MINISTÈRE
DE LA CULTURE

Liberté
Égalité
Fraternité

STRUCTURES LABELLISÉES
SENSIBILISATION AU RISQUE CYBER

Sommaire

1. Etat de la menace Cybersécurité (10 mn)
2. Retour d'expérience du CND Normandie-Rouen suite à incident cyber (30 mn)
3. Mesures curatives et préventives (20 mn)

1. Etat de la menace

Caractéristiques d'une crise Cyber

- **Point d'entrée Cyber, avec impact sur les métiers**

- **Crise de nature technologique centrée sur l'expertise**

Cela implique :

  - d'être vigilant pour rendre compréhensible les messages que l'on souhaite passer (vers les décideurs, personnels, externe)
  - d'avoir des compétences permettant de comprendre les impacts de l'attaque, les modalités de l'attaquant, et d'identifier les mesures de remédiation en lien avec le métier

- **Double temporalité (effets immédiats et remédiation longue) :**

Etre en capacité de s'inscrire dans une crise qui dure plusieurs jours, semaines, mois.

- **Adaptation – une menace intelligente qui s'adapte**

Bien maitriser sa communication

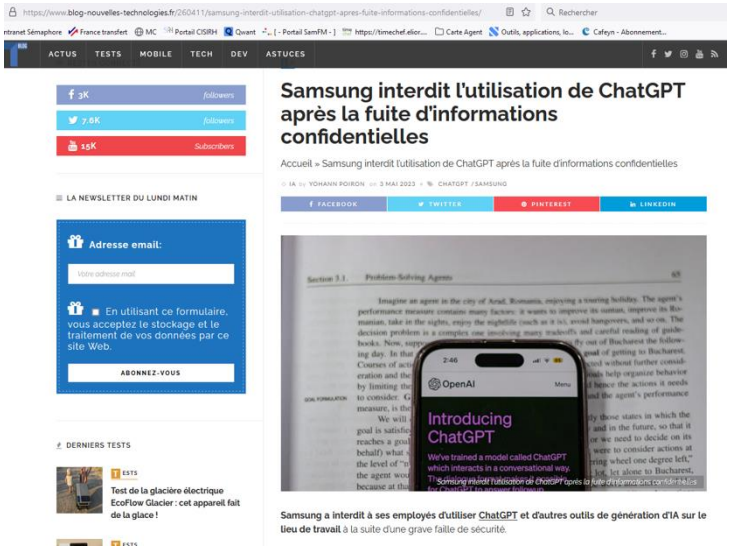
- **Propagation – Absence d'unicité de lieu**

Difficulté de circonscrire un incident en début de crise au moins

- **Le problème de l'attribution**

Le fait de la difficulté de l'attribution contribue à semer le doute sur la motivation de l'attaquant. Est-ce un rançongiciel uniquement ou le pirate a-t-il aussi volé des données, ou déposé de manière discrète une porte dérobée ?

MINISTÈRE
DE LA CULTURE
Liberté
Égalité
Fraternité



ACTUS TESTS MOBILE TECH DEV ASTUCES

3K followers
7.6K followers
15K Subscribers

LA NEWSLETTER DU LUNDI MATIN

Adresse email:

En utilisant ce formulaire, vous acceptez le stockage et le traitement de vos données par ce site Web.

ABONNEZ-VOUS

DERNIERS TESTS

Test de la glacière électrique EcoFlow Glacier : cet appareil fait de la glace !

Samsung interdit l'utilisation de ChatGPT après la fuite d'informations confidentielles

Accueil » Samsung interdit l'utilisation de ChatGPT après la fuite d'informations confidentielles

IA by YOHANN POIRON on 3 MAI 2023 CHATGPT / SAMSUNG

FACEBOOK TWITTER PINTEREST LINKEDIN

Samsung a interdit à ses employés d'utiliser ChatGPT et d'autres outils de génération d'IA sur le lieu de travail à la suite d'une grave faille de sécurité.

Ingérence russe : des députés britanniques demandent une enquête sur la campagne du Brexit

Le Royaume-Uni a publié mardi un rapport parlementaire sur de possibles ingérences russes, notamment dans la campagne sur le référendum de 2016 ayant abouti au Brexit, dans un contexte de relations glaciales entre Londres et Moscou. Le Kremlin a immédiatement démenti ces allégations.

