DOCUMENT DE COMMUNICATION EXTERNE D'UNE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL AUX PERSONNES CONCERNÉES

NOTIFICATION DE VIOLATION DE DONNÉES

La présente concerne une situation préoccupante relative à vos données à caractère personnel. Conscients de la valeur que vous attachez à votre vie privée, nous accordons une attention toute particulière à la protection de vos données personnelles.

1. Que s'est-il passé ?

Le 09/01/2024, notre Service Informatique a détecté que l'un de nos serveurs locaux, utilisé dans le cadre de certaines activités pédagogiques, a été victime d'une cyber-attaque. Au cours de l'investigation, les informaticiens ont identifié le programme concerné : *Moodle*. Ce programme utilise un compte local différent des comptes *School Management System* (SMS) et *Office365* (O365) dans la mesure où le programme est stocké sur un serveur local de l'Ecole. Bien qu'actif, le processus automatique du programme, « Inactive user cleanup », n'a pas fonctionné. Par conséquent, des données vous concernant étaient toujours enregistrées.

2. Quelles informations ont été impliquées ?

Des informations vous concernant ont été exfiltrées.

Les informations concernées comprenaient :

- Adresse email fournie par l'école ;
- Nom ;
- Prénom ;
- Cycle et niveau (pour les élèves uniquement) ;
- Username.

3. Conséquences probables de la violation de données à caractère personnel

À la suite de cet évènement indésirable, nous supposons qu'une ou plusieurs des éventualités suivantes peuvent se produire :

- Vos adresses électroniques peuvent faire l'objet de tentatives de mailing et ou fishing/phishing. Dans la mesure où vous ne faites plus partie de notre établissement, le risque est faible, voire nul. Néanmoins, si cela se produit, pour vous protéger, des préconisations vous sont détaillées au point 5 page 3 sur 3 ;

- Les données pourraient être supprimées du serveur. Ce qui n'aura aucun impact.

4. Que faisons-nous ?

Dès la détection de l'incident, nous avons rapidement pris des mesures pour déterminer la nature et la portée de cet évènement indésirable. Nous collaborons également avec la Commission Nationale pour la Protection des Données (CNPD), le Computer Incident Response Center Luxembourg (CIRCL) et la Police.

Mise en place de mesures destinées à protéger notre communauté :

- Arrêt du serveur impacté dès le 09/01/2024 ;
- Identification et correction de la vulnérabilité du programme attaqué ;
- Suppression de vos données.

5. Que devez-vous faire ?

Compte tenu des circonstances et des efforts déployés par l'École Européenne pour atténuer la situation, nous pensons que :

☐ Il n'est pas nécessaire que vous entrepreniez des actions supplémentaires ;

☒ Il est nécessaire que vous entrepreniez les actions suivantes :

- Si vous détectez un email suspect, le supprimer de votre messagerie sans même l'ouvrir ;
- Si vous réceptionnez un email dont vous ne pouvez définir s'il est suspect ou non, celui-ci doit être envoyé à votre Service informatique afin que ce dernier procède à un contrôle et vous informe des suites à donner.

6. Pour plus d'informations

Pour plus d'informations, veuillez contacter notre Délégué à la Protection des Données (DPO) : LUX-DPO-CORRESPONDENT@eursc.eu

Bien à vous,