Déclaration CGT - CSEC 06 et 07.11.2025

Déclaration sur la Cyberattaque

Une fois de plus, la CGT France Travail alerte le CSE central sur la gravité de la situation en matière de sécurité informatique au sein de notre établissement publique administratif. La récente cyberattaque qui a touché France Travail a pris sa source sur plusieurs postes de demandeurs d'emploi. Un logiciel malveillant diffusé par le groupe de hackers STORMOUS y a été déposé pour voler des données personnelles.
La récupération des identités complètes, des coordonnées, des historiques professionnels, des RIB, des CNI, des contrats et des bulletins de salaire permet aux hackers de disposer d'un kit d'usurpation de haut vol ! Les pirates ont exploité un compte France Travail dont les identifiants, enregistrés localement, ont été récupérés.

Cette **6ème Cyber attaque**, en 2 ans était évitable : si les mesures de sécurité dont l'authentification multifactorielle (MFA) avait été généralisée à toutes connexions sur notre SI (partenaires, prestataires et usagers), l'attaque n'aurait pas pu se produire.
Cette mesure, déjà effective dans beaucoup d'organismes privés et publics tels que les banques, les assurances, le Trésor Public, la CAF ou l'URSAF, la CGT l'avait déjà exigé dès 2023. Nous avons réitéré encore en 2024. A l'époque, la Direction et le RSSI affirmaient devant les élus CSE DSI que, suite à la cyber attaque via Kairos en juillet 2025, l'ensemble des partenaires avait la double authentification. Mais en affirmant cela, ils occultaient la population des usagers demandeurs d'emploi.

Et pourtant à ce jour, en plus des millions de DE, plus de 50 000 comptes partenaires (collectivités locales, organismes de formation, structures associées…) ne disposent toujours pas du MFA alors qu'ils possèdent des accès avec des privilèges importants (via des API, entres autres).
La direction, tout en ayant connaissance du risque, s'est abstenue d'agir, préférant minimiser l'ampleur du problème et désinformer les représentants du personnel.

Cette légèreté est inadmissible et irrespectueuse envers le personnel et ses représentants.

Le nouveau responsable de la DGA Tech s'est dit choqué par la situation alors que France Travail sort déjà d'une cyberattaque majeure ayant compromis 43 millions de données personnelles. À la suite de ce vol de données en mars 2024, un audit de la CNIL est en cours. Il pourrait déboucher sur une sanction sans précédent pour un Service Public avec plusieurs millions d'euros d'amende imputable à France Travail.

La CGT France Travail constate :

- ✓ L'absence persistante d'un déploiement complet du MFA pour toutes les connexions sur notre SI y compris les partenaires extérieurs,
- ✓ Des audits de sécurité insuffisants et non conformes aux standards recommandés,
- ✓ Le non-respect des préconisations de la CNIL et des obligations issues des directives européens NIS2.0 concernant, notamment, les mesures contre la cybersécurité en Europe
- ✓ Des accès excessivement ouverts pour les 2 300 prestataires de la DSI et les prestataires régionaux, bénéficiant souvent des mêmes droits que les personnels internes,
- ✓ Des failles majeures liées à l'usage croissant des IA et des interfaces API, dont la sécurité est très en deçà des exigences actuelles (pas de limite de volumétrie de données transférée, de limite de débit ou de CAPTCHA par exemple)

Pendant ce temps, les agents de la DSI, et les agents dans nos agences, pourtant mobilisés et compétents, subissent les conséquences de ces manquements : ils sont injustement tenus pour responsables alors que les causes résident dans des choix de direction.

La CGT France Travail rappelle que la directive Européenne NIS 2.0 prévoit des **sanctions pénales,** en plus des sanctions financières, pour les manquements graves, notamment pour les dirigeants d'entités concernées. La France n'ayant pas encore voté la transposition de la directive dans le droit français, les décideurs qui ont abouti à cette situation s'en sortent bien. Mais la donne pourrait changer car la transposition est en cours d'examen à l'Assemblée nationale, avec une adoption définitive attendue d'ici le début d'année 2026.

CGT France travail - 38 rue des frères Flavien - 75020 Paris
syndicat.cgt@francetravail.fr

La mauvaise Loi Plein emploi, France Travail impose à France Travail de mettre en œuvre et de maintenir des outils numériques à disposition pour le réseau national pour l'emploi. Cette mission implique une exigence absolue de fiabilité, de confidentialité et de sécurité des systèmes informatiques. Les alertes relatives à la cybersécurité sont donc non seulement légitimes mais essentielles à la continuité et à la crédibilité de cette mission.

La CGT France Travail renouvelle donc ses demandes :

- La fermeture immédiate des accès à notre SI pour tous les partenaires qui ne disposent pas de MFA (2FA),
- La réalisation immédiate d'un audit de sécurité indépendant, présenté au CSE DSI, au CSEC puis aux salariés,
- La généralisation obligatoire du MFA à l'ensemble des connexions sur notre SI (partenaires et des salariés en prestations de service d'ici la fin de l'année avant leur ré internalisation),
- La transparence complète sur les accès prestataires et les mesures correctives engagées,
- La mise en place du principe de moindre privilège (dans la gestion des habilitations) appliquée de manière stricte, particulièrement pour les salariés externes, partenaires ou prestataires de service qui ne doivent pas disposer des mêmes droits que les internes (accès 24h/24, 7j/7 et 365j /365 sur le SI)
- La revue par la Direction de sa politique d'attribution des activités de sécurité confiées à la prestation de service, ce domaine doit impérativement être maitrisé par des agents de France Travail,
- La présentation par la Direction au CSE DSI des mesures de sécurité qui seront mise en place pour tout nouveau projet qui nécessiterait une connexion sur notre SI.
- La suspension du déploiement des outils liés à l'IA.

La CGT France Travail ne cessera pas d'alerter tant que la protection des données des usagers et des salariés ne sera pas garantie. Nos administratrices au Conseil d'administration (CA) et nos représentants au Comité National pour l'Emploi (CNE) ont été alertés une nouvelle fois, comme pour les autres cyber-attaques.

La cybersécurité ne peut pas continuer à être négligée et sacrifiée sur l'autel de l'économie et de l'opacité. Plutôt que de prioriser la réorganisation de la DSI DGA TECH et le redéploiement des fonctions support vers le réseau, la Direction Générale devrait répondre à ses obligations légales en matière de sécurité informatique. En complément, il est désormais plus qu'indispensable, aux vues des risques exponentiels autour des IA, qu'une négociation sur un accord les encadrant à France Travail s'ouvre au plus vite dans notre établissement.