Fiche réflexe diagnostic prévention cyber

Objectifs et acteurs concernés:

Région :

- Partenaires de la région (ARS, Medef, CGPME, CCI),
- Entités sensibles du niveau régional,
  → Groupe Cyber des SR , réservistes numériques.

Groupements :

- mairies, élus → tous C-NTECH de la circonscription,
- entreprises liées à la crise : hôpitaux, cliniques, industries santé, collectivités territoriales,...
  → SOLC, NTECH (en présence au bureau ou confinés),
  → Les UE appuient la manœuvre en renseignant sur le maintien ou non de l'activité et sur la présence de personnes dans les locaux.

Actions à mener

Télétravail (s'ils y ont recours) :

- quels sont les moyens mis en place ;
- utilisation d'un VPN pour se connecter
- utilisation du protocole RDP (conseils sur la fermeture des ports)
- utilisation d'un FW pour les accès à l'infrastructure de l'entité
- quels outils de visioconférence (donner des conseils audio conf ovh, orange, visio : tixeo)
- charte utilisateur en télétravail (diffuser guide ANSSI nomadisme numérique)

SSI :

- l'entreprise dispose-t-elle d'une charte informatique
- montée de version des OS (serveur, PC, télétravail)
- présence d'un antivirus à jour, de stations blanches
- la salle des serveurs dispose-t-elle d'un contrôle d'accès
- des sauvegardes sont elles réalisées à intervalle régulier, sont elles stockées hors réseau
- cloisonnement des réseaux bureautiques et administrations, présence DMZ
- l'entreprise dispose-t-elle d'un site web, quel nom de domaine (à auditer)
- faire référence aux CVE et inviter le contact à vérifier ces vulnérabilités sur le site

Ingénierie sociale :

- les personnels ont ils été sensibilisés aux risques cyber,
- à la nécessité de ne pas communiquer d'informations sensibles sans avoir pris de précautions (rappel du numéro habituel du contact, validation hiérarchique, fiche réflexe)
- le service comptabilité est il sensibilisés aux risques de faux virements
- le service achat est il informé des nombreuses escroqueries de faux produits liés au Covid19

Prise de contact

Il est nécessaire de sensibiliser nos contacts sur le fait qu'ils ne doivent pas communiquer d'informations sensibles sans s'être assuré au préalable de l'identité de leurs interlocuteurs.
Ainsi, en fonction des ressources disponibles et de leur présence ou non dans les locaux de service :
De demander à l'entreprise de

- consulter le numéro de la gendarmerie sur https://lannuaire.service-public.fr
- d'appeler ce numéro pour ensuite établir une communication avec notre interlocuteur.

De charger le référent sûreté ou la cellule rens de prévenir les entités qu'elles seront contactées par la gendarmerie à des fins de prévention cyber.