MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Gendarmerie nationale

LA LETTRE CYBER *en région Grand Est*

été 2023

La thématique du mois
VACANCES ET CYBERSECURITE

? Les vacances estivales : un risque plus élevé ?

De manière générale, les vacances estivales voient régulièrement la diminution des effectifs, l'arrivée de nouvelles recrues, le recrutement de stagiaires pour combler les effectifs, la mise en place du télétravail sur les lieux de vacances etc.
Quels risques à titre professionnel ou personnel cela peut il engendrer ?

• Les risques !

Durant la période estivale, les risques dont vous avez connaissance sont toujours présents malgré votre absence (ransomware, phishing, vol de données etc.). Cette période ne doit donc pas être synonyme de relâchement en matière de cybersécurité. En effet ces risques peuvent être multipliés durant cette période. Retrouvez ci-dessous pourquoi ces risques sont multipliés et des conseils pour ne pas baisser votre vigilance.

• Éviter d'annoncer son départ sur les réseaux sociaux.

Dans notre lettre du mois de mai 2022, nous vous parlions de "social engineering", les réseaux sociaux sont la base de cette pratique. En effet quel que soit votre positionnement hiérarchique, divulguer vos dates d'absences sur les réseaux sociaux sont une information capitale pour un attaquant et ouvre la porte à une tentative d'escroquerie aux faux ordre de virement ou encore à se dire « tiens le chef du service informatique n'est pas là, c'est le moment d'envoyer un ransomware ». A titre personnel vous pourriez voir augmenter les tentatives de phishing sur vos boîtes mail pour vous proposer des locations proches de vos lieux de vacances par exemple. Portez également une attention aux réseaux de vos proches.

• Éteindre les appareils non utilisés.

Chaque appareil allumé et connecté au réseau est une porte d'entrée potentielle pour un attaquant. Une intrusion sur un Système d'Information (SI) passe le plus souvent par la compromission d'un équipement connecté non mis à jour. Il est donc important d'éteindre les machines inutilisées, d'autant plus que cela réduira la consommation d'énergie de l'entreprise, et de mettre à jour les systèmes et logiciels afin d'y apporter les derniers correctifs de sécurité.

Porter une attention particulière aux nouveaux arrivants.

Peu importe les raisons, vous pouvez voir arriver des stagiaires, des extras, ou de nouveaux personnels pendant la période estivale. Ces personnels sont naturellement moins sensibilisés à la cybersécurité au sein de votre entreprise. Il est important de porter une attention particulière à leur sensibilisation et de limiter les droits d'accès à leurs stricts besoins.

Déléguer le pouvoir décisionnaire.

Les vacances sont faites pour se relâcher, se détendre, il est donc important de déléguer le pouvoir décisionnaire à une personne de confiance qui restera sur place et restera concentrée sur le travail. Il est important que ce pouvoir soit exercé sur place afin de réagir rapidement en cas d'attaque, sensibiliser les personnels cités ci-dessus, mais également réduire le risque d'escroquerie aux faux ordres de virement pour lesquel les escrocs profitent de l'absence sur les lieux du pouvoir décisionnel habituel.

Prendre des précautions en cas de travail à distance.

Vous ne pouvez/voulez pas décrocher totalement pendant vos vacances ? Il vous faudra prendre quelques précautions.
N'utilisez pas d'appareils publics comme par exemple un ordinateur mis à disposition par votre hôtel, ceux ci ne sont pas sécurisés et vous n'êtes pas à l'abri qu'une tierce personne puisse récupérer vos données personnelles en utilisant l'appareil après vous.
Utilisez un VPN afin d'accéder à une connexion privée et sécurisée même si vous utilisez un WI-FI public. A défaut privilégiez une connexion via le partage de connexion de votre mobile plutôt que le wi-fi public qui pourrait permettre à des individus d'accéder à vos données personnelles.
De manière plus générale, ne mélanger pas vos appareils et vos connexions personnelles avec ceux de nature professionnelle.

Ne pas négliger les sauvegardes.

Le risque étant présent même si vous suivez tous ces conseils, réalisez une sauvegarde de vos données avant votre départ afin de pouvoir les récupérer en cas d'attaque.
Pour rappel : SAUVEGARDE 3-2-1 : 3 sauvegardes sur 2 supports différents, dont 1 support mis en sécurité dans un lieu géographique différent de votre lieu de travail.

+ D'INFOS

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR, DE L'OUTRE-MER ET DES COLLECTIVITÉS TERRITORIALES

internet-signalement.gouv.fr
Portail officiel de signalement des contenus illicites de l'Internet

PHAROS
PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

Région de gendarmerie du Grand Est

LA LETTRE CYBER en région Grand Est

Directeur de la publication : GCA S. OTTAVI
Responsable éditorial : COL A. SCHWEITZER
Rédacteurs : COL A. SCHWEITZER – ADJ M. KNOBLOCH
MAJ (ER) WOLFERT

Si vous souhaitez recevoir cette lettre, envoyez un mail à :
arnaud.schweitzer@gendarmerie.interieur.gouv.fr
mathieu.knobloch@gendarmerie.interieur.gouv.fr

Suivez l'actualité de la gendarmerie :