin de limiter le risque de fuite de données et de simplifier la traçabilité.

Par ailleurs, pour la CGT, **les missions qui relèvent du SI devraient être réinternalisées à France travail.**

Enfin, pour éviter toutes nouvelles Cyberattaques, sur proposition de la CGT DSI, **les éluEs de la DSI ont voté à l'unanimité, au CSE Extraordinaire du 4 avril, la capacité d'ester en justice sur la fuite de données et de sécurité du SI.**