|  |  |
| --- | --- |
| Mission 1 – Solutionner les problèmes de réseau et sensibiliser le personnel aux rançongiciels  | Capture d’écran |
| Durée : 1 h  | *Homme avec un remplissage uniouDeux hommes avec un remplissage uni* | Source |

### Une image contenant ingénierie, acier, machine, bleu  Description générée automatiquementContexte professionnel

La société Berod a été créée  par Sylvie Berod qui en est PDG. Elle est un référent métier dans la collecte et la gestion des déchets. Elle propose une solution globale dans le domaine du recyclage qui s'étend de la récupération des ferrailles et métaux au tri et à la valorisation des déchets. Elle travaille essentiellement avec les entreprises, les collectivités locales et les particuliers.

Dans le cadre de son activité quotidienne plusieurs **incidents** vous sont soumis. Vous devez en identifier les causes.

**Travail à faire**

1. À partir du **documents 1**, identifiez des causes possibles des incidents évoqués dans le **document 2** et proposez des actions adaptées aux situations en complétant le **document 2**. (Le nombre de ligne affichée en face de la panne indique le nombre de causes à trouver).
2. Mme Berod souhaite sensibiliser le personnel aux attaques par rançongiciel (ou ransomware). À l’aide des informations transmises dans **le document 3** créez une fiche d’explication sur l’attitude à avoir pour prévenir les attaques par rançongiciel.

**Doc. 1  Schéma de l’organisation informatique de la société**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PC1****Mme Berot****Une image contenant Appareils électroniques, ordinateur, Périphérique de sortie, Appareil électronique  Description générée automatiquement** | **PC2****Attaché gestionUne image contenant Appareils électroniques, ordinateur, Périphérique de sortie, Appareil électronique  Description générée automatiquement** | **PC3****Resp. productionUne image contenant Appareils électroniques, ordinateur, Périphérique de sortie, Appareil électronique  Description générée automatiquement** | **PC4** **Comptable****Une image contenant Appareils électroniques, ordinateur, Périphérique de sortie, Appareil électronique  Description générée automatiquement** | **PC5** **Resp. commercialUne image contenant Appareils électroniques, ordinateur, Périphérique de sortie, Appareil électronique  Description générée automatiquement** | **Imprimante****Une image contenant équipement électronique, imprimante, intérieur  Description générée automatiquement** |
|  |  |  |  |  |  |
|  | **Serveur** **application/données** |  |  |  |  |
|  | **Une image contenant ordinateur  Description générée automatiquement** |  | **Une image contenant texte, routeur, équipement électronique  Description générée automatiquement** | **Commutateur****Routeur - Pare-feu** |  |
| **PC6****Commercial 1Une image contenant texte, équipement électronique, ordinateur  Description générée automatiquement** | **PC7****Commercial 2Une image contenant texte, équipement électronique, ordinateur  Description générée automatiquement** |  |  | **Internet**Internet, le Web, le W3C, quelle histoire ? | Votresite |  |

**Doc. 2  Problèmes rencontrés**

|  |  |  |
| --- | --- | --- |
| **Incidents rencontrés** | **Causes possibles** | **Solution proposées** |
| Aucun ordinateur du réseau ne parvient à se connecter à Internet |  |  |
|  |  |
| Le PC2 ne parvient pas à se connecter à Internet alors que les autres ordinateurs y arrivent. |  |  |
|  |  |
|  |  |
| Aucun ordinateur ne parvient à imprimer |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| Le responsable de production ne peut plus accéder aux données commerciales du PGI |  |  |
| Le PC 5 n’arrivent pas à imprimer alors que les autres ordinateurs y arrivent |  |  |
| Internet fonctionne mais aucun ordinateur n’accède aux données des applications de gestion du réseau |  |  |
|  |  |
|  |  |
| Lorsque l’ordinateur est allumé les noms des fichiers sont remplacés par code de type *1111111-AB11-4-DFG-FA12-038F3-2FE82D5.thor*  |  |  |

# Doc 3  Qu'est qu'un ransomware ou rançongiciel ?

Vous êtes de plus en plus nombreux à recevoir des **messages douteux**contenant des **pièces jointes** ou des **liens** vous invitant à les ouvrir.

Prenez garde ! Des **logiciels malveillants** appelés « rançongiciels » ou « ransomware » peuvent s’y cacher.

Leur but ? **Chiffrer (coder) vos données**pour vous les rendre moyennant une**rançon**. Bien entendu, la payer ne garantit pas la récupération de vos données. Mieux vaut donc vous prémunir contre ce type d’attaque.

## Comment se prémunir d'un ransomware ?

### Conseil n°1 : effectuez des sauvegardes régulières de vos données

C’est le meilleur moyen de couper l’herbe sous le pied aux pirates souhaitant prendre vos données en otage ! Déplacez physiquement la sauvegarde de votre réseau (hors réseau), placez-la en lieu sûr et veillez à ce qu’elle fonctionne !

### Conseil n°2 : n’ouvrez pas les messages dont la provenance ou la forme est douteuse

Ne vous laissez pas tromper par un simple logo ! Pire, le hacker peut avoir récupéré certaines de vos données préalablement (les noms de vos clients par exemple) et créer des adresses de messagerie ressemblant à un détail près à celle de vos interlocuteurs habituels.

Restez donc très vigilants ! Certains messages paraissent tout à fait authentiques.

Apprenez à identifier les courriels piégés (ou autres formes de récupération de vos données) sur le site de l'**Agence nationale de la sécurité des systèmes d'information (ANSSI)**[.](https://www.hack-academy.fr/techniques)

Vous avez un doute ? Contactez le messager par un autre biais.

### Conseil n°3 : apprenez à identifier les extensions douteuses des fichiers

Vous recevez habituellement des fichiers en .doc ou .mp4 (par exemple) et le fichier du message dont vous avez un doute se finit par un autre type d’extension ?

Ne les ouvrez surtout pas ! Voici quelques exemples d'extensions douteuses : .pif, .com, .bat ; .exe, .vbs, .lnk, ...

Attention à l’ouverture de pièces jointes de type .scr ou .cab. Comme le rappelle l’**Agence nationale de la sécurité des systèmes d'information (ANSSI)**, il s’agit des extensions de compression des campagnes CTB-Locker sévissant chez les particuliers, les PME ou les mairies.

### Conseil n° 4 : mettez à jour vos principaux outils

On  ne vous le dira jamais assez : traitement de texte, lecteur PDF, navigateur mais aussi antivirus… Veillez à mettre à jour vos logiciels !

Si possible, désactivez les macros des solutions de bureautique qui permettent d’effectuer des tâches de manière automatisée. Cette règle évitera en effet la propagation des rançongiciels via les vulnérabilités des applications.

Considérez que, d'une manière générale, les systèmes d'exploitation en fin de vie, qui ne sont plus mis à jour, donnent aux attaquants un moyen d'accès plus facile à vos systèmes.

### Conseil n° 5 : utilisez un compte « utilisateur » plutôt qu’un compte « administrateur »

Évitez de naviguer depuis un compte administrateur. L’administrateur d’un ordinateur dispose d’un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés de votre ordinateur.

Préférez l’utilisation d’un compte utilisateur. Cela ralentira, voire dissuadera le voleur dans ses actions malveillantes.

**Réponses**

1. **Mme Berod souhaite sensibiliser le personnel aux attaques par rançongiciel (ou ransomware). À l’aide des informations transmises dans le document 3 créez une fiche d’explication sur l’attitude à avoir pour prévenir les attaques par rançongiciel.**