LA SECURITE INFORMATIQUE : L'AFFAIRE DE TOUS.

Nos obligations : La continuité d'un service public visant à servir l'intérêt général, et la protection des ressources

Les impacts d'une attaque

Disponibilité (interruption du service public), Intégrité (destruction de données ou de systèmes), Confidentialité des données (divulgation d'information, atteinte à la réputation)

Les types d'attaques

- Hacking : malveillance délibérée (virus, vol de données, interruption de service)
- cybercriminalité : motivation pécuniaire (extorsion de fond, rançongiciel, hameçonnage)
- cyber-influence : atteinte à la réputation, prise de pouvoir, déstabilisation états.

Les portes d'entrée

- Les mails (pièces jointes infectées, lien vers des sites internet détournés)
- L'usurpation d'identité (vol des identifiants et mots de passe, appels avec usurpation)
- Les clés USB (virus, malwares)
- Les téléphones
- Les failles de filtrage sur les réseaux internet
- Les obsolescences des systèmes
- La tendance : les objets connectés.

En quoi suis-je concerné·e ?

Les cybercriminels peuvent chercher à s'introduire dans les systèmes en abusant les personnes. L'éducation de chacun à la sécurité informatique est donc un des leviers de prévention et de lutte pour diminuer les risques :

➔ **Chacun peut agir à son niveau**

24, bd Paul Vaillant Couturier – 94200 IVRY SUR SEINE
Tél. 01.43.90.25.30 - Email : direction@siim94.net

PROTEGEZ-VOUS : les bonnes pratiques

Votre service informatique veille à la protection de vos applications, de votre réseau et de votre PC en appliquant les règles de bonnes pratiques de sécurité. A votre niveau, vous pouvez agir dans votre activité quotidienne :

Les mots de passe :

- Utilisez des mots de passe tous différents et complexes (au minimum 8 lettres avec majuscules, minuscules, chiffres, caractères spéciaux).
- N'écrivez aucun mot de passe, mémorisez-les et stockez-les dans une application spécifique (Keypass par exemple).

Gestion des mails :

- Méfiez vous des factures qui arrivent en pièces jointes sous Word.
- Contrôlez l'identité de expéditeurs avant d'ouvrir des pièces jointes.
- N'ouvrez jamais les pièces jointes dont les extension sont : *.vbs, *.hta, *.pif, *.bat, *.com, *.exe, *.ink sans être certains de l'innocuité de la pièce (prenez attache auprès de votre service infomratique).
- N'envoyez jamais de données sensibles non chiffrée par mail : Utilisez des sites spéciaux de transferts de données.
- Ne consultez pas vos messages personnels sur votre poste professionnel.

demandes urgentes des autorités :

- N'accédez à aucune demande d'accès à une application ou déblocage de fond sans vérifier l'identité de l'autorité.

Internet :

- Attention : les données sur Internet circulent « en clair »
- Sur votre lieu de travail, Limitez votre navigation aux sites professionnels sécurisés

Nomadisme :

- Ne stockez pas de données professionnelles sur un PC portable (réduire les risques de vol de données), si vous le devez : chiffrez-les.
- Sur le PC professionnel, ne connectez ni clés USB, ni téléphone.
- N'installez aucune application sur PC sans approbation de votre DSI.

24, bd Paul Vaillant Couturier – 94200 IVRY SUR SEINE
Tél. 01.43.90.25.30 - Email : direction@siim94.net

SIIM94
Partageons la transformation numérique

Tous ensemble pour sécuriser notre outil informatique

Pour votre matériel personnel

Pour vos messageries :

- ne suivez jamais les liens non sollicités dans les mails : les banques et institutions n'envoient jamais de pièces jointes ou de liens, connectez-vous à leur site par un lien officiel.

