CR de la visioconférence "cyberattaque visant l'Education nationale ", mardi 25 août 2026 à 14h

La FNEC FP-FO a participé à la visioconférence du 25/08 convoquée en urgence par le cabinet du ministre, concernant le vol de données informatiques à l'Education nationale.

En introduction, le ministère s'est voulu rassurant sur un retour à la normale dans toutes les académies, à deux exceptions près, les académies de Nantes et de Toulouse, où le ministère prévoit un retour à la normale « sous quinzaine ». Il conclut par : *« aucun agent ne doit s'inquiéter pour le versement des paies. Le nécessaire est fait et il ne devrait pas y avoir de rupture ».*

Pour le ministère, à l'heure actuelle, il n'y aurait pas eu de vol de données mais seulement des intrusions. Les investigations sont en cours, tout comme les enquêtes judiciaires. Une plainte a été déposée et un signalement effectué auprès de la CNIL.

Un RETEX est prévu le 11 septembre avec le cabinet du ministre et la DNE. Dès le 28/08, une nouvelle visioconférence est programmée pour faire un nouveau point avec le ministre, très attentif à la situation.

Des OS font part de leurs craintes concernant le vol des données ainsi que de la difficulté de mise en œuvre de certains applicatifs.

La FNEC-FP-FO a dénoncé le fait que le ministère n'accorde que deux minutes d'intervention aux syndicats pour se débarrasser d'un problème aussi grave. Puis elle a pointé l'absence d'information publique, précise et détaillée : s'il n'y avait pas de risque concernant le versement des payes ou le vol de données, le ministère aurait communiqué, or ce n'est pas le cas et les remontées de nos syndicats sont très préoccupantes, notamment concernant les affectations de rentrée (remplaçants, contractuels, stagiaires…), le versement des payes, les renouvellements de contrats. Quelle est l'ampleur de la fuite des données ? Qui est concerné ? Quelles sont les données compromises ? Le ministère a-t-il lui-même pris la mesure des risques encourus par ses agents, par les élèves ?

FO a pointé l'inacceptable faiblesse structurelle de l'informatique, en lien avec les choix budgétaires du gouvernement et insisté sur la situation des personnels devant se débrouiller seuls et sans moyens…

Elle a demandé une information individuelle systématique de tous les agents, une protection spécifique des personnels, des garanties pour les étudiants et stagiaires en formation, pour les contractuels, l'absence de toute sanction contre les agents, ainsi que des moyens humains et budgétaires pour les établissements et les services, sans reporter cette charge sur les personnels — notamment les personnels de direction — ni passer par la publication d'un nouveau

vadémécum ou de nouvelles fiches. Les personnels administratifs ne doivent pas faire d'heures supplémentaires pour rattraper le retard !

Enfin, nous avons vu la communication du recteur de Nantes. Nous tenons à dire que nous ne sommes pas les cogestionnaires de l'inaction gouvernementale ! C'est à l'employeur de prendre ses responsabilités ainsi que toutes les mesures pour que le service public fonctionne, pour que ses personnels soient effectivement protégés, et rémunérés ! Nous n'acceptons pas ce fonctionnement de l'Ecole en mode dégradé.

Face à ces différentes remarques, les représentants du ministère rappellent que la situation est circonscrite malgré certaines difficultés (sans donner davantage de précisions). Une mission d'inspection sera diligentée pour rendre des conclusions au sujet d'une réorganisation et d'une communication. L'une des premières mesures sera la mise en œuvre de la double authentification.

Lors de la réunion de rentrée des recteurs, ces derniers ont reçu des éléments de langage pour communiquer sur le problème des intrusions informatiques.

Cette visioconférence donne l'impression d'une opération de communication organisée en catastrophe, à une semaine de la rentrée. Son contenu n'a répondu ni aux interrogations ni aux demandes. Le ministère apparaît comme dépassé par la gravité des événements, dans l'incapacité d'informer, et surtout de protéger ses agents.