BTS SIO

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

SYNTHÈSE DE CYBERINTELLIGENCE ET SURVEILLANCE DES MENACES

Candidat : Alenzo Wauters

Spécialité : SISR (Solutions d'infrastructure, systèmes et réseaux)

Thématique : Analyse des flux CERT-FR et veille sur les vulnérabilités critiques.

SOMMAIRE

Table des matières

1. Introduction : Pourquoi surveiller la menace ?

Visant à terme un poste de **Manager en infrastructures**, je considère la compréhension des alertes techniques comme une étape indispensable à la réussite de mon projet professionnel. Je dois savoir quelles sont les "portes" que les attaquants essaient d'ouvrir en ce moment même.

La cyberintelligence, c'est ce qui me permet d'avoir un coup d'avance pour protéger mon réseau.

2. Le CERT-FR : Ma source de confiance technique

Le **CERT-FR** (Centre d'alerte et de réaction aux attaques informatiques) est ma référence absolue.

- **Ce que je surveille :** Les bulletins d'alerte sur les systèmes Microsoft, VMware et les équipements réseaux (Cisco, Fortinet).
- **Ma méthode :** Dès qu'une alerte sort, je regarde le **score CVSS** (gravité) pour savoir si c'est une urgence absolue.

3. Étude d'une vulnérabilité majeure : L'attaque d'envergure contre les lycées des Hauts-de-France (Octobre 2025)

Date de rédaction du présent dossier : 17 janvier 2026

Le 10 octobre 2025, le Conseil régional des Hauts-de-France a détecté une intrusion massive sur son infrastructure numérique, impactant directement les 263 lycées publics de la région. Cette attaque, toujours au cœur de l'actualité au moment où je rédige ces lignes, constitue l'un des incidents les plus graves touchant le secteur éducatif français.

Informations concrètes sur l'incident :

- **Type d'attaque :** Selon les éléments partagés par les services de l'État et les organisations syndicales comme l'UNSA, il s'agit d'une **cyberattaque par rançongiciel (ransomware)** d'une grande technicité. Les attaquants ont réussi à s'infiltrer dans le réseau régional et à chiffrer des serveurs critiques.
- **Source et vecteurs :** L'analyse préliminaire indique que la faille initiale pourrait provenir d'une compromission d'identifiants ou d'une vulnérabilité sur un service d'accès distant, permettant aux pirates de se propager latéralement dans l'architecture régionale.
- **Impact opérationnel :** La paralysie a été totale pour les outils de gestion (ENT, logiciels de vie scolaire, accès Wi-Fi, services de restauration et de paie). En décembre 2025, soit deux mois après l'attaque, de nombreux services restaient inaccessibles, forçant les établissements à un retour "au papier" pour de nombreuses missions administratives.
- **Résolution et perspectives :** À ce jour (janvier 2026), le rétablissement complet est encore en cours. La Région a engagé des experts en cybersécurité pour reconstruire un environnement sain, privilégiant une remise en service progressive pour éviter toute réinfection.

Arguments pour le dossier de veille : Cette situation est "critique" car elle met en évidence une absence de perspectives de retour à la normale rapide, soulignant qu'une attaque par ransomware ne se résout pas simplement par une restauration de sauvegarde. Pour mon objectif professionnel de

Manager en infrastructures, ce cas d'école démontre l'importance vitale du **Plan de Reprise d'Activité (PRA)**. Le fait que l'attaque ait pu paralyser toute une région souligne la nécessité de **segmenter les réseaux** de manière beaucoup plus drastique pour isoler chaque établissement en cas de compromission du nœud central.

ıмedi 17 janvier
te des Roseline

ici

Télévision Radio L'actu chez vous

ise agricole Thématiques Services Radio musicale Partir en week-end

Nord • Pas-de-Calais

Cyberattaque dans les lycées des Hauts-de-France : la Région lance un plan massif pour renforcer la sécurité

Il y a encore des perturbations dans certains établissements où les enseignants doivent adapter leur pédagogie (image d'...

Sophie Morlans

Publié le jeudi 11 décembre 2025 à 18:04

Encore des lycées pénalisés dans leur fonctionnement pédagogique

Ce plan est très attendu dans les lycées où il y a des disparités selon les établissements constate Florence Delannoy, proviseure du lycée Montebello à Lille et secrétaire académique adjointe du SNPDEN, le syndicat national du personnel de direction de l'Éducation nationale. "*Dans mon établissement, on est opérationnel malgré des ralentissements internet. En revanche, c'est plus difficile dans les lycées où l'outil numérique est indispensable d'un point de vue pédagogique, comme les lycées professionnels ou ceux qui proposent des enseignements techniques. Il y a un accompagnement par les inspecteurs, mais malgré leur investissement, cela devient difficile.*"

Ces difficultés sont prises en compte par le rectorat et le seront aussi pour les examens, mais cela ne répond pas aux inquiétudes de Nicolas Penin, secrétaire régional du syndicat UNSA Education. "*Deux mois de pénalité, c'est énorme dans une année scolaire, notamment pour les élèves qui sont en contrôle continu ou qui préparent des concours dans des écoles qui ne prendront pas en compte la spécificité de notre région.*"

Un chantier immense

"*Nous espérons que les choix technologiques qui seront faits seront les bons*", ajoute Florence Delannoy. "*Certes la Région a mis beaucoup de moyens, mais c'est un chantier immense. On s'interroge beaucoup sur la mise en place de ce prochain système.*"

État des lieux de la cyberattaque en décembre 2025. Cette source confirme la paralysie prolongée des services numériques et l'incertitude quant à la date de résolution complète, justifiant une approche de sécurité plus résiliente.

Source : https://www.francebleu.fr le jeudi 11 décembre 2025.

4. Impact pour l'entreprise et remédiation

Face à une menace, je réfléchis aux actions à mener :

- **Correctif :** Appliquer les mises à jour de sécurité (patching).
- **Protection :** Isoler les serveurs sensibles (segmentation) pour éviter que le virus ne se propage.
- **Sauvegarde :** Vérifier que les backups sont déconnectés du réseau pour rester à l'abri.

5. Conclusion : La cyberintelligence au quotidien

Cette veille me permet d'être réactif. En tant qu'étudiant en **SISR**, savoir lire et interpréter une alerte technique est aussi important que de savoir configurer un routeur. C'est cette vigilance qui garantit la **continuité de service** d'une infrastructure moderne.