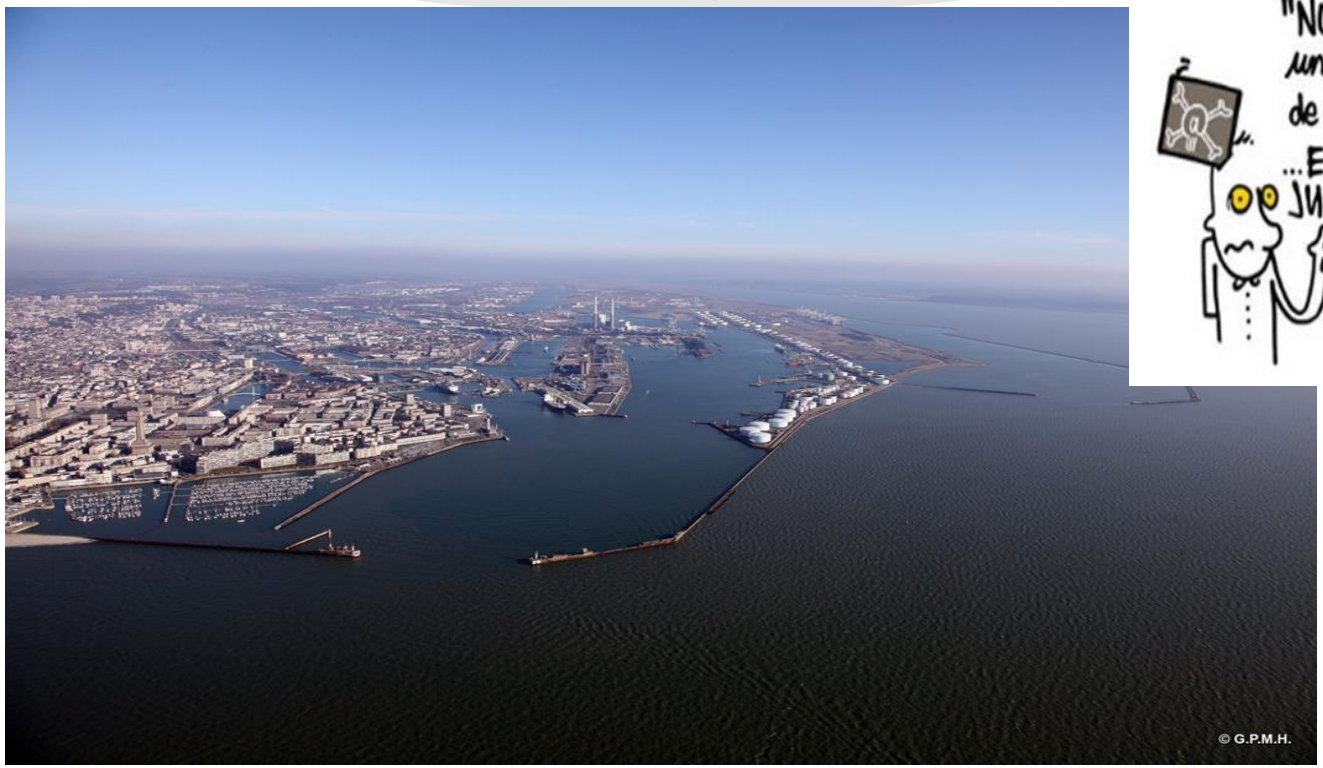
- HAROPA LE HAVRE -
Cybersécurité et crise COVID



Contexte

- Une pandémie sanitaire dans un avenir de grande incertitude
- Une gestion de crise permanente au sein de l'entreprise : du jamais vu
- Des mesures de confinement et de distanciation physiques jusqu'alors inconnues
- Une entreprise plus que jamais dépendante des infrastructures numériques dans un moment critique
- Une recrudescence des cyber attaques

Les enjeux

1/3 – A très court terme : Gérer la crise et la continuité d'activité

2/3 – A court terme : Gérer la reprise d’activité

3/3 – Moyen/long terme : S'adapter et innover dans un monde incertain

Les enjeux 1/3

<u>A très court terme</u> : Gérer la crise et la continuité d'activité

→ Assurer une protection optimale à l'entreprise et aux salariés contre les cyber malveillances (phishing, ransomware, etc.) lors de la crise ;

→ Assurer la continuité des activités, quoiqu'il arrive, même en mode dégradé, via l'organisation de gestion de crise ;

→ Prévoir et encadrer les éventuelles entorses aux règles de sécurité (télétravail, etc.).

RESILIENCE

Résilience 1/3

1 / Maintenir l'activité durant la crise en gérant les risques

S'assurer de la résilience et de la sécurité des infrastructures et des applications critiques accessibles sur Internet (VPN, serveurs mail, visioconférence, partage de fichiers, outils de sécurité, applications métiers, etc.)

2/ Gérer les nouveaux risques et éviter les sur-incidents

3/ Sensibiliser et aider les collaborateurs

Les enjeux 2/3

A Court terme : Gérer la reprise d'activité (Recovery)

→ Assurer le retour à des modalités de travail habituelles en terme sanitaire (présentiel, mesures, etc.) ;

→ Assurer des conditions de cybersécurité acceptables ;

→ Remédier aux entorses de sécurité qui avaient été adoptées.

Reprise d'activité 2/3

1/ Assurer la sortie de crise et rétablir un dispositif de cybersécurité adapté

Préparer et piloter le retour à l'état nominal des systèmes d'information et de la posture cybersécurité

2/ Tirer les leçons de la crise sanitaire

3/ Initier la transformation de la fonction cyber pour s'adapter au nouveau contexte

Les enjeux 3/3

A moyen/long terme : s'adapter et innover (New realities)

→ Adapter la roadmap et l'operating model de la cybersécurité de l'entreprise ;

→ Répondre pleinement aux besoins de l'entreprise mais aussi des clients ;

→ Prendre en compte les impacts économiques ;

→ Réévaluer les moyens alloués à la cybersécurité.

S’adapter et innover 3/3

1/ S’adapter au monde post-crise et assurer l’alignement sur la stratégie de l’entreprise

(Transformer la filière cybersécurité dans l’entreprise pour l’adapter aux nouvelles réalités)

2/ Anticiper et accompagner les projets de transformation numérique et de résilience de l’entreprise face aux risques sanitaires ou autres

4/ Créer un nouveau modèle de place portuaire (SOC)

Merci à toutes et à tous !