# Sécurité des données : l'éditeur de logiciel Aplim s'engage sur la protection de vos systèmes d'information

**Dans un monde géopolitique complexe où la sécurité des données est devenue la priorité pour les utilisateurs et les éditeurs de logiciels, Aplim se distingue par son engagement envers la protection des SI[1]. Conscient de l'importance que cela revêt pour les écoles, Reynald Marien, directeur général d'Aplim partage les stratégies mises en œuvre et des recommandations[2].**

Pour l'ensemble de ses progiciels Charlemagne et EcoleDirecte, Aplim développe une politique stricte de sécurité des données comprenant un ensemble de protocoles basés conjointement sur de nombreux investissements technologiques et humains.

**Une approche prédictive**

Nous réalisons régulièrement via des audits, une évaluation des risques permettant d'identifier éventuellement des actifs critiques et des menaces potentielles nous aidant ainsi à concentrer nos efforts sur des vulnérabilités prédictives.

**Sécurité par conception**

Dans la conception de nos logiciels, nous intégrons des processus de sécurité dès le début, cela signifie que nous appliquons des principes de conception sécurisée et que nous effectuons des revues de codes régulières.

**Formation et sensibilisation**

Des tests de résilience, de pénétration, de phishing sont autant d'armes que nous déployons afin d'accompagner en permanence nos équipes et rester sans cesse sensibilisés face aux diverses menaces. De plus, nous collaborons avec des cabinets experts pour être informé des meilleures pratiques en matière de sécurité et mettons un plan de formation annuel à destination de notre ingénierie de développement et de nos administrateurs systèmes afin de maintenir les niveaux d'exigence nécessaires dans ce domaine.

**Cryptage des données.** Dans la suite de nos logiciels, nous appliquons des techniques de cryptages des données, autant sur des datas stockées que des datas en transit sur le réseau.

**Intégration de l'Intelligence Artificielle.** Nous déployons aujourd'hui une IA spécifique sur la détection de menaces.

**Évaluation des performances.** Comme toute entreprise, la société est dotée de tableaux de bord permettant de collecter des indicateurs de performance clés (KPI) pour évaluer les mesures mises en place (nombres d'incidents, temps de réactivité, etc.)

**Plan de Reprise d'activité.** Dans son mode Cloud ou son mode SaaS, Aplim a conçu un plan de reprise d'activité c'est-à-dire un ensemble de procédures (techniques, et organisationnelles) qui permettent à l'entreprise de prévoir par anticipation les mécanismes de reconstruction des serveurs en cas de sinistres critiques (cyberattaques, incendie, etc.). Le PRA permet ainsi de relancer des serveurs en leur affectant des données répliquées afin de redémarrer les applications dans un temps imparti.

**Feedback, Information et Amélioration continue.** Nous encourageons les retours d'information de la part des utilisateurs sur

> *Nous collaborons avec des cabinets experts pour être informé des meilleures pratiques en matière de sécurité et mettons un plan de formation annuel à destination de notre ingénierie de développement.*

[1] *Systèmes d'information*

[2] *Pour des raisons confidentielles et de sûreté, vous comprendrez aisément que cet article restera sur une approche macroscopique et généraliste du sujet.*

les aspects de sécurité et communiquons régulièrement avec eux afin de sans cesse améliorer la bonne posture en cas de doute ou de menace. D'ailleurs à ce niveau, nous constatons un grand nombre de comportements malveillants dus à une baisse de vigilance des utilisateurs (divulgation de son identifiant et mot de passe via de faux sites internet...). Exemple, les cas d'usurpation d'identité pour accéder à son compte EcoleDirecte est le plus fréquemment rencontré. Il faut être extrêmement attentif car le seul et unique but du hacker sera de diffuser des messages inappropriés à l'ensemble de la communauté éducative en se faisant passer pour un élève ou un professeur, et parfois avec de graves conséquences.

**Labellisation, Conformité et Réglementation**

Aplim a fait un choix stratégique de production de son activité basée en France (développement des logiciels, services d'assistance, de formation et d'hébergement de ses produits) qui lui confère les labels "Origine France garantie" et "Service France garantie". D'autre part, la société répond à toutes les exigences législatives en vigueur en matière de sécurité et notamment la réglementation RGPD.

**Recommandations aux établissements**

Sur ce sujet, nous ne pouvons que conseiller les Ogec et les chefs d'établissement à mener également des mesures simples et efficaces de premier ordre pour protéger leurs systèmes d'information et leurs utilisateurs.

- Mettre à jour régulièrement les systèmes d'exploitation, se munir de firewall de dernière génération : les vulnérabilités non corrigées sont des cibles faciles pour les attaquants.

> *Nous ne pouvons que conseiller les Ogec et les chefs d'établissement à mener des mesures simples et efficaces de premier ordre pour se protéger.*

- Si l'établissement possède ses propres serveurs, il faut envisager un audit régulier de son infrastructure et des process de sauvegarde à froid, soit déconnectée de tout réseau.
- Le déploiement de PRA est également indispensable. Les menaces étant de plus en grandes et les technologies très évolutives, le risque de cyberattaque est démultiplié.
- S'orienter vers des choix d'infogérance ***(Charlemagne sur site)*** ou l'externalisation en mode Cloud si l'établissement n'a pas d'expertise interne dans la gestion des données.
- Réaliser des tests de pénétration et de phishing.
- Sensibiliser toute la communauté éducative aux signes d'activités suspectes, à la gestion de données, par le biais de formation ou de conférences spécialisées.

Nous sommes déterminés à fournir aux établissements des solutions informatiques fiables, via une approche holistique de la sécurité des données : de la conception des applications en passant par les bonnes pratiques d'usage jusqu'à l'hébergement des données.

### La sensibilisation, la formation sont des piliers complémentaires à l'expertise d'Aplim[1]

Il faut inculquer à toutes nos parties prenantes une véritable "Culture de la sécurité". C'est un élément crucial dans le paysage technologique contemporain. À une époque où les menaces numériques évoluent constamment et deviennent de plus en plus sophistiquées, l'importance d'une conscience et la mise en place de procédures spécifiques ne doivent pas être sous-estimées. Cette culture ne se limite pas aux seuls spécialistes que nous sommes, mais s'étend à tous les utilisateurs des systèmes informatiques.

*[1]Il est aussi important de reconnaître que tout cela reste un processus évolutif. La culture de la sécurité informatique doit s'adapter continuellement aux nouvelles menaces émergentes et cela nécessite un engagement constant de la part de tous les acteurs pour créer un environnement sûr et résilient.*