pour vos PC

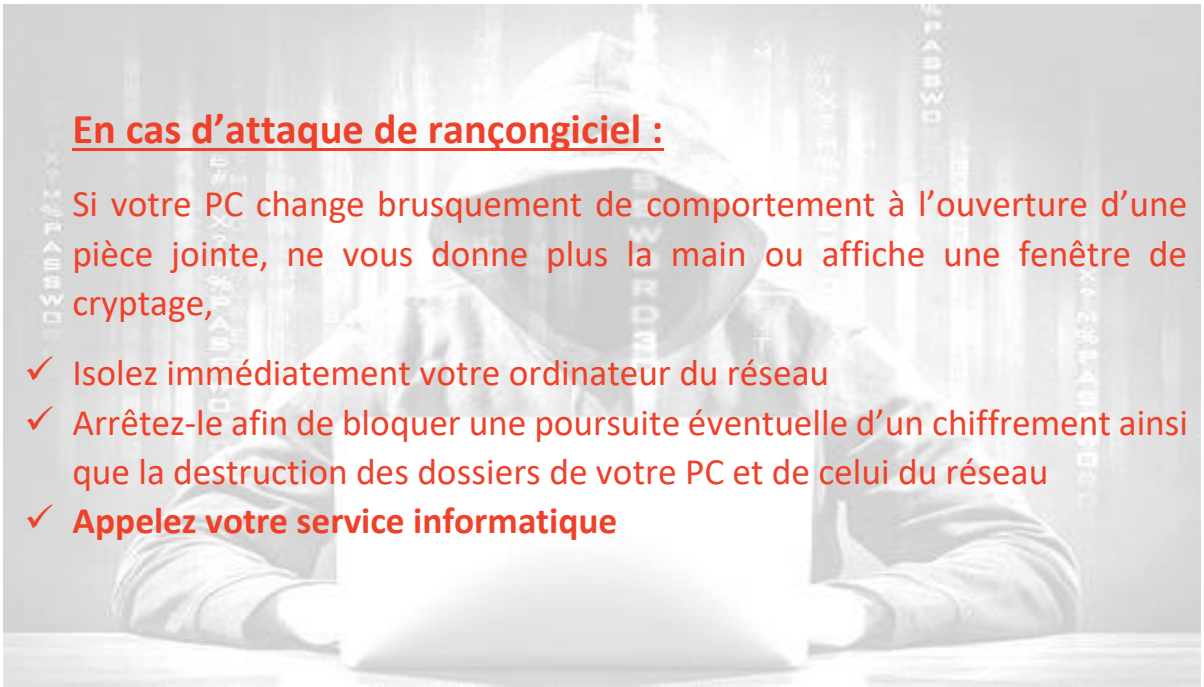
- Soyez vigilants à mettre à jour vos systèmes et surtout vos antivrus.
- Ne téléchargez aucune application non vérifiée.

Pour la sécurité de vos données

- Activez les options de chiffrage de données.
- Sauvegarder régulièrement vos données sur des supports externes non connectés.

le téléphone

- votre téléphone est comme un PC --> protégez le
- ne suivez jamais les lien dans les sms



En cas d'attaque de rançongiciel :

Si votre PC change brusquement de comportement à l'ouverture d'une pièce jointe, ne vous donne plus la main ou affiche une fenêtre de cryptage,

- ✓ Isolez immédiatement votre ordinateur du réseau
- ✓ Arrêtez-le afin de bloquer une poursuite éventuelle d'un chiffrement ainsi que la destruction des dossiers de votre PC et de celui du réseau
- ✓ **Appelez votre service informatique**

24, bd Paul Vaillant Couturier – 94200 IVRY SUR SEINE
Tél. 01.43.90.25.30 - Email : direction@siim94.net

Pour approfondir

Qui contacter ?

- En interne : votre DSI, votre DPO, votre hiérarchie, le SIIM94
    - En externe : La CNIL, le site www.cybermalveillance.gouv.fr, L'ANSII

Porter plainte :

- Signalez une arnaque au 0 811 02 02 17 ou sur le site www.internet-signalement.gouv.fr
- Consulter le site de l'agence nationale de sécurité des systèmes d'information (ANSSI) www.ssi.gouv.fr
- Consulter le site du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques CERT-FR : www.cert.ssi.gouv.fr
- Déposez plainte si vous le souhaitez auprès des services de police ou de gendarmerie ou faite une déclaration directement sur le site de pré-plainte en ligne www.pre-plainte-en-ligne.gouv.fr

Quelques chiffres complémentaires.

En 2018 et en France, huit entreprises sur dix disent avoir été touchées par une cyberattaque au moins une fois, selon le baromètre du Club des experts de la sécurité de l'information et du numérique (Cesin).

Les cyberattaques coûteraient quelque 400 milliards d'euros par an à l'économie mondiale, estime la Commission européenne, qui évoque un chiffre multiplié par cinq entre 2013 et 2017

2019 aura été, selon les chercheurs en cybersécurité de Kaspersky, *« l'année des attaques de ransomware contre les municipalités. »* : 174 villes et 3 000 administrations municipales ont été ciblées par un rançongiciel (augmentation de plus de 60 % par rapport à 2018) :

- Juin 2017 : rançongiciel Notpetya : 250 m€ chez Saint-Gobain, arrêt de l'usine Renault de Maubeuge pendant 4 jours,
- 2018 : ministère des affaires étrangères (vol de données de 500 000 personnes),
- 2019 : ransomware : ALTRAN, aéroport Marseille (vol de données bancaires), Fleury Michon (arrêt des usines sur 4 jours), Baltimore (28 m$), AIRBUS, groupe M6, GOSPORT, ENDERED),
- 10/08 : rançongiciel sur 120 hôpitaux,
- 12/10 : rançongiciel Grand cognac,
- 15/11 : rançongiciel CHU de Rouen,
- 01/2020 : rançongiciel Bouygues construction, rançongiciel sur un Datacenter du jura hébergeant les données de 50 entreprises, l'entreprise met plus d'un mois à rétablir l'informatique,
- 02/2020 : DECATHLON : vol : 9 Go, 123 millions d'enregistrement sur les clients et personnels,
- 02/2020 : la région Grand Est victime d'un malware : 7500 agents bloqués pendant 8 jours.