Prévenir et réagir à des cyberattaques par ransomware ou rançongiciel

Objectifs :

Comprendre les mécanismes utilisés par les cybercriminels et les failles de sécurité des TPE/PME qu'ils utilisent pour s'introduire sur le réseau informatique, se propager silencieusement et s'activer pour bloquer complètement le réseau informatique en demandant le paiement d'une rançon pour libérer le réseau informatique de la TPE/PME attaquée. Comprendre les gestes qui sauvent et comment réagir en cas d'attaque. Identifier les mesures de sécurité à appliquer dans la TPE/PME pour réduire l'exposition à une attaque.

Date, durée et lieu :

- Vendredi 2/12/2022 de 11h à 12h (1h), en distanciel synchrone via le logiciel Zoom (un lien de connexion vous sera envoyé 48h avant le début de la formation).

Prix : 0 € ; Attention, pour bénéficier de cette condition tarifaire vous devez être membre correspondant France Gestion.

Public concerné : Expert-comptable

Intervenant : Ely de Travieso, expert en sécurité IT, fondateur Guardea Cyberdefense

Pré-requis : Aucun

Moyens techniques et pédagogiques :

Techniques :
- Accès à une plateforme de visioconférence Zoom après envoi d'un lien et d'un code de connexion.

Pédagogiques :
- Exemples pratiques
- Exposés théoriques
- Mise à disposition en ligne de supports à la suite de la formation

Moyens avant la formation :

Un questionnaire d'analyse des besoins et d'évaluation des acquis avant la formation conçu par l'intervenant et validé par France Gestion sera transmis aux participants avant la formation afin que le formateur s'adapte à leurs attentes et leurs besoins.

Validation des acquis :

Validation des objectifs de la formation :
- Lors du déroulement de la formation :
  - Mises en situations, exercices et corrigés
  - Temps dédié à l'ancrage des savoirs (reformulation, questions/réponses)
- A l'issue de la formation :
  - Questions orales et réponses
  - Un point sera effectué sur ce qui a été étudié dans la journée afin de s'assurer que tout a bien été assimilé et de pouvoir reprendre certaines parties en fonction des retours des apprenants.

Qualité et évaluation de la formation :

- Un questionnaire d'évaluation sera remis à chaque participant à la fin de la formation pour mesurer le niveau de satisfaction au regard des attentes.

Accessibilité :

Si l'un des futurs participants de la formation (ou vous-même si vous êtes le participant) est en situation de handicap, et pour toute question y compris sur l'accessibilité, vous pouvez prendre contact avec notre référent handicap :
- Francis Villoz, responsable formation
- Francis.villoz@france-gestion.fr / Tél. 01 39 07 49 15 (ligne directe)

Du lundi au jeudi de 8h30 à 18h00 et le vendredi de 8h30 à 17h.
Nous vous répondrons sous 48 heures.

Programme :

- Introduction

Présentation de données publiques et des faits connus

1ère partie : Comment se déroule une attaque par ransomware ?

- La sélection de la cible
- L'intrusion sur le réseau informatique
- La propagation du virus
- L'activation du virus
- La demande de rançon

2ème partie : Comment réagir lors d'une attaque par ransomware ?

- D'un point de vue Informatique
- D'un point de vue RH
- D'un point de vue Juridique
- D'un point de vue commercial et marketing
- Du point de vue de la demande de rançon

3ème partie : Les bonnes pratiques pour mieux se protéger

- Le PCA PRA
- La sauvegarde sécurisée
- La cyber assurance