COVATEAM
DIRECTION INFORMATIQUE EXTERNALISÉE

Offices de Tourisme 73
SAVOIE MONT BLANC

Quizz sécurité informatique OT Savoie

02/10/2023

QUIZZ INTERACTIF: www.kahoot.it

Bien entendu, ce qui va suivre est imaginaire…et n'arrive jamais…

Toute ressemblance avec
des personnes ou situations réelles
ne seraient que fortuites …

1 - Le danger de l’email

- Cas :

Le comptable de l'OT reçoit un email qui vient d'un fournisseur, avec un document au format PDF en pièce jointe qui porte un nom banal. Il l’ouvre et s’aperçoit que le document est vide.

Il supprime l’email et passe à autre chose.

- Evénement de sécurité :

A l’ouverture du PDF un logiciel malveillant furtif s’est installé et a courcircuité l’antivirus présent sur le poste.

En quelques jours il s’est diffusé sur la plupart des postes de l’entreprise et a envoyé des données sensibles sur internet pendant plusieurs mois avant d’être détecté.

➢ **Les attaques par email (phishing) comportent souvent un rançongiciel (ransomware) qui va crypter tous les ordinateurs et bloquer toute activité**.

1 - Le danger de l'email

Cher John Doe

Afin de supporter notre nouveau programme « travailler à domicile » les employés peuvent utiliser leur ordinateur personnel pour accéder aux applications de la société et aux données sur disques partagés, grâce à une connexion sécurisée. Les employés désireux de participer à ce programme doivent se connecter avec leur compte Windows a ce lien.

Sandra Smith
Responsable du programme affilié HUP / EMEA

1 - Le danger de l'email

- Question :

Quel est le pourcentage d'attaques réussies provenant des emails ?

- Réponse :

- 20%
- 40%
- 60%
- 80% et plus

Recommandation :

S'assurer d'avoir un service de messagerie électronique bien sécurisé (anti-spam/anti-virus) et une analyse des emails entrants humaine (adresse des émetteurs cohérents, contenus, liens avec adresses internet cohérentes).

2 - L’authentification des utilisateurs

- Cas rencontré:

Un jeune stagiaire utilise le même identifiant et mot de passe Windows qu’une personne de l’équipe : son maitre de stage.

Il accède à des documents sensibles (futur plan marketing du territoire par exemple) et se créé des « pass » pour accéder gratuitement à des services qui l’intéressent, sans laisser de trace.

- Evénement de sécurité :

Il récupère pour lui et réutilise des droits au détriment de l’OT. (Service payant par exemple Adobe)

Personne ne s’en est aperçu, mais le stagiaire récupère le futur plan marketing du territoire qui n’est pas encore public et le fourni en toute discrétion aux journaux locaux et lance ainsi des débats avant l’heure dans tout le territoire. Il est impossible de prouver que cette divulgation vient de lui.

2 - L’authentification des utilisateurs

- Question :

Quel est la longueur des mots de passes nécessaires pour protéger un accès sensible ?

- Réponse :

-8 caractères

-12 caractères

-**18 caractères**

-24 caractères.

- Recommandation :

La complexité des mots de passe nécessaires les rend difficiles à retenir, utiliser des « passes de phrase ». La puissance de calcul des ordinateurs aujourd’hui permettent de trouver un mot de passe en peu de temps,

Il faut donc utiliser un gestionnaire de mot de passe [1] ou des authentifications fortes à deux facteurs lors d’une connexion (mot de passe plus simple et application mobile).

Ne pas les stocker sur un post-it, Excel ou Word, sous le clavier, dans un carnet dans le tiroir du bureau

Ne partager jamais vos mots de passe et ne pas les utiliser pour plusieurs accès.

[1] Exemple Keepass : gestionnaire gratuit.

3 - Le smartphone ou Ordiphone

- Cas :

Le Manager utilise son smartphone professionnel avec quelques applications professionnelles et personnelles.

Il échange aussi des fichiers entre son ordinateur et son smartphone. Et utilise son smartphone pour certaines actions bancaire de l'OT sur lesquelles il a délégation

Parfois il installe des programmes gratuits, comme par exemple un jeu.

- Evénement de sécurité :

Le jeu, populaire et bien mis en avant sur les plateformes, s'avère infecté et permet de récupérer des informations personnelles et bancaires transmises en toute discrétion.

3 - Le smartphone ou Ordiphone

- Question :

Combien les Apple Store ou Google Store diffusent-ils d'applications vérolées (téléchargements)?

