

**FORMATION SPECIALISEE DE SITE
DES LYCEES ET DU CREPS**

REUNION DU 18 AVRIL 2024

RAPPORT POUR INFORMATION

**Point sur le piratage des Environnements Numériques de Travail (ENT) et la
sûreté-sécurité dans les lycées**

1/ Contexte

Pour mémoire, l'éducation est un service public national dont l'organisation et le fonctionnement sont assurés par l'Etat, sous réserve des compétences attribuées aux collectivités territoriales qui y participent.

La Région a ainsi la charge des lycées publics dont elle a la propriété et, à ce titre, en assure la construction, la reconstruction, l'extension, les grosses réparations et les travaux à vocation patrimoniale comprenant notamment la sécurisation périmétrique des bâtiments, la sûreté et la sécurité incendie. Dans le cadre de ses missions relatives à la « prévention », elle conseille le Chef d'établissement en matière d'hygiène et de sécurité, afin de prévenir les dangers susceptibles de compromettre la sécurité et la santé des agents. Cette fonction relève des dispositions du Code du travail.

Lorsqu'un danger grave et imminent se déclare dans l'enceinte de l'EPLE, c'est par contre au Chef d'établissement qu'il appartient, au titre de sa mission de protection des personnes et des biens, de prendre toutes mesures d'urgence propres à préserver la sécurité (Code de l'éducation).

Diffusion de messages malveillants sur les ENT régionaux dès le 21 mars 2024

Depuis le jeudi 21 mars près de 400 établissements sur une vingtaine d'académies ont fait l'objet de messages malveillants via les Environnements Numériques de Travail (ENT). Ces incidents ont été très marquants par leur ampleur (caractère national et coordonné) et la nature de leurs contenus (diffusion de menaces et d'une vidéo choquante), conduisant la Ministre de l'éducation nationale et de la jeunesse à rapidement décider la suspension des messageries ENT.

C'est au cours du week-end des 23 et 24 mars 2024 que de tels messages ont été diffusés sur les messageries de l'ENT HDF.

Pour mémoire, l'ensemble des écoles, collèges et lycées des Hauts-de-France utilisent l'ENT HDF, ce qui fait de cet ENT le 1^{er} ENT au niveau national, et même européen, de par son ampleur. Il permet de réunir **2,8 millions d'utilisateurs, dont près d'1 million d'élèves**.

Dès les premiers signalements le samedi 23 mars matin, les acteurs du projet HDF (collectivités, académies et prestataire) se sont mobilisés pour mettre en œuvre les mesures nécessaires afin de protéger les usagers et fournir les informations demandées par les forces de l'ordre.

Chronologie des faits en Hauts-de-France :

Samedi 23 mars matin : La région académique Hauts-de-France a signalé des menaces (menaces terroristes) via l'ENT régional pour plusieurs établissements (collèges et lycées). La cellule de crise a immédiatement été activée et il a été décidé la fermeture de la messagerie de l'ENT pour les élèves pour l'ensemble des 5 000 établissements concernés, le temps d'évaluer l'ampleur de la situation, de bloquer les comptes usurpés, de « nettoyer » les messageries ciblées et de saisir les autorités judiciaires.

Dimanche 24 mars soir : des personnels d'établissements agricoles signalent la circulation de messages comportant une vidéo violente dans la messagerie de l'ENT HDF, ce qui a très rapidement déclenché la fermeture complète de la messagerie, par la cellule de crise, afin de protéger tous les utilisateurs et de réaliser les investigations nécessaires.

Après investigations au niveau national et par les collectivités, il n'a pas été relevé d'intrusions par exploitation de failles ou de vulnérabilité de sécurité. Il ne s'agirait donc pas d'une cyber-attaque, mais d'usurpations d'identité avec récupération d'identifiants et de mots de passe.

Ces usurpations d'identité ont concerné 13 comptes le samedi et 18 comptes le dimanche pour l'ENT HDF.

Menaces attentat et alertes à la bombe concomitantes

Depuis le 21 mars 2024 se sont également succédées les menaces attentat et alertes à la bombe. En Hauts-de-France, 10 lycées ont été concernés au total : 5 par des alertes à la bombe et 5 par des menaces d'attentat.

