CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Protéger l'atelier : les 10 fondamentaux de la cybersécurité industrielle

2017 · NotPetya

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE



200-300 M$

d'impact pour Maersk

Maersk, Saint-Gobain, Merck, Mondelez... dans le monde entier

Type d'attaque	Logiciel destructeur déguisé en rançongiciel : les données ne pouvaient pas être récupérées
Point d'entrée	Mise à jour piégée d'un logiciel comptable ukrainien, puis propagation automatique sur les réseaux
Production	Maersk paralysé du 27 juin au 9 juillet. Saint-Gobain revenu à la normale le 10 juillet
Impact financier	Saint-Gobain : ≈ 250 M€ de chiffre d'affaires et ≈ 80 M€ de résultat d'exploitation perdus

2019 · Norsk Hydro

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE



≈ 800 M NOK

coût total estimé par l'entreprise (≈ 70 M€)

Producteur d'aluminium, 19 mars 2019

Type d'attaque	Rançongiciel (LockerGoga) qui chiffre le système d'information de l'ensemble du groupe
Production	Fonderies et laminage tournent en mode manuel. L'activité extrusion est la plus touchée
Réponse	Restauration depuis les sauvegardes et communication publique transparente tout au long de la crise
Couverture	Une assurance cyber en place auprès d'assureurs reconnus

2021 · Colonial Pipeline

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE



4,4 M$

de rançon payée, en partie récupérée par le FBI

Plus grand oléoduc de carburant des États-Unis

Type d'attaque	Rançongiciel à double extorsion (groupe DarkSide), environ 100 Go de données volées
Point d'entrée	Mot de passe d'un ancien compte VPN inutilisé, sans authentification multifacteur
Production	Oléoduc arrêté par précaution du 7 au 12 mai, alors que seule l'informatique de gestion était touchée
Impact	Près de la moitié du carburant de la côte Est, pénuries et état d'urgence dans plusieurs États

Qui sont les attaquants ?

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE



Cybercriminels

Groupes organisés qui vivent de leurs attaques : rançongiciels, revente de données.



Hacktivistes

Militants qui attaquent pour une cause : sites bloqués, données publiées.



États

Services de renseignement ou militaires : espionnage et sabotage d'infrastructures.



Terroristes

Cherchent à frapper les esprits ou à provoquer des dégâts physiques.

Quelles sont les motivations ?

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE



Économique

Rançon, revente de données ou de savoir-faire : la motivation la plus fréquente.



Espionnage

Voler plans, procédés de fabrication et secrets industriels.



Idéologie

Défendre une cause ou nuire à l'image d'une entreprise.



Politique

Déstabiliser un pays, ses infrastructures et son économie.

Pourquoi l'atelier est si exposé

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Tout est connecté

L'atelier est relié au bureau, au cloud, à l'ERP et aux fournisseurs. Une attaque au bureau peut atteindre la production.

Des équipements qui durent 20 ans

Conçus avant les menaces actuelles, souvent obsolètes et difficiles à mettre à jour.

La production ne doit pas s'arrêter

Pas question de redémarrer ou de patcher un automate à tout moment : chaque intervention se planifie.

Les 10 fondamentaux

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

1 Cartographier

2 Segmenter

3 Accès distants

4 Sauvegarder

5 Identités

6 Mises à jour

7 Surveiller

8 Sensibiliser

9 Cyber dans les process

10 Préparer la crise

1 · Cartographier

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

On ne protège que ce que l'on connaît.

- Inventaire des équipements IT et OT : automates, robots, PC de supervision
- Versions, fournisseurs et fin de support
- Flux et accès externes : qui se connecte, d'où, et pourquoi

Question à se poser : *si un automate tombe demain, savez-vous à quoi il est relié ?*



2 · Segmenter

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Une attaque au bureau ne doit pas atteindre l'atelier.

- Réseau de production séparé du réseau bureautique
- Pare-feu et zone tampon (DMZ) pour les échanges
- Seulement les flux strictement nécessaires
- Aucun automate ni supervision exposé directement sur Internet



Question à se poser : *un e-mail piégé ouvert à la compta peut-il atteindre l'atelier ?*

3 · Maîtriser les accès distants

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

La télémaintenance est la porte d'entrée préférée des attaquants.

