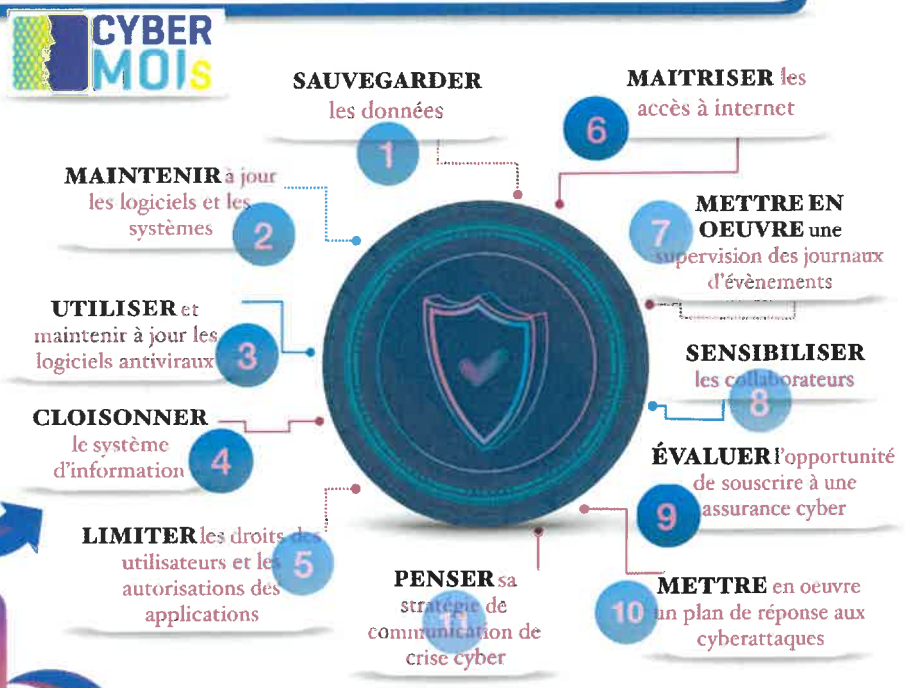
GROUPEMENT DE GENDARMERIE DES ALPES-MARITIMES

BULLETIN D'ALERTE ET DE PRÉVENTION SUR LES CYBERMENACES

La gendarmerie des Alpes-Maritimes communique et alerte les usagers des réseaux des technologies de l'information et de la communication, professionnels ou particuliers sur les cybermenaces. Un **rançongiciel** - *ransomware* en anglais - est un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon. Les rançongiciels figurent au catalogue des outils auxquels ont recours les cybercriminels motivés par l'appât du gain.

Autour de ce chantage numérique qui peut impacter particuliers comme professionnels, la gendarmerie nationale participe au « **CyberMoi/s** » européen de la cybersécurité 2020, coordonné par l'Agence Nationale de la Sécurité des Systèmes Informatiques (ANSSI)[1], et vous conseille sur : comment **RÉDUIRE LE RISQUE D'ATTAQUE** et comment **RÉAGIR EN CAS D'ATTAQUE**

CYBERMENACES Rançongiciels Prévention



CYBERMENACES Rançongiciels Réagir en cas d'attaque

1 – ADOPTER LES BONS RÉFLEXES

- Ouvrir une main courante permettant de tracer les actions et les évènements liés à l'incident
- Déconnecter au plus tôt vos supports de sauvegardes après vous être assurés qu'ils ne sont pas infectés
- Isoler les équipements infectées les déconnectant du réseau
- Laisser éteints les équipements non démarrés
- Conserver les données chiffrées
- Piloter la gestion de crise cyber
- Établir les stratégies de communication interne comme externe et les éléments à fournir en vue de la judiciarisation (*dépôt de plainte) ou de notification réglementaire (avis à la CNIL)

2 – TROUVER L'ASSISTANCE TECHNIQUE

- Le cas échéant, faire appel à des prestataires spécialisés dans la réponse aux incidents de sécurité
- L'État a mis en place la plateforme **cybermalveillance.gouv.fr** qui permet d'entrer en contact avec des prestataires de proximité
- En liaison avec le prestataire, s'assurer lorsque c'est possible de la préservation des éléments de preuves techniques (emails, pièces jointes, historique de navigation) permettant le travail judiciaire sur le vecteur d'attaque et la catégorisation de la charge malveillante

3 – COMMUNIQUER AU JUSTE NIVEAU

- Communication interne adaptée : rassurer les collaborateurs et leur rappeler qu'ils sont soumis à une clause de confidentialité
- Communication externe adaptée : centraliser la communication vers l'extérieur : être transparent vis-à-vis des entités institutionnelles

4 – NE PAS PAYER LA RANÇON

- Son paiement ne garantit pas l'obtention d'un moyen de déchiffrement
- Cela incite les cybercriminels à poursuivre leurs activités et entretient donc ce système frauduleux
- Le paiement de la rançon n'empêchera pas votre entité d'être à nouveau la cible de cybercriminels

5 – RESTAURER LES SYSTÈMES DEPUIS DES SOURCES SAINES

- Réinstaller le système sur un support connu et de restaurer les données depuis les sauvegardes effectuées, de préférence, antérieures à la date de compromission du système
- Vérifier que les données restaurées ne sont pas infectées par le rançongiciel

6 – DÉPOSER PLAINTE

- Déposer plainte auprès des services de police ou de gendarmerie
- La BRIGADE NUMÉRIQUE répond aux besoins et aux attentes des usagers. Ses missions : accueillir, orienter, informer et guider les internautes 24h/24h. gendarmerie.interieur.gouv.fr

[1] https://www.ssi.gouv.fr