Dossier de Veille Technologique

Réalisé par Kevan Poirier – Dewi Guerin

Sommaire

Introduction

La transformation numérique, bien que porteuse d'opportunités, expose les organisations à de nouveaux risques, notamment les **cyberattaques**. Cette veille technologique porte sur la **vulnérabilité des secteurs disposant de ressources limitées** (PME, santé, éducation, collectivités locales) face aux menaces numériques, ainsi que sur les **mesures de protection adaptées à leurs moyens**.

Notre objectif est d'identifier :

- Les secteurs les plus touchés durant la période observée.
- Les attaques marquantes survenues entre **février et avril 2024**.
- Les solutions ou bonnes pratiques pouvant être mises en œuvre avec des ressources limitées.

Outils et Méthodes de Veille Utilisés

Pour mener cette veille, nous avons utilisé les outils suivants :

- **Google Alerts** : Configuration d'alertes avec des mots-clés comme *"cyberattaque PME"*, *"hôpital piraté"*, *"ransomware éducation"*, etc.
- **Feedly** : Agrégation de flux RSS spécialisés (ANSSI, ZDNet, BleepingComputer, CERT-FR).
- **Sites spécialisés** : Consultation régulière de sites tels que **LeMagIT**, **Cybermalveillance.gouv.fr**, **The Hacker News**.

Fréquence de veille : Lecture et synthèse des alertes et flux **1 à 2 fois par semaine**, avec un focus renforcé sur les incidents concrets survenus entre le 15 février et le 11 avril 2024.

Bilan de la Veille

Tendances observées (février–avril 2024)

Durant cette période, plusieurs attaques ont mis en lumière la vulnérabilité persistante de certains secteurs :

- **Centre Hospitalier d'Armentières (Nord)** :
  Dans la nuit du 10 au 11 février 2024, le CH d'Armentières a été victime d'une cyberattaque revendiquée par le groupe Blackout. Environ 300 000 patients sont concernés par les fichiers volés lors de cette attaque. L'établissement a dû fermer temporairement ses urgences à la suite de cette cyberattaque.
- **Centre Hospitalier de Cannes** :
  Le 16 avril 2024, le centre hospitalier Simone Veil de Cannes a été victime d'une cyberattaque. Près de 62 Go de données compressées volées ont été divulguées.
- **Consulting Radiologists Ltd. (États-Unis)** :
  Le 11 février 2024, un important fournisseur de services de radiologie à distance aux États-Unis a été victime d'une cyberattaque, entraînant des perturbations dans les services de diagnostic dans plusieurs cliniques, affectant principalement les petites structures de santé.

Analyse des causes

Les raisons pour lesquelles ces secteurs sont vulnérables incluent :

- Faibles budgets dédiés à la cybersécurité.
- Manque de formation du personnel.

- Systèmes d'information anciens ou non mis à jour.
- Absence d’équipes internes spécialisées en sécurité.

Mesures de protection abordables

Voici les actions recommandées, même avec un budget limité :

- **Sensibilisation des utilisateurs** (campagnes internes, phishing simulé).
- **Sauvegardes régulières** externalisées.
- **Logiciels open source de sécurité** (ex. : pfSense pour firewall, ClamAV pour antivirus).
- **Mise en place de MFA (authentification à deux facteurs)**.
- **Recours aux plateformes de signalement et d'assistance** (ex. : cybermalveillance.gouv.fr).

Tableau de Veille Technologique

Date	Événement / Source	Secteur concerné	Type de menace	Réponse / Solution observée
11/02/2024	Cyberattaque au CH d'Armentières	Santé	Ransomware	Fermeture temporaire des urgences, enquête en cours
16/04/2024	Cyberattaque au CH de Cannes	Santé	Ransomware	Divulgation de données, reprise partielle des activités
11/02/2024	Cyberattaque chez Consulting Radiologists Ltd.	Santé (États-Unis)	Ransomware	Perturbations des services de diagnostic, enquête en cours

Conclusion

Cette veille technologique a permis d'observer une **intensification des cybermenaces** sur des secteurs souvent démunis face aux attaques. Malgré cela, des actions concrètes et accessibles existent pour **améliorer la résilience numérique** de ces structures.

Elle a aussi permis de comprendre l'importance de :

- Maintenir une veille régulière et multicanale.
- Renforcer la **culture de sécurité** en interne.
- Mutualiser les ressources et les compétences (ex : regroupements de collectivités, syndicats intercommunaux).

Enfin, il est essentiel de **ne pas sous-estimer les risques**, même dans de petites structures, et de faire de la cybersécurité une **priorité stratégique**, au même titre que la continuité d'activité.