Contact : nouvelle-aquitaine@ssi.gouv.fr 16/01/2023

Quelques conseils en matière de cybersécurité pour les élèves du BTS SNIR du lycée Alfred Kastler

Les organisations (écoles, collectivités, associations etc.), toutes tailles confondues, sont aujourd'hui de plus en plus la cible d'attaques cyber, notamment via des rançongiciels. Ces attaques sont indifférenciées et touchent tout type d'organisation (personne n'est à l'abri). Pour mieux connaitre l'état de la menace et quelques scénarios constatés lire : https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-002/.

Plusieurs éléments d'actualités récentes, dont certaines en Nouvelle-Aquitaine, corroborent cette analyse :

- https://www.brut.media/fr/news/victime-d-une-cyberattaque-les-services-de-la-ville-d-angers-paralyses-98ef8f15-267b-45a9-8413-10ca228d72c5
- https://www.sudouest.fr/landes/cyberattaque-a-l-hopital-de-dax-notre-dossier-8379691.php
- https://www.lunion.fr/id234241/article/2021-02-18/arnaque-au-faux-president-le-cder-escroque-de-presque-15-millions-deuros
- https://www.millenium.org/news/376575.html
- https://www.tf1info.fr/societe/covid-19-confinement-ecole-a-la-maison-cyberattaque-contre-la-plateforme-du-cned-l-oeuvre-de-petits-malins-pour-faire-l-ecole-buissonniere-2182897.html
- https://www.lemondeinformatique.fr/actualites/lire-les-stations-d-assainissement-d-oloron-sainte-marie-visees-par-un-ransomware-maj-84347.html
- https://www.lemondeinformatique.fr/actualites/lire-faille-log4j-un-cauchemar-pour-des-millions-d-applications-java-85099.html
- https://www.lefigaro.fr/flash-eco/le-groupe-d-ingenierie-akka-frappe-par-une-attaque-au-rancongiciel-20220527
- https://www.zdnet.fr/actualites/orange-cyberdefense-victime-d-une-fuite-de-donnees-39946760.htm

Afin de se protéger de ce type d'attaque et sécuriser davantage les informations stratégiques et critiques des entités (finances, comptabilité, systèmes de production, propriété intellectuelle, données clients, administratifs, RH…), des règles de base d'hygiène informatique doivent être adoptées pour réduire les risques attaques. Pour ce faire, appliquer les 12 bonnes pratiques de l'ANSSI :
1) Choisir avec soin ses mots de passe 2) Mettre à jour régulièrement vos logiciels 3) Bien connaître ses utilisateurs et ses prestataires 4) Effectuer des sauvegardes régulières 5) Sécuriser l'accès Wi-Fi 6) Être aussi prudent avec son ordiphone (smartphone) ou sa tablette qu'avec son ordinateur 7) Protéger ses données lors de ses déplacements 8) Être prudent lors de l'utilisation de sa messagerie 9) Télécharger ses programmes sur les sites officiels des éditeurs 10) Être vigilant lors d'un paiement sur Internet 11) Séparer les usages personnels des usages professionnels 12) Prendre soin de ses informations personnelles, professionnelles et de son identité numérique.
A contrario, ci-après une vidéo présentant des pratiques à proscrire : https://youtu.be/I5jZWXbFP5c

Un grand nombre d'attaques proviennent des mauvais usages ou de méconnaissances des risques de la part des utilisateurs, il est donc recommandé de **mener et de poursuivre régulièrement des actions de sensibilisation**, et ce, auprès de tous les métiers et tous les échelons hiérarchiques. Pour cela, des ressources sont d'ores et déjà accessibles gratuitement pour vous aider de ces actions :

- Guide des 12 bonnes pratiques citées précédemment : https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf
- Kit de sensibilisation : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation
- MOOC de l'ANSSI sur la cybersécurité (modules à la carte) : https://secnumacademie.gouv.fr/

Il peut être également intéressant **d'établir un 1er diagnostic cyber** idéalement via un tiers de confiance en s'appuyant, selon son niveau de maturité, sur les différents guides de bonnes pratiques ANSSI :

1. La cybersécurité pour les TPE PME : https://www.ssi.gouv.fr/uploads/2021/02/anssi-guide-tpe_pme.pdf
2. Attaque par rançongiciels tous concernés, comment les anticiper et réagir en cas d'incident : https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf
3. Guide d'hygiène informatique : https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

Il ne faut pas oublier que devoir remédier à un incident dans l'urgence peut s'avérer bien plus coûteux que la prévention. Cependant, si l'incident arrive comment réagir ? Les premières actions techniques proposées, dans les guides ci-après, permettent de réduire les pertes liées à une telle attaque, si elles sont mises en place rapidement :

- https://www.ssi.gouv.fr/uploads/2022/02/20220311_cyberattaque-comment-reagir.pdf
- https://www.ssi.gouv.fr/guide/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique/
- https://www.ssi.gouv.fr/guide/anticiper-et-gerer-sa-communication-de-crise-cyber/
- Nous vous incitons également à vous exercer à la gestion d'un incident cyber : https://www.ssi.gouv.fr/administration/guide/organiser-un-exercice-de-gestion-de-crise-cyber/

Par ailleurs, il convient de signaler votre incident auprès du site https://www.cybermalveillance.gouv.fr/ qui vous indiquera les prestataires référencés ou labellisés *Expert Cyber* susceptibles d'intervenir auprès des PME pour remédier aux attaques et vous mettra en lien avec les services d'enquête (Police et/ou Gendarmerie Nationale).

Si nécessaire les adresses mails des référents Cyber des services judiciaires en région Nouvelle-Aquitaine :

- Gendarmerie : securite-economique-nouvelleaquitaine@gendarmerie.gouv.fr
- Police : cybermenaces-bordeaux@interieur.gouv.fr

La cybersécurité est une filière d'avenir et passionnante, elle manque aujourd'hui grandement de ressources, environ 6000 postes (hors région d'Ile de France) reste actuellement non pourvues. Voici 2 études menées par l'observatoire des métiers qui développent davantage les métiers variés de la cybersécurité, les profils souhaités et les offres d'emploi ouvertes :

- https://www.ssi.gouv.fr/uploads/2021/10/anssi-panorama_metiers_cybersecurite-2020.pdf
- https://www.ssi.gouv.fr/guide/les-profils-de-la-cybersecurite/

Pour aller plus loin :

- Site du CERT-FR publiant régulièrement des alertes et bulletins de sécurité : https://www.cert.ssi.gouv.fr/
- Rapport des menaces associées aux tensions internationales actuelles : https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/
- Top 10 des vulnérabilités exploitées en 2021 : https://www.cert.ssi.gouv.fr/actualite/CERTFR-2022-ACT-008/
- Produits et solutions certifiés par l'ANSSI : https://www.ssi.gouv.fr/administration/visa-de-securite/