Publié le : 21/07/2020 - 12:36 Modifié le : 21/07/2020 - 13:00

Suite à votre choix :
- Les articles ne peuvent plus afficher les contenus externes comme les vidéos YouTube, citations Twitter ou photos Instagram.
- Des cookies non liés à vos données personnelles seront créés pour permettre au site de fonctionner.
- Des publicités de moindre qualité risquent d'apparaître.

Le Monde Politique Assemblée nationale Gouvernement Borne Newsletter Politique @. Mincult

PROJET PEGASUS → L'essentiel

PROJET PEGASUS • POLITIQUE

« Projet Pegasus » : un téléphone portable d'Emmanuel Macron dans le viseur du Maroc

Par Damien Leloup et Martin Untersinger

Publié le 20 juillet 2021 à 17h59, modifié le 04 novembre 2022 à 11h15

Lecture 8 min.

Etat de la menace

Contexte Cyber :

Evolution des pratiques : numérique devenu indispensable → Forte dépendance

Les tensions internationales → recrudescence d'attaque Cyber.

JOP → ⚠

Incidents récents sur notre périmètre :

- Dénis de service à répétition (plusieurs par mois ciblant le ministère, EP)
- Compromissions de machines
- Compromissions de bal
- (04/2023) Incendie chez l'hébergeur d'un EP (31 sites HS)
- Rançongiciels (exemple d'un EP – Billetterie HS, coût estimé à 500k€)
- etc.

Recrudescence d'attaques Cyber :

- Rançongiciels
- Attaques étatiques (ingérence, espionnage, …)
- Dénis de service par activistes
- Défiguration des sites
- Sabotage par code malveillant
- Vols de données

2. Retour d’expérience suite à incident cyber

Intervention du CND Normandie-Rouen

3. Mesures curatives et préventives

Quelques règles de sécurité pour éviter une compromission :

👉 Maintenir à jour les logiciels, appliquer les patchs de sécurité des éditeurs sur les systèmes et les applications

👉 Utiliser et maintenir à jour les logiciels antivirus

👉 Limiter les droits des utilisateurs et des administrateurs au strict nécessaire

👉 Maîtriser les accès Internet

👉 Utiliser des mots de passe sécurisés, différents pour les usages professionnels et personnels

👉 Cloisonner le système d'information

👉 Sauvegarder les données et disposer de copies déconnectées du réseau

👉 Sensibiliser le personnel, notamment aux bonnes pratiques sur la messagerie.

👉 Suivre les alertes et les avis de sécurité émis par le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) : *www.cert.ssi.gouv.fr*

MINISTÈRE
DE LA CULTURE
Liberté
Égalité
Fraternité

Quelques conseils en cas d'incident cyber, voire de crise :

Gestion technique d'un incident :

👉 Déconnecter immédiatement la ou les machines concernées du réseau et ne les éteignez pas.

👉 S'appuyer sur une société de sécurité informatique pour mener des actions de confinement/ investigation/ remédiation

Pour diagnostiquer l'incident :

👉 Consulter le site Cybermalveillance.gouv.fr afin d'être conseillé sur la résolution de l'incident et d'obtenir un diagnostic : https://www.cybermalveillance.gouv.fr

Gestion de crise :

👉 Activer une cellule de crise cybersécurité, présidée par le responsable du service ou l'organisme.

👉 Mettre en œuvre les mesures prévues pour la continuité d'activité

👉 Anticiper sur une communication de crise.

👉 Déposer plainte auprès des services de police ou de gendarmerie, ou auprès du procureur de la République du tribunal judiciaire

MINISTÈRE
DE LA CULTURE
Liberté
Égalité
Fraternité

Pour aller plus loin :

⚠ En cas de violation de données à caractère personnel : Notifier cette compromission à la CNIL via le lien : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

⚠ En cas de rançongiciel : **Ne jamais payer la rançon**, le paiement ne garantit en rien le déchiffrement de vos données.

Quelques contacts :

CERT-FR ANSSI	cert@ssi.gouv.fr	Pour demander une assistance en cas d'incident de cybersécurité
CSIRT Culture	csirt@culture.gouv.fr	Pour informer le ministère de la Culture de l'incident

MINISTÈRE
DE LA CULTURE
Liberté
Égalité
Fraternité

Merci pour votre écoute !