Cyberattaque contre des établissements scolaires

SGEC/2024/395
25/03/2024

DESTINATAIRES : Directeurs diocésains,
Organisations professionnelles de chefs d'établissements.

POUR INFORMATION : Commission Permanente

Mesdames, Messieurs,
Chers amis,

Vous avez pu le lire dans la presse en fin de semaine dernière, de très nombreux établissements scolaires, publics et privés, ont fait l'objet d'une cyberattaque par laquelle ont été, notamment, diffusés des messages, photos et vidéos à caractère terroriste.

Aplim, éditeur de la solution EcoleDirecte, et Charlemagne nous ont alertés sur les tentatives de piratage au sein de leur ENT (Environnement Numérique de travail).

Pour être très précis, il ne s'agit pas d'une attaque de la plateforme informatique elle-même mais d'un usage inapproprié de certains comptes élèves, à leur insu. Ce type d'attaque est appelée fishing ou usurpation d'identité.

Il circule sur le « Dark Web » un nombre considérable d'identifiants et de mots de passe volés à travers de faux sites internet, lors d'oubli de mise à jour d'antivirus, de téléchargements, d'applications extensives…. Ces identifiants sont utilisés par des hackers qui ont ensuite toute la liberté de diffuser des messages dans les établissements en se faisant passer pour un élève, voir un enseignant.

Lors de ce type d'attaque, les équipements de sécurité empêchent l'accès aux bases de données. Aucune donnée n'a donc été impactée ou fuit à l'occasion de ces attaques.

Secrétariat Général de l'Enseignement Catholique – Pôle ressources
277 rue Saint-Jacques – 75240 Paris cedex 05 – ✆ 01 53 73 73 84 – @ y-diraison@enseignement-catholique.fr

Fort heureusement, depuis de nombreux mois la société Aplim investit considérablement dans de nouvelles technologies ce qui a permis d'éviter 98% des tentatives de ces derniers jours.

Les dispositifs de sécurité en vigueur ont permis de bloquer les tentatives d'intrusion dans 48 établissements catholiques. A notre connaissance, un seul de nos établissements a été victime de l'attaque de la semaine dernière.

Aplim travaille en étroite collaboration avec la Direction de la police judiciaire, sous-direction de lutte contre la cybercriminalité, de Nanterre qui regroupe l'ensemble des cyberattaques.

Cette attaque est l'occasion de rappeler quelques consignes de bases aux utilisateurs d'ENT :

- Changer régulièrement son mot de passe ;
- Créer un mot de passe fort (au moins 10 caractères majuscule, minuscule chiffre, signe) et ne le communiquer à personne ;
- Ne pas stocker son identifiant dans le navigateur ou dans un fichier stocké dans l'ordinateur ;
- Ne pas laisser son ordinateur ou smartphone sans surveillance, notamment dans les transports ;
- Ne pas laisser sa session ou son navigateur ouverts ;
- Etre discret lors de la saisie de son mot de passe en public ;
- Ne pas utiliser des sites ou applications non officielles ;
- Equiper son ordinateur d'un antivirus avec mise à jour automatique.

Vous souhaitant bonne réception de ces informations, je vous assure de mes sentiments dévoués.

Yann DIRAISON
Adjoint au Secrétaire Général de l'Enseignement Catholique