Ces alertes et menaces ont à chaque fois conduit à des évacuations complètes des établissements concernés (et dépôts de plainte). Elles s'ajoutent à l'attentat et aux 4 alertes à la bombe déjà vécus par les lycées Gambetta et Savary-Ferry à Arras du 13 octobre au 5 décembre 2023 :

ÉTABLISSEMENTS VICTIMES D'ACTES MALVEILLANTS				
DEPARTEMENT	VILLE	EPL	DATE DU DEPOT DE PLAINTE	OBJET
NORD	ROUBAIX	Jean Moulin	23/01/2024	Alerte à la bombe et évacuation de l'établissement
NORD	ROUBAIX	Loucheur	23/01/2024	Alerte à la bombe et évacuation de l'établissement
NORD	ROUBAIX	Van Der Meersch	07/02/2024	Menace attentat et évacuation de l'établissement
NORD	GRANDE SYNTHE	Noordover	09/02/2024	Menace attentat et évacuation de l'établissement
NORD	LOOS	Duhamel	21/02/2024	Menace attentat et évacuation de l'établissement
NORD	LOOS	Duhamel	23/02/2024	Menace attentat et évacuation de l'établissement
NORD	MONTIGNY EN OSTREVENT	René Cassin	02/04/2024	Menace attentat et évacuation de l'établissement
NORD	SOMAIN	Pasteur	02/04/2024	Menace attentat et évacuation de l'établissement
NORD	CAMBRAI	Paul Duez	08/04/2024	Alerte à la bombe et évacuation de l'établissement
PAS-DE-CALAIS	ARRAS	Gambetta	13/10/2023	Attentat et évacuation de l'établissement
PAS-DE-CALAIS	ARRAS	Gambetta	16/10/2023	Alerte à la bombe et évacuation de l'établissement
PAS-DE-CALAIS	ARRAS	Gambetta	06/11/2023	Alerte à la bombe
PAS-DE-CALAIS	ARRAS	Gambetta	07/11/2023	Alerte à la bombe
PAS-DE-CALAIS	ARRAS	Savary / Ferry	05/12/2023	Alerte à la bombe
PAS-DE-CALAIS	LENS	Robespierre	07/02/2024	Alerte à la bombe et évacuation de l'établissement
SOMME	AMIENS	Cité Sud	27/03/2024	Alerte à la bombe et évacuation de l'établissement

2/ Sécurisation de l'ENT (DDPE)

A titre introductif, il est rappelé que l'accès à l'ENT HDF est réalisé par fédération d'identité pour les comptes élèves, parents et personnels de l'Education nationale. L'authentification des utilisateurs est réalisée par des services Educonnect et Arena, gérés et administrés par le

Ministère de l'Education nationale et les autorités académiques. Après investigations, les usurpations ont été constatées sur ces comptes Educonnect et Arena.

Les enquêtes judiciaires qui ont eu lieu lors d'une précédente vague d'actes malveillants ont montré que les usurpations de comptes d'accès des élèves ou des familles étaient essentiellement dues à la négligence des utilisateurs (absence de déconnexion, mot de passe visible de tous, à faible niveau de sécurité, etc.), ou liés à des logiciels malveillants dérobeurs de mots de passes. Ces outils, très largement diffusés et implantés dans des logiciels contrefaits sont faciles à prendre en main notamment par des utilisateurs malveillants.

Par ailleurs, il est régulièrement publié sur Internet des bases de données d'identifiants volés que des individus malintentionnés peuvent se procurer. Les comptes Educonnect permettant l'accès à de nombreuses applications, il est alors aisé d'accéder à la messagerie de l'ENT.

Cependant, il est important de préciser que, au cours de l'analyse de ces usurpations, il n'a pas été relevé d'intrusions par exploitation de failles ou de vulnérabilités de la sécurité de l'ENT HDF, qui fait l'objet d'audits réguliers par les collectivités qui le déploient, démontrant le haut niveau de sécurité de la plateforme.

