Politique sur le traitement des vulnérabilités

Chez ÉtudeSecours, la sécurité de notre plateforme est une priorité absolue. Cette politique vise à établir les étapes suivies pour traiter les vulnérabilités de façon structurée afin de garantir la confidentialité, l'intégrité et la disponibilité de nos systèmes.

L'équipe de développeurs est responsable de la surveillance continue des vulnérabilités de la plateforme, de leur classification et de la mise en place du plan d'action.

L'équipe pédagogique et à l'organisation scolaire doit signaler toute vulnérabilité potentielle dès sa découverte et collaborer étroitement avec l'équipe de développeurs pour faciliter la résolution.

Chez ÉtudeSecours, nous avons établi les étapes suivantes pour structurer le travail lorsqu'une vulnérabilité est identifiée :

1- Identification : L'équipe de développeurs utilise des outils automatisés et des analyses manuelles pour identifier les vulnérabilités potentielles. Les situations anormales soulevées par l'équipe pédagogique et à l'organisation scolaire sont aussi présentées au chargé de projets technologiques afin de les consigner dans notre système de distribution de tickets.

2- Évaluation et priorisation : Les vulnérabilités sont classées en fonction de leur gravité, de l'impact potentiel sur la sécurité, sur les activités de l'entreprise et l'expérience de l'utilisateur. Les vulnérabilités critiques sont traitées en priorité.

3- Plan d'action : Un plan détaillé de traitement des vulnérabilités est élaboré pour chaque vulnérabilité critique. Ce plan inclut des délais clairs, des responsabilités définies et des mesures de suivi.

4- Communication : Les personnes concernées sont tenues informées de la vulnérabilité et des mesures de remédiation en cours. Une communication transparente est maintenue tout au long du processus.

5- Mise en œuvre des correctifs : Les correctifs sont développés, testés et déployés dès que possible. L'équipe de développeurs est responsable de la mise en œuvre des correctifs.

6- Vérification : Les correctifs sont évalués pour s'assurer qu'ils ont été appliqués correctement et qu'ils ont résolu la vulnérabilité. Des tests supplémentaires peuvent être effectués pour garantir l'efficacité des correctifs.

7- Documentation : Toutes les étapes, y compris les détails de la vulnérabilité, les actions prises et les résultats, sont consignées de manière détaillée (log).

Cette politique sera régulièrement révisée pour s'assurer de son efficacité. Des audits réguliers de sécurité sont aussi effectués pour identifier de nouvelles vulnérabilités et évaluer l'efficacité des mesures de remédiation mises en place.

Madame Marie-Claude Harnois, directrice générale, est responsable de la mise en œuvre de la Politique sur le traitement des vulnérabilités. Pour toutes questions, il est possible de lui écrire à l'adresse suivante : cybersecurité@etudesecours.com.