



S'ENGAGER POUR CHACUN
AGIR POUR TOUS

Picardie Éducation

Compte-rendu du groupe Blanchet du vendredi 24 octobre

Point de situation par M. Le Recteur concernant la cyberattaque. Cette dernière n'est pas un fait isolé mais l'une des soixante attaques massives revendiquées par le groupe Qilin.

Il semble que seuls 16 établissements aient été touchés avec exfiltration de leurs données. Ces établissements sont tous dans l'académie de Lille, aucun dans l'académie d'Amiens.

L'attaque est limitée au parc informatique du Conseil Régional, les applications métier (Pronote, ENT, Opale...) restent accessibles par Internet.

Point d'étape sur les étapes en cours, première semaine des vacances :

- Action conjointe de la Région et de la DRASI : sécurisation du parc administratif (5000 machines) mais aucune récupération des données perdues. Pour l'instant aucune connexion au réseau.
- Les PC infectés sont limités en nombre mais quasiment tous les serveurs, administratifs et pédagogiques, sont impactés (3 serveurs sur 4)
- Tout le système de sauvegarde est atteint, voire détruit (à priori même tout ce qui était dans le Drive Hdf)
- L'annuaire académique sera consolidé ce vendredi

NB : pour les établissements utilisant GFC, pour ceux qui ont effectué des sauvegardes pas de difficulté, pour les autres les données sont perdues. Dans ce cas les établissements ont déjà été contactés par la DRASI pour une installation en réseau local.

Des clefs OTP sont disponibles pour les personnels administratifs, il ne faut pas hésiter à en demander, elles ne sont plus limitées à trois par établissement.

Deuxième semaine des vacances :

- Finalisation du plan de continuité pédagogique par les IA-IPR ce vendredi et diffusion en début de semaine prochaine
- Interventions sur le parc pédagogique (environ 100 000 machines) à distance. Des interventions possibles en présentiel dans certains établissements.
- Priorisation des établissements ayant des BTS (inscriptions aux examens)
- Déploiement d'imprimantes pour les postes « admin »
- Réinitialisation des identifiants et des mots de passe à faire pour tous les comptes utilisateurs, y compris pour tous les élèves.
- Installation d'outils pour sécuriser l'accès aux réseaux des lycées

NB : il n'y aura pas de retour à la normale le 3 novembre. Les environnements académiques auront été nettoyés, tous les logiciels obsolètes ou hors licence Hdf auront été effacés. Un logiciel de « nettoyage » sera installé, il sera interdit de le désactiver pour remettre des logiciels « maison ».

Il est important de penser à quitter sa session et d'éteindre les ordinateurs en fin de journée pour éviter la diffusion des virus. Il a été constaté 300 ordinateurs connectés non éteints pendant cette première semaine de vacances.

Il a été rappelé de ne pas connecter d'ordinateur personnel aux photocopieurs et vidéoprojecteurs. Mettre à jour son anti-virus pour le cas où une clé USB aurait été utilisée entre les ordinateurs réseau et un ordinateur personnel (a priori pas de contamination mais principe de précaution).

Pour la CFDT Picardie Éducation,

Sandrine Lemoine-Roussel

Laurent Martinel