FICHE PRATIQUE

LUTTE CONTRE LA CYBERCRIMINALITÉ : QUELQUES BONNES PRATIQUES

www.cgalsace.fr

(votre contact : Steve ARBOGAST - s.arbogast@cgalsace.fr)
(Ligne directe : 03.88.45.65.51 - Standard : 03.88.45.60.20)

04/01/2024

I. SI VOTRE ENTREPRISE EST VICTIME D'UNE ATTAQUE (cryptovirus, rançongiciel, cheval de Troie …), il faut :

1. **Déconnecter immédiatement l'appareil infecté** d'internet et/ou du réseau, avec ou sans fil, de l'entreprise. Débrancher le disque dur externe, la clé USB …
2. **Ne pas éteindre l'appareil infecté,** car cette action efface les données de la mémoire vive. Or, ce contenu peut s'avérer très utile pour la remise en état du système, ainsi que pour la traque des auteurs de l'attaque.
3. **Ne pas payer** dans le cas où une rançon est demandée. Dans la majorité des cas, les victimes de l'attaque n'obtiennent pas la clé de décryptage.
4. **Contacter la gendarmerie ou la police immédiatement,** afin de débuter l'action judiciaire au plus vite, car les traces électroniques sont « fugaces ».

II. QUELQUES BONNES PRATIQUES PRÉVENTIVES EXISTENT ; il faut :

1. **Réaliser des sauvegardes régulières** sur un support non connecté, **et les vérifier périodiquement**.
2. **S'équiper d'un logiciel antivirus efficace** et veiller à ce qu'il soit toujours à jour.
3. **Effectuer les mises à jour des logiciels sans tarder**, notamment celles concernant Windows, mais aussi Microsoft, Java, Flash Player …, dès qu'elles vous sont notifiées (si vous ne recevez pas de notification, il faut revoir les paramètres de mise à jour du logiciel concerné).
4. **Afficher les extensions de fichiers** (.pdf, .exe, .jpeg …). L'option se trouve dans les paramètres Windows. Cela vous permettra de repérer plus facilement les fichiers suspects et, notamment, les doubles extensions.
5. **Ne pas ouvrir les emails douteux et encore moins les pièces jointes.** Avant d'ouvrir un email, il faut :
   - S'assurer de sa provenance, qui m'écrit ? Pourquoi ? (exemple : email de "Orange" avec une extension de l'adresse de l'expéditeur en ".be").
   - Vérifier l'orthographe et la grammaire (les emails frauduleux comportent souvent des fautes de français).
   - Vérifier l'extension de la pièce jointe, si elle existe.
   - Ne pas cliquer sur un lien contenu dans un email si vous n'êtes pas certain de sa provenance.
   - Analyser les pièces jointes à l'aide de votre logiciel antivirus. Pour cela, enregistrer la pièce sans l'ouvrir, puis « clic droit » et lancer l'analyse.
   - Répondre "NON" à une demande d'activation de macros lors de l'ouverture d'une pièce jointe.
6. **Ne jamais penser ou croire que la cybercriminalité ne concerne que les grandes entreprises ;** toutes les entreprises (même les TPE) peuvent faire l'objet, un jour, d'attaques informatiques de cybercriminels.