- Recenser tous les accès : TeamViewer, VPN, modems 4G
- Comptes nominatifs et authentification multifacteur (MFA)
- Fermés par défaut, ouverts à la demande et tracés



Question à se poser : *combien d'accès distants sont ouverts en permanence ?*

4 · Sauvegarder

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

La sauvegarde, c'est ce qui permet de redémarrer.

- Données, programmes d'automates, robots et recettes
- Au moins une copie hors ligne
- Restauration testée régulièrement



Question à se poser : *une sauvegarde jamais restaurée n'est qu'un espoir.*

5 · Gérer les identités

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Un mot de passe par défaut est une porte ouverte.

- Changer tous les mots de passe par défaut
- Supprimer les comptes partagés et inutilisés
- Droits limités au strict nécessaire, MFA pour les administrateurs



Question à se poser : *un salarié parti l'an dernier peut-il encore se connecter ?*

6 · Mettre à jour

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

En usine, on ne patche pas comme au bureau.

- Suivre les vulnérabilités de vos équipements (CERT-FR, fournisseurs)
- Planifier les correctifs pendant les arrêts programmés
- Isoler ce qui ne peut pas être mis à jour



Question à se poser : *combien de postes Windows XP ou 7 tournent encore à l'atelier ?*

7 · Surveiller

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Quand on ne peut pas tout corriger, il faut au moins voir.

- Centraliser les journaux des pare-feu et serveurs
- Détecter les flux anormaux entre bureau et atelier
- Sonde de détection OT, et quelqu'un pour lire les alertes



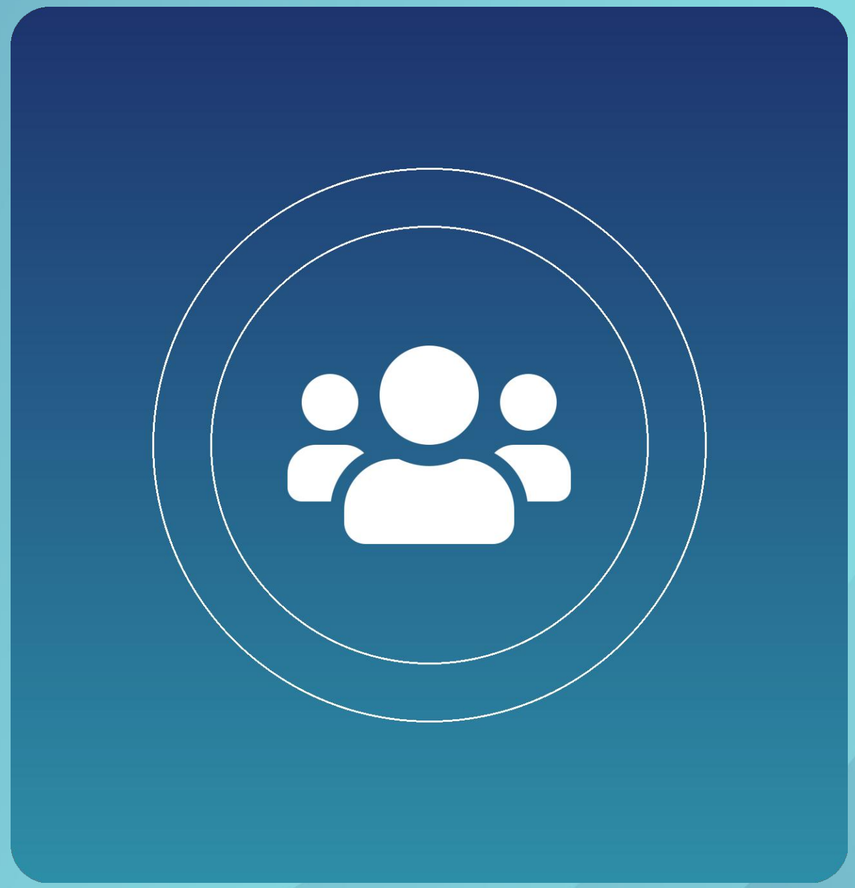
Question à se poser : *combien de temps faudrait-il pour voir un intrus ?*

8 · Sensibiliser

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Les opérateurs sont la première ligne de défense.

- Former l'atelier et la maintenance, pas seulement le bureau
- Station de décontamination pour les clés USB
- Savoir signaler un incident sans crainte



Question à se poser : *vos opérateurs savent-ils à qui signaler un comportement anormal ?*

9 · La cyber dans les process

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

La sécurité se décide en amont.

