ENJEUX CYBER / RESSOURCES À DISPOSITION DES ORGANISATIONS

Aide-mémoire à vocation non exhaustive.

LA MENACE ET LES ENJEUX, EN QUELQUES MOTS

Sur les signalements d'attaques par rançongiciels reçus par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en 2024, 37% ont concerné des TPE/PME et 23% des collectivités.

Ces attaques sont souvent opportunistes : elles ne ciblent pas particulièrement l'entité touchée, mais « ratissent large » et se concentrent sur les plus vulnérables : nul besoin d'être une cible pour être une victime !

Lorsqu'une telle attaque frappe une collectivité, celle-ci ne doit pas gérer une crise cyber ou virtuelle, mais une crise bien réelle dont l'origine est cyber ! Concrètement, la cyberattaque peut bloquer tout ou partie des applications que la structure utilise pour fournir des services (parfois essentiels à la population) : gestion des clients, pilotage des services, etc. Ainsi, décider de maîtriser le risque cyber relève bien de la direction de l'organisation.

La bonne nouvelle, c'est que l' « hygiène informatique » offre déjà un premier niveau de protection face aux attaques opportunistes, et peut s'avérer raisonnable en matière de coûts de mise en œuvre et de maintenance. En tout cas bien moins coûteuse que les impacts financiers d'une attaque réussie, comme en témoignent plusieurs collectivités de la région.

COMMENCER À SE PROTÉGER AU BON NIVEAU (à retrouver sur Mes Services Cyber)

Mesures de cybersécurité

Le guide à destination des dirigeants de TPE/PME permet aux organisations avec peu ou pas de compétence en sécurité numérique de faire un état des lieux sur les fondamentaux, et peut aussi les aider à demander un point de situation à leur équipe ou prestataire informatique. La page 10 règles d'or préventives apporte aussi un complément utile.

Mon Aide Cyber

L'ANSSI met en place une démarche de diagnostic cyber de premier niveau, grâce à l'appui d'une communauté d'aidants et d'une plate-forme numérique Mon Aide Cyber. L'objectif est de proposer un diagnostic d'1H30 maximum, et un plan d'action cyber avec 6 mesures prioritaires à mettre en place dans les 6 prochains mois.

Gestion de crises d'origine cyber

Le guide dédié à la gestion d'une crise d'origine cyber, partage des conseils pratiques afin d'adapter les dispositifs de crise aux enjeux cyber et (bien) réagir en cas d'incident. Ce guide est complété de mesures dédiées à la communication de crise cyber. Enfin un guide supplémentaire accompagne l'organisation d'un exercice de gestion de crise cyber.
Il est également possible de préparer et tester un premier dispositif de gestion de crise cyber en participant le 18 septembre prochain à l'exercice REMPAR 25.

MOOC de formation à la sécurité numérique
Si une organisation veut former un référent cyber (par exemple pour gérer le prestataire informatique), le MOOC SecNumAcadémie propose d'atteindre un premier niveau de référence en une douzaine d'heures (modulable), avec délivrance d'une attestation de réussite.

D'AUTRES POINTEURS UTILES.

Portail Cybermalveillance.gouv.fr
https://cybermalveillance.gouv.fr est un portail riche en ressources directement exploitables (affiches, conseils) et permet de rechercher de l'aide en cas d'attaque. Administré par le groupement d'intérêt public ACYMA, il est particulièrement adapté aux TPE, collectivités et particuliers disposant d'un système d'information simple (quelques ordinateurs).

Sites et productions des forces de sécurité intérieure
Qu'il s'agisse du MOOC Sency-crise, de la brigade numérique, des portails THESEE ou PHAROS, la gendarmerie et la police nationales portent de nombreux services en ligne pour notamment réagir aux incidents de sécurité et aux escroqueries numériques.

Mon Espace NIS2
L'ANSSI anime un espace dédié à la directive NIS2, comprenant une présentation de la directive, un test en ligne permettant de savoir si la structure est concernée par l'application de la directive et une FAQ. Cet espace est mis à jour au fur et à mesure de l'évolution des travaux législatifs, réglementaires et opérationnels.

DES DISPOSITIFS D'ACCOMPAGNEMENT NATIONAUX ET LOCAUX

Cyber PME : BPI France propose aux PME Un programme d'accompagnement composé du diagnostic cybersécurité d'un appui-conseil dans la mise en œuvre du plan de sécurisation ainsi qu'une aide pour financer les dépenses afin de renforcer la sécurité de l'entreprise. Cyber PME (bpifrance.fr).

Association Urgence Cyber Région Sud
Issus du plan France Relance, les CSIRT régionaux sont des centres de réponse aux incidents cyber tournés vers les entités publiques et privées de taille intermédiaire, qui peuvent aussi les mettre en relation avec des prestataires de réponse à incident et des partenaires étatiques.
En Provence-Alpes-Côte d'Azur, le CSIRT régional est une association nommée Urgence Cyber Région Sud, joignable au 0 805 036 083.

Mon bouclier cyber : la Région Sud appuie les entreprises dans l'acquisition des solutions adaptées (protection réseau et sites web, veille de vulnérabilité, achat de matériel et autres mesures préventives de vos systèmes d'information). Le dispositif est en train d'être finalisé.
Mon bouclier cyber expert - Région Sud - Provence-Alpes-Côte-d'Azur (maregionsud.fr)

L'appui des CCI : les CCI de la région accompagnent également les organisations via les conseillers numériques et cyber en proposant diverses actions (ateliers de sensibilisation, webinaire spécialisés, formations cyber certifiantes, partages d'informations). Cybersécurité des TPE-PME : l'enjeu qui mobilise notre réseau CCI | CCI Provence Alpes Côte d'Azur (paca.cci.fr)