Actions réalisées et décisions prises

La gestion de cet incident a fait l'objet de réunions quotidiennes de la cellule de crise réunissant l'ensemble des collectivités (via Régions de France et l'Association des Départements de France), dont une en présence de la Ministre de l'Education nationale, et de nombreux échanges avec Régions de France dans le cadre du comité technique ENT et avec la DNE (Direction du Numérique pour l'Education du Ministère de l'Education Nationale) pour statuer sur un plan d'actions commun à l'ensemble du territoire national.

Suite à ces incidents ne remettant pas en cause la sécurité des ENT, le groupement de commandes (la Région, les cinq Départements) et le prestataire en charge de l'ENT ont décidé d'appliquer des mesures complémentaires à plus ou moins long terme et notamment :

- Le blocage des comptes utilisateurs usurpés,
- L'effacement des messages menaçants,
- Le dépôt de plainte par les chefs d'établissement et la Région,
- Le blocage du compte après plusieurs tentatives infructueuses,
- La réinitialisation de tous les mots de passe des comptes « manuels » qui ne disposent pas d'accès via Educonnect (<5% des comptes) et la suppression de tous les comptes manuels qui disposent d'une authentification possible via Educonnect,
- Le filtrage par adresse « internet protocole » (IP) de connexion : déploiement du dispositif Carapace qui permet de bloquer les IP étrangères, les VPN étrangères et françaises, ainsi que les IP illégitimes (liste noire). Par ailleurs, une liste blanche est en place, en particulier pour les IP d'établissement,
- L'envoi d'un courriel d'alerte en cas de connexion suspecte (navigateur inhabituel et/ou adresse IP),
- La fermeture nocturne des messageries : désactivation des envois de messages entre 23h et 7h,
- La surveillance proactive des messages,
- L'application du principe du moindre privilège pour les droits de messagerie : les règles de communication pour les profils élèves et parents sont limitées au périmètre de la classe, et

peuvent être ajustées localement en fonction du contexte de chaque école et établissement par les administrateurs locaux.

Du côté des autorités académiques et du Ministère de l'EN, des mesures ont également été décidées et sont en cours :

- La réinitialisation de tous les mots de passe Educonnect (élèves, parents, enseignants, personnels) avec, si possible techniquement, l'interdiction des x mots de passe précédents,
- La diffusion de bonnes pratiques de sécurité auprès des utilisateurs,
- La sensibilisation des utilisateurs aux risques de stealers et de hameçonnage,
- La surveillance du dark web.

En attendant la mise en œuvre de l'intégralité de ces mesures relevant de la responsabilité de différents partenaires, la messagerie de l'ENT HDF reste inaccessible aux élèves et partiellement accessible aux parents, personnels et enseignants (fermeture la nuit) depuis le mercredi 3 avril.

Des rappels de bonnes pratiques sur l'usage des outils numériques sont réalisés chaque fois que nécessaire pour sécuriser, à titre préventif comme en réaction à des messages malveillants, l'ensemble des accès et des messageries des parents, élèves, enseignants et personnels. Dans un contexte international particulièrement instable, ces rappels de bonnes pratiques sont indispensables et il doit être fait appel à la vigilance et à la responsabilité de toute la communauté éducative.

3/ Sûreté – sécurité des établissements (MIPAL / DEPL)

Pour mémoire et ainsi que rappelé lors de la réunion de la FSS du 20/02/2024, afin d'assurer la sécurité incendie et de développer la sûreté au sein des Etablissements Publics Locaux d'Enseignement (EPL), la Région a adopté un plan de sûreté, décliné de la manière suivante : sonneries différenciées dans le cadre de la mise en œuvre des Plans Particuliers de Mise en Sûreté (PPMS), priorisation des travaux de sûreté périmétrique des bâtiments (clôtures-portails) et généralisation de la vidéo-protection aux entrées et sorties des EPL.

Par ailleurs, le maintien, auprès des Commissions de sécurité, des « Avis favorables » à l'exploitation des lycées nécessite le remplacement des Systèmes de Sécurité Incendie (SSI) obsolètes et la levée des prescriptions émises par ces Commissions.