- Réponse :

- Moins de 100,
- 100 à 1000
- 1000 à 10000
- **10000 à 50000**

Recommandation :

Le smartphone est aujourd'hui un ordinateur, il faut donc utiliser préférentiellement des applications provenant d'éditeur connus, utiliser un antivirus et rester vigilant sur les droits donnés aux applications installées.

4 - Les sauvegardes

- Cas :

Une clé USB a été trouvé à l'accueil, la conseillère en séjour la branche sur son PC pour tenter d'identifier son propriétaire, mais elle contient un logiciel malveillant inconnu de l'antivirus qui se déploie sur le poste.

Ce dernier s'active et cartographie le réseau interne, se propage sur les stations et serveurs, il détecte aussi les moyens de sauvegarde en place.

Quelques jours après il crypte l'ensemble des fichiers et sauvegardes en réseau puis bloque les accès aux utilisateurs.

Enfin une demande de rançon est envoyée par le pirate.

- Evénement de sécurité :

Plus aucune donnée n'est utilisable.

Il a été nécessaire de réinstaller les postes et certains serveurs, puis de restaurer toutes les données depuis une ancienne sauvegarde sur support amovible.

L'OT a été arrêté pendant une semaine, des données ont été définitivement perdues.

4 - Les sauvegardes

- Question :

Quelle est la proportion de données sauvegardées et testées dans les entreprises ?

- Réponse :

- **Moins de 25%**
- De 25 à 50%
- De 50 à 75%
- Plus de 75%

- Recommandation :

S’assurer que les données utilisées sont bien sauvegardées, y compris celles pouvant être temporaires.

Prévoir une conservation minimum de deux mois. Un jeu de sauvegarde hors ligne doit exister et être utilisé à intervalles adaptés

Et assurez-vous régulièrement quelles sont récupérables.

5 – L’arnaque au président

- Deux Cas :

1/ Un appel insistant du "président" pour faire un virement en urgence, avec un email qui semble confirmer et présentant un RIB vers lequel faire le virement.

2/ Un email d’un fournisseur connu, demande le paiement d’une facture avec un nouveau RIB. L’adresse email de l’émetteur est légitime, mais l’utilisateur s’était fait pirater sa boîte email.

1 -> Le comptable effectue la transaction.

2 -> Le comptable connaissant la personne, modifie le RIB et fait le versement correspondant à la facture sans vérification interne

Dans les deux cas on s'aperçoit quelques jours plus tard que c'était une arnaque.

- Evénement de sécurité :

Une perte financière immédiate et irrécupérable.

5 – L’arnaque au président

- Question :

Comment sécuriser les opérations bancaires ?

- Réponse :

- Par un appel du donneur d'ordre et envoi d'une copie de pièce d'identité
- Par un email et un SMS
- Par un email du donneur d'ordre
- **Par une procédure systématique de validation par rappel du comptable aux donneurs d'ordre et confirmation écrite**

Recommandation :

Mettre en place une procédure incluant une vérification systématique, éventuellement de deux personnes différentes.

Mettre en place un circuit de validation dématérialisé avec signature électronique et authentification forte.

6 - Les réseaux sociaux

- Cas :

Un chargé de communication se rend compte que suite à un piratage de compte, des messages indésirables sont postés sur un grand réseau social nuisant gravement à l'image de l'OT.

Rien n'est prévu face à cette situation et le pirate effectue un chantage financier, sans pouvoir avoir une garantie que à l'issue du paiement de la rançon les accès seront restitués.

- Evénement de sécurité :

Une perte réputationnelle et d'abonnés.

6 - Les réseaux sociaux

- Question :

Comment sécuriser les réseaux sociaux ?

- Réponse :

- En appelant le support du réseau social
- **En s'aidant d'une agence web ou d'un audit de configuration**
- En décochant toutes les options de partage

Recommandation :

Vérifier la configuration détaillée du réseau social utilisé

Bien gérer les comptes ayant des droits d'administration et de publication, avec une bonne gestion des mots de passe. Activer systématiquement la double authentification sur les comptes d'administrations lorsque cela est proposé

7 - Le verrouillage de session

- Cas :

La responsable accueil est en télétravail ce jour, il a laissé sa session ouverte à midi le temps d'aller manger. Un de ses enfants, présent à la maison, consulte l'ordinateur ainsi laissé disponible pour trouver des jeux sur internet et des coloriages. Par une mauvaise manipulation, il supprime le dossier de travail de l'ordinateur (et du coup du serveur), voyant qu'il a fait une bêtise, il vide la corbeille par peur de se faire réprimandé et pour passer inaperçu .

