INSTITUT LIMAYRAC

Synthèse veille technologique

(Référentiel B1)

1. Présentation des thèmes de veille

Dans le cadre du référentiel B1, la compétence "Organiser son développement professionnel" impose la mise en œuvre d'une veille technologique rigoureuse. L'informatique étant un secteur en constante mutation, j'ai choisi de structurer ma veille autour du thème de la cybersécurité.

J’ai choisi ce thème car la cybersécurité représente aujourd'hui un enjeu vital pour toute infrastructure. Le domaine “cyber” englobe en effet la protection globale de l'espace numérique : sécurisation des réseaux, des appareils, des données, mais aussi prévention face aux erreurs humaines. Dans ce contexte, suivre l'évolution constante des nouvelles menaces et des méthodes de défense est indispensable pour garantir la confidentialité et l'intégrité des systèmes informatiques. Il est donc crucial de maintenir une veille rigoureuse sur les différents types d'attaques afin d'adopter une posture proactive et de prévenir toute compromission.

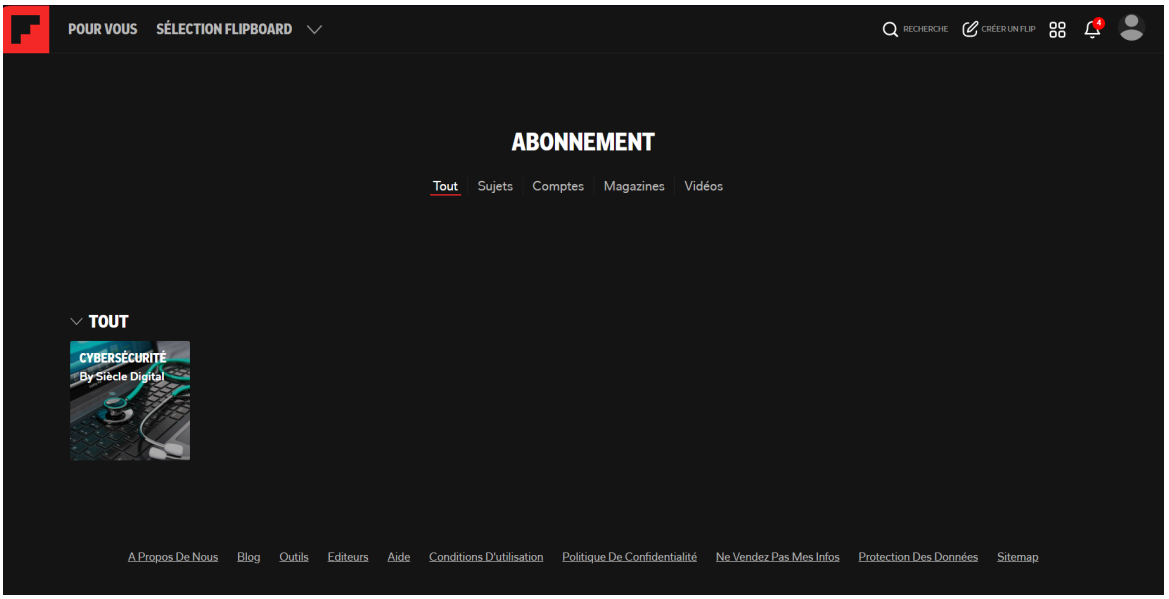
2. La Stratégie de Collecte

FlipBoard : FLIPBOARD

Flipboard est un outil indispensable pour ceux qui veulent rendre leur veille informationnelle plus visuelle et élégante. Conçu comme un magazine numérique personnalisé, il rassemble des contenus provenant de nos sources préférées, de réseaux sociaux et de sujets choisis pour les présenter sous forme de pages à consulter.

Pour ma veille technologique, je me suis abonné à un magazine Cybersécurité en lien avec ma formation.

Je consulte également des articles intéressants sur les recommandations, mais le plus souvent je reste sur les magazines auxquels je suis abonné



3. Exploitation et Traitement des données

Exploitation :

Dans le cadre de cette synthèse de veille technologique, mon choix s'est porté sur une sélection d'articles de référence, afin de mettre en lumière les principaux enjeux actuels.

Traitement des articles :

Les articles que je choisis de retenir pour cette synthèse sont répertoriés dans le répertoire personnalisé que j'ai mis en place.

Il est crucial pour moi de vérifier les sources pour savoir si l'article est fiable ou non, afin d'éviter de lire des 'fake news', ce qui est courant.

4. Synthèse

Article : Un risque d'explosion des arnaques à la livraison : Relais Colis confirme avoir été victime d'une cyberattaque massive.

Source : Cnews
Date de l'alerte : 16 janvier 2026 (toujours d'actualité)
Lien : Cnews

Le 16 janvier 2026, l'entreprise de livraison Relais Colis a officiellement confirmé avoir été victime d'une fuite de données d'envergure. Bien que la compromission provienne initialement d'un prestataire tiers, les conséquences touchent directement les clients finaux. Les pirates auraient mis en vente ou diffusé une base de données contenant jusqu'à 10 millions de lignes d'informations sur des forums spécialisés dans le piratage.

Recommandation :

- Ignorer les liens : Ne pas cliquer sur aucun lien reçu par SMS ou e-mail réclamant des frais de livraison même s'il mentionne votre nom.

- Vérifier à la source : Suivre le colis en vous rendant directement sur l'application ou le site web officiel du commerçant ou du transporteur.

- Protéger ses données bancaires : Ne jamais donner votre numéro de carte bleue à la suite d'un message inattendu.

- Changer ses mots de passe : Modifier le mot de passe Relais Colis par simple précaution.

- Réagir vite en cas d'erreur : Faire immédiatement opposition auprès de la banque si vous avez cliqué et saisi vos coordonnées.

Article : Fuite massive de données médicales et administratives touchant 15 millions de Français. Source : Siècle Digital (et autres médias nationaux début mars 2026).

Source : Siècle Digital
Date : Début Mars
Lien : Siecledigital

L'article rapporte l'une des plus importantes fuites de données de santé en France. Une cyberattaque survenue fin 2025 a ciblé un logiciel d'édition médicale appartenant à la société **Cegedim Santé**. Ce logiciel était utilisé par environ 1 500 médecins sur le territoire. Les conséquences de ce piratage ont été confirmées récemment, révélant que les données d'environ **15 millions de patients** se sont retrouvées exposées et en libre accès sur le net.

Recommandation :

- Hyper-vigilance sur les communications : Ne communiquer aucune coordonnée bancaire, mot de passe ou identifiant *Ameli* suite à un appel, un SMS ou un e-mail inattendu, même si la personne connaît votre nom et votre médecin.

- Double authentification (2FA) : Renforcer la sécurité de tous ses espaces personnels liés à la santé (Ameli, mutuelle, messageries).

- Se renseigner : Si votre médecin utilise ce logiciel, surveillez attentivement les notifications officielles qui pourraient vous être adressées par les autorités ou la CNIL.

5. Diffusion :