Considérant que la sécurité des usagers est une priorité institutionnelle, la Région Hauts-de-France s'est engagée dans la mise en œuvre d'un plan de sûreté au sein des établissements scolaires relevant de sa compétence (délibération n°20170468 du 18 mai 2017).

29 millions d'euros ont depuis été affectés à cette politique et une Autorisation de Programme (AP) de 3,5 millions d'euros est retenue au titre du Budget Primitif 2024.

A la suite de l'attentat perpétré au lycée Gambetta Carnot d'Arras, une enquête flash a été lancée mi-octobre auprès des 272 lycées publics et CFA régionaux afin d'identifier l'ensemble des dysfonctionnements et fragilités constatés sur la sûreté périmétrique (clôture, portail, portillon, tourniquet), la vidéo protection et les dispositifs PPMS.

Des alertes et demandes d'adaptions d'aménagement sont venues compléter cet état des lieux via différents canaux (courriers, mails d'interpellations de proviseurs, élus...).

Afin d'accélérer les interventions relatives à la sécurisation des lycées, toutes les équipes en capacité d'y contribuer ont été mobilisées. La compétence sûreté sécurité périmétrique des lycées (portail, portillon, clôtures, tourniquet, gestion accès) a ainsi été reprise par la DEPL depuis début novembre 2023, la MIPAL amplifiant ses interventions relatives aux PPMS, aux SSI et à la vidéo-protection.

Une délibération créant une enveloppe spécifique dotée d'une autorisation de programme de 10 millions d'euros a été votée en séance plénière du 15 décembre 2023 pour financer une 1ère phase de travaux de sécurisation globale des sites en 2024.

S'agissant des travaux de sûreté périmétrique, sur les 272 lycées que compte la Région, 178 sont considérés comme « traités » au regard de l'enjeu de sécurisation accrue des établissements dans ce contexte, dont 34 avec encore quelques ajustements nécessaires et en cours de traitement.

94 établissements nécessitent des travaux plus conséquents en cours de programmation (pour une réalisation en 2024-2025) : 33 dans le Nord, 30 dans le Pas-de-Calais, 13 dans l'Aisne, 9 dans l'Oise et 9 dans la Somme. Cela représente 35 établissements de moins qu'au 6 décembre 2023.

S'agissant de la mise en conformité des dispositifs « PPMS » et de la généralisation de la vidéo-protection placée aux entrées et sorties des lycées, 147 établissements restent à traiter totalement ou partiellement (complément de caméras). **26 commandes de travaux ont été engagées** et les études se poursuivent pour les autres établissements.

En parallèle, la DRH déploie une formation à destination de l'ensemble des établissements en lien avec cet enjeu de sûreté - sécurité : formation à la Sûreté - Sécurité Incendie.

Cette formation concerne l'ensemble des agents d'accueil de la collectivité, soit plus de 300 agents. En lien avec les travaux du Plan de sûreté au profit des lycées, son contenu a été complété pour intégrer les aspects de la sécurité incendie.

A l'issue de cette formation de 2 jours, les agents devront ainsi maîtriser le cadre théorique et pratique et être en mesure de mettre en œuvre les comportements adéquats dans une situation de risque.

Les objectifs de la formation sont :

En matière de sûreté :

- Le contexte sécuritaire actuel
- Le cadre légal et secteurs concernés
- Les grands principes de la lutte contre la malveillance et les mesures préconisées
- Mesures préventives pour les différents type d'actes ou de risques (malveillance, intrusions, terrorisme ...)
- Les comportements suite à une agression (rôle attendu de chacun, les bons comportements à adopter, les bonnes pratiques à connaître)

En matière de sécurité incendie:

- Les notions de sécurité incendie au sein des Etablissements Recevant du Public (ERP)
- La définition et composition d'un Système de Sécurité Incendie (SSI)
- Temporisation de l'équipement d'alarme
- Exploitation de l'alarme restreinte et levée de doute
- Alarme générale et évacuation du public
- Alerte auprès des sapeurs-pompiers
- Accueil des services de secours

Le besoin a été intégré à l'accord-cadre 2023/2026 « Achat de prestations de formation en matière de sécurité, santé et prévention des risques professionnels, sureté – sécurité incendie » dont le renouvellement a été lancé fin 2022.