- Evénement de sécurité :

Une violation d'accès aux données suite à une erreur humaine et une perte de travail pour la personne et ses collègues qui travaillez depuis le début de matinée sur le dossier. La sauvegarde se faisant le soir, pas de restauration possible.

7 - Le verrouillage de session

- Question :

A quel moment les vols sur des sessions ouvertes sont les plus pratiqués ?

- Réponse :

- Lors d'une effraction,
- La nuit
- **Durant la pause déjeuner**
- Durant les vacances

Recommandation :

Fermer les sessions (manuellement ou automatiquement au bout de 10 minutes), aussi pour les smartphones, mettre sous clé les documents papiers sensibles (« bureau propre »). Raccourci Windows +L

8 - La réaction sur la détection d’un logiciel malveillant

- Cas :

Un collaborateur administratif découvre un matin que son PC est anormalement lent. Il patiente et va prendre un café en attendant.

Une fois les applications bureautiques lancées le ralentissement n’est pas gênant, il est ignoré.

- Evénement de sécurité :

Le virus fraîchement arrivé sur le poste a donc analysé le poste complètement avant de faire fuiter des informations.

Le carnet d’adresse, des informations personnelles et bancaires ont ainsi été transférées sur internet.

8 - La réaction sur la détection d'un logiciel malveillant

- Question :

Qu'est-ce que le collaborateur aurait dû faire en premier ?

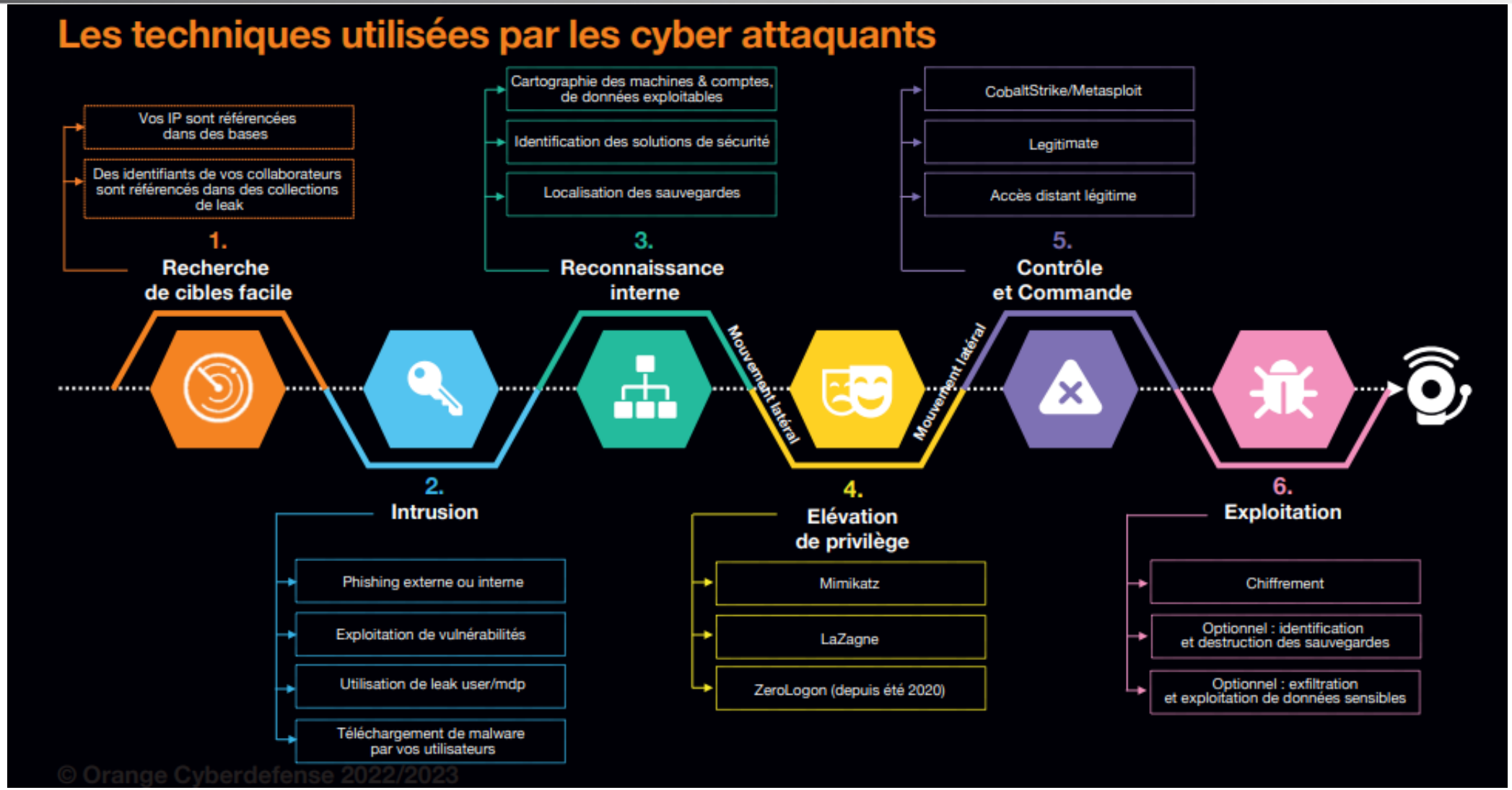
- Réponse :

