CYBERHYGIÈNE

RÉGION-IHEDN
POITOU-CHARENTES

Règles à appliquer en amont des cyber-attaques

RAPPEL : DERNIÈRES CYBER-ATTAQUES MAJEURES

1 – SENSIBILISEZ VOS COLLABORATEURS

2 – GÉREZ VOS MOTS DE PASSE

3 – METTEZ A JOUR VOS APPAREILS, LOGICIELS, ANTI-VIRUS

4 – ÉVITEZ LES COMPORTEMENTS A RISQUES

5 – SAUVEGARDEZ

6 – METTEZ EN PLACE DES GARDE-FOUS

7 – N'HÉSITEZ PAS A ENVISAGER DES SOLUTIONS LIBRES

Conséquences possibles d'un piratage

- Détérioration et destruction des données.
- Interruption d'activités.
- Vol de propriété intellectuelle, données personnelles et financières.
- Détournement de fonds.
- Fraude, perturbations de la chaîne d'approvisionnement.
- Frais liés aux enquêtes judiciaires et restauration des systèmes et serveurs piratés.
- Atteinte à la réputation.

Exemples d'attaques

Au cours des dernières années, 4 grandes institutions de santé ont été piratées en France avec des fuites importantes de données personnelles :

- Novembre 2019, Centre hospitalier universitaire de Rouen,
- Février 2021, Hôpital de Dax,
- Septembre 2021, Centre informatique de l'Assistance Publique-Hôpitaux de Paris (AP-HP),
- Août 2022, Hôpital de Corbeil-Essonnes.

Cyberattaques dans la région

HÔPITAL de la Rochelle
SEMIS à Saintes
FOUNTAINE PAJOT à la Rochelle

Évolution 2020-2021 du nombre d'attaques informatiques (1/2)

- Recherche / Bureaux d’études +75 %
- Services informatiques / Internet +67 %
- Communication +51 %
- Santé +71 %
- Gouvernement / Militaire +47%

(1) statistiques globales sur les risques assurés

Évolution 2020-2021 du nombre d'attaques informatiques (2/2)

- Europe + 68%
- Amérique du Nord + 61%
- Amérique Latine + 0 %
- Asie Pacifique + 25%
- Afrique +13%

Cartographie des risques pour les entreprises en 2023

Source : baromètre d'Allianz

- Le risque cyber, à la 8ème place en 2014 se retrouve au 1er rang en 2023.

- Le coût moyen d'une violation de données qui était de 4,35 millions USD en **2022**, devrait dépasser les 5 millions USD en **2023**.

Évènements marquants en 2022 (1/2)

DATE	PIRATE	CIBLE	LIEU	CONSÉQUENCES
Mars	LAPSUS £	Microsoft, Samsung, Ubisoft	Monde	Vol de données sensibles et tentatives d'extorsion
Mars	Lazarus et APT38	Joueurs en ligne	Corée du Nord	Piratage du jeu en ligne Axie infinity
Mars	inconnu	Shields Health Care Group	USA	Violation des données de 2 millions de patients
Août	inconnu	UK National Health Service (NHS)	Royaume-Uni	Attaque avec demande de rançon

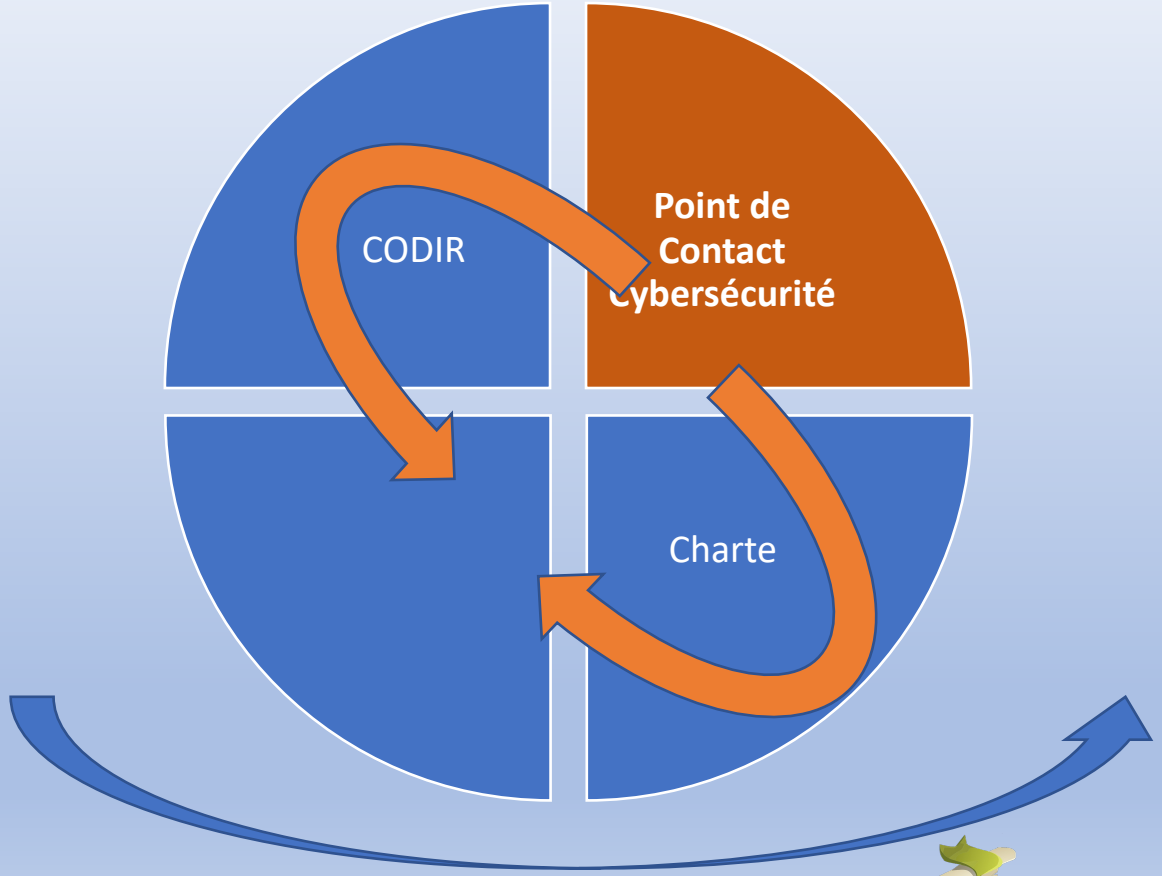
Évènements marquants en 2022 (2/2)