Afin d'être au plus proche des résidences administratives des agents, sur cette thématique, 5 lots ont été identifiés (1 par département). L'organisme CREFO a été retenu. Le dossier a été présenté à la CAO de juin 2023. La mise en œuvre a débuté en février 2024.

Une priorisation par bassins d'éducation a été faite et les chefs d'établissement ont été sensibilisés pour faciliter l'accès des agents aux formations. Les formations sont faites uniquement sur les temps de permanence pendant les vacances scolaires.

Planning actuel avec dates :

Thématique	Date 1er jour	Date 2ème jour	Lieu	Nombre d'agents
HDF - SURETE - SECURITE INCENDIE - ARRAS	26/02/2024	27/02/2024	Lycée Savary Ferry	15
HDF - SURETE - SECURITE INCENDIE - BETHUNE	22/04/2024	23/04/2024	Lycée Louis Blaringhem	12
HDF - SURETE - SECURITE INCENDIE - LIEVIN	26/02/2024	27/02/2024	Lycée Henri Darras	16
HDF - SURETE - SECURITE INCENDIE - SAINT POL SUR TERNOISE	22/04/2024	23/04/2024	Lycée Pierre Mendès France	15

Planning à venir :

Les dates ne sont pas encore arrêtées. Une projection est en cours avec l'organisme.

Au 22 mars 2024, 216 agents sont inscrits :

Thématique	Lieu	Nombre d'inscrits
HDF - SURETE - SECURITE INCENDIE - ABBEVILLE	Lycée des métiers Boucher de Perthes	5
HDF - SURETE - SECURITE INCENDIE - AMIENS	Lycée Jean Baptiste Delambre	13
HDF - SURETE - SECURITE INCENDIE - ARMENTIERES	Lycée Gustave Eiffel	14
HDF - SURETE - SECURITE INCENDIE - BEAUVAIS	Lycée Paul Langevin	8
HDF - SURETE - SECURITE INCENDIE - BOULOGNE SUR MER	Lycée Mariette	14
HDF - SURETE - SECURITE INCENDIE - CALAIS	Lycée Pierre de Coubertin	13
HDF - SURETE - SECURITE INCENDIE - CAMBRAI	Lycée Paul Duez	9
HDF - SURETE - SECURITE INCENDIE - CHAUNY	Lycées publics de Chauny	15
HDF - SURETE - SECURITE INCENDIE - CLERMONT	Lycée Cassini	9
HDF - SURETE - SECURITE INCENDIE - COMPIEGNE	Lycée Mireille Grenet	7
HDF - SURETE - SECURITE INCENDIE - DENAIN	Lycée Alfred Kastler	13
HDF - SURETE - SECURITE INCENDIE - HAUTMONT	Lycée Placide Courtoy	14
HDF - SURETE - SECURITE INCENDIE - LA FERTE MILON	Lycée Château Potel	11
HDF - SURETE - SECURITE INCENDIE - LOMME	Lycée Sonia Delaunay	10
HDF - SURETE - SECURITE INCENDIE - SIN LE NOBLE	Lycée Arthur Rimbaud	10
HDF - SURETE - SECURITE INCENDIE - TOURCOING	Lycée Le Corbusier	11
HDF - SURETE - SECURITE INCENDIE - VILLENEUVE D'ASCQ	Lycée Raymond Queneau	16
HDF - SURETE - SECURITE INCENDIE - WATTRELOS	Lycée Emile Zola	9
HDF - SURETE - SECURITE INCENDIE - WORMHOUT	Lycée de l'Yser	15

Un premier bilan intermédiaire montre que les premières sessions programmées présentent un taux d'absentéisme important : 47 % à Arras soit 6 agents présents, et 30 % à Liévin soit 11 agents présents. Les premiers retours de la part des agents sont cependant positifs. Les agents présents ont fortement adhéré à cette formation et trouvé que la présentation de l'intervenant était très prenante.