- **Débrancher l'ordinateur du réseau**
- Eteindre l'ordinateur
- Lancer une analyse antivirus
- Laisser en l'état et prévenir l'équipe informatique.

- Recommandation :

Un comportement anormal d'un PC doit être traité comme un incident significatif.

Isoler l'ordinateur du réseau (wifi et câble) évitera une éventuelle propagation d'un logiciel malveillant ou d'une attaque par rebond d'un pirate, et permettra au service informatique d'intervenir pour analyse et sans risquer de perdre les traces au redémarrage du poste.



Orange Cyberdefense 2022/2023, Security Navigator 2023

Quelques cas connus de la région

- **Ardèche** : le 6 avril 2022, les serveurs du département sont touchés par le très prolifique ransomware Lockbit. Les données sont publiées une semaine plus tard, faute de paiement.

- **Bourg Saint Maurice – Les Arcs**, complètements verrouillés suite à une attaque en Avril 2021
- **Communauté de communes Cœur de Maurienne Arvan** : l'intercommunauté savoyarde a débuté l'année avec une attaque par ransomware lancée le 15 janvier 2022 par le groupe Blackat.
- **Aix-les-bains** : les services de la ville savoyarde sont paralysés le 22 mars 2022. Les serveurs auraient été utilisés pour miner des cryptomonnaies.

Qui sommes nous ?

Nous accompagnons les entreprises dans le conseil, le choix et la mise en œuvre d'usages et d'outils informatiques plus performants

Des experts en temps partagé pour faire avancer vos projets

INFORMATIQUE - DIGITAL

GESTION DU CHANGEMENT

SECURITE DES DONNEES - RGPD

20 ans d'expérience
services informatiques
usages numériques

9 Consultants

1200 jrs de missions en 2019

Economie de Proximité

covateam.com

Les OT nous font confiance sur le RGPD (30 organismes accompagnés)

Offices de Tourisme 73 SAVOIE MONT BLANC

Oisans BIENVENUE DANS LES ALPES

i&d TOURISME OFFICES DE TOURISME & TERRITOIRES DE HAUTE-SAVOIE

flaine 1600-2500 HAUTE-SAVOIE

Les Gets Portes du Soleil

TRAJECTOIRES Tourisme PÔLE PROFESSIONNALISATION AUVERGNE RHÔNE-ALPES

LA PLAGNE Paradiski

ARECHES BEAUFORT

châtel Portes du Soleil

MANIGOD

Sources du lac d'Annecy Tourisme

office de tourisme Auvergne VolcanSancy

LES CONTAMINES MONTJOIE

La Chartreuse un Parc naturel régional

DESTINATION LEMAN 360° de latitude

Evian tourisme & congrès

Praz de Lys Sommand TOURISME

clermont auvergne tourisme

Pays d'Albertville ENTRE LACS & MONTAGNES SAVOIE MONT-BLANC

PEISEY VALLANDRY Paradiski

HAUT RHONE TOURISME

THONON LES BAINS

PASSY TOURISME Camp de Base DES LOISIRS NATURE

Destination Combrailles 100 % Auvergne

la Rosière ESPACE SAN BERNARDO

Saint Jean d'Arves Les Sybelles Destination Emotions

COMBLOUX 360° mont blanc france

Sallanches tourisme LA VILLE AU PAYS DU MONT-BLANC

Grand Massif Montagnes du Giffre

Livradois-Forez PARC NATUREL RÉGIONAL EN AUVERGNE