DATE	PIRATE	CIBLE	LIEU	CONSÉQUENCES
Août	inconnu	**Ernergoatom opérateur nucléaire ukrainien**	Ukraine	Cyberattaque (russe?)
Août	inconnu	Centre Hospitalier de Corbeil-Essonnes	France	Demande de rançon
Septembre	**Hacker âgé de 18 ans**	UBER	USA	Piratage d'une grande partie des infrastructures
Octobre	inconnu	Lloyd's de Londres	GB	Activité inhabituelle sur le réseau
Octobre	inconnu	Medibank assureur santé australien	Australie	Vol de données personnelles de clients

Sensibilisez vos collaborateurs

- Menez des **actions de sensibilisation** avec **l'appui** de **votre comité de direction** (diffusion des bonnes pratiques, de documentation, campagnes de prévention, etc.).
- **Formez** vos **collaborateurs** en leur proposant des **formations dédiées**.
- Établissez un **code de bonne conduite** et assurez-vous qu'il est **bien appliqué.**
- Désignez parmi vos collaborateurs un **point de contact cybersécurité** qui sera **l'ambassadeur** des **bonnes pratiques** au sein de votre **entreprise**.
- **Valorisez** vos **collaborateurs**, faites-en les **acteurs** de votre **cyberdéfense**

Sensibilisez vos collaborateurs



Gestion des mots de passe

- Un **mot de passe** doit être **individuel** et rester **confidentiel.**
- Pour être efficace, un **mot de passe** doit être **long et complexe.**
- Créer un **mot de passe différent** pour **chaque usage.**
- Utilisez des **gestionnaires** de mots de passe.
- Un **mot de passe** doit être **changé régulièrement**

Évitez les comportements à risque

- N’ouvrez **jamais** une **pièce jointe** suspecte ou **provenant d’un expéditeur inconnu.**
- Ne **connectez** jamais une **clé USB** en apparence **abandonnée** : **elle est là pour vous tenter !**
- Avant de cliquer sur un lien, passez votre souris dessus pour apercevoir le nom de domaine.
- Ne vous connectez **jamais** à un **réseau WIFI public.**

Mettez à jour vos appareils, vos logiciels et vos antivirus

- Vérifiez régulièrement que vous utilisez bien les dernières versions disponibles.
- Lorsque votre système d'exploitation est à jour, activez les mises à jour automatiques si votre éditeur le permet.
- Installez uniquement les mises à jour proposées par votre éditeur ou fournisseur, provenant d'une source officielle fiable.
- Privilégiez **deux** éditeurs **d'antivirus différents** : un pour vos **serveurs** et un autre pour vos **postes de travail.**

Sauvegardez... (1/2)

- Réalisez des sauvegardes régulières.
- Choisissez une solution de sauvegarde adaptée à vos besoins.
- **Planifiez vos sauvegardes**. La plupart des solutions de sauvegarde intègrent une fonctionnalité permettant de planifier la sauvegarde à échéance régulière.
- **Déconnectez** votre support de sauvegarde de votre système d'information.

Sauvegardez... (2/2)

- Protégez vos sauvegardes.
- **Conservez vos sauvegardes sur un support extérieur à votre outil informatique.**
- Assurez-vous régulièrement que vos **sauvegardes sont conformes** et **exploitables** en faisant des **tests de restauration.**

Mettez en place des garde-fous

- **Restreignez** les accès **Internet** uniquement aux **sites nécessaires** à vos collaborateurs.
- Un ordinateur ne doit **pas être partagé.**
- Un ordinateur doit être **personnel** et **stocké sous clé**.
- Passez **systématiquement** à l'antivirus **toute clé USB** que vous connectez.
- **Bloquez** les **ports USB** de vos appareils **si** vous n'en avez **pas l'utilité.**

Quelle plage choisiriez-vous ?

Et quel système d'exploitation ?