- Achats : exigences cyber dans le cahier des charges
- Prestataires : exigences au contrat, interventions tracées
- Projets : sécurité prévue dès la conception
- Arrivées et départs : ouvrir et fermer les accès



Question à se poser : *savez-vous ce que fait votre prestataire quand il intervient sur vos machines ?*

10 · Préparer la crise

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

La préparation décide de la durée de l'arrêt.

- Annuaire de crise : direction, IT, fournisseurs, assureur, CSIRT
- Production en mode dégradé, procédures sur papier
- Un exercice de crise par an



Question à se poser : *si votre SI est bloqué demain matin, que faites-vous à 8 h ?*

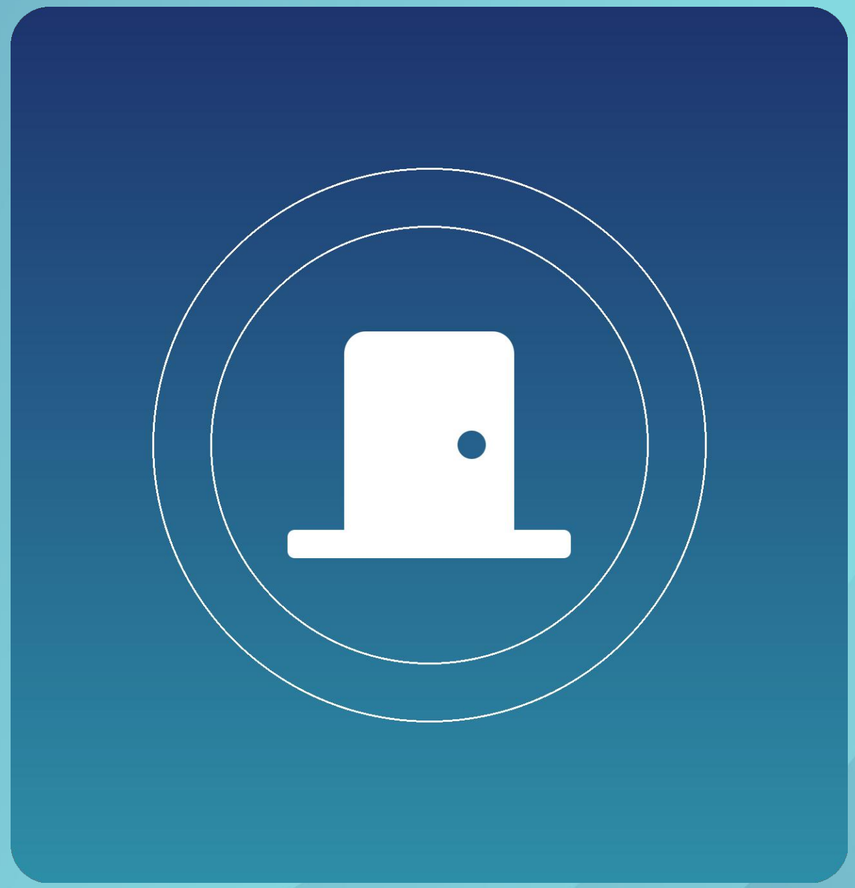
11 · Bonus : sécurité physique

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Une clé USB branchée vaut une attaque à distance.

- Accès aux locaux techniques contrôlés et tracés
- Armoires et coffrets électriques fermés à clé
- Ports USB et réseau inutilisés bloqués
- Visiteurs et intervenants accompagnés

Question à se poser : *un visiteur peut-il brancher une clé USB sur une machine sans être vu ?*



Campus Cyber Summit 2026

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Au programme, pour les dirigeants de PME industrielles :

- *« RSSI et dirigeants : qui décide vraiment du risque ? »*
- *« Sécuriser l'usine 4.0 »*
- *« Cyber assurance : ce que les sinistres nous apprennent »*
- *« NIS 2 : où en sont nos voisins européens ? »*

Inscription : www.campuscybersummit.fr



5 novembre 2026

EuraTechnologies, Lille
8 h 30 – 18 h

CAMPUS CYBER

HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Merci

Camille DESAUNOIS

Startup Manager Cybersécurité

cdesaunois@hdf.campuscyber.fr

hdf.campuscyber.fr