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 - Sécurité des informations, qu'est-ce que c'est ?

- Cas :

Le chargé de communication de l'OT transfère des photos à un partenaire de l'office de tourisme pour illustrer son site web, mais en fait non libres de droits à l'image.

- Evénement de sécurité :

La diffusion d'information sensible ou personnelle (image) sur internet ou à des destinataires non désirés, génère une utilisation inappropriée.

Cela peut dégrader l'image et la confiance envers l'organisation, etc.

Cet OT a besoin de mieux gérer la sécurité de ses données et les flux d'information.

1 - Sécurité des informations, qu’est-ce que c’est ?

- Question :

Quel est le 4ème critère de sécurité de sécurité d'une information.

Quatre critères fondamentaux sont à prendre en compte : disponibilité, intégrité, traçabilité, xxx ?

- Réponse :

- **Confidentialité**
- Répudiation
- Conformité
- Légalité

- Recommandation :

Identifier les données sensibles et personnelles, ainsi que leurs supports et en gérer la sécurité.

2 - 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.

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 années avant d’être détecté.

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

2 - 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).

3 - L’authentification des utilisateurs

- Cas :

Le jeune stagiaire utilise le même identifiant et mot de passe Windows que l’équipe.

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

- Evénement de sécurité :

Il récupère pour lui et réutilise des droits au détriment de l’OT.

Personne ne s’en est aperçu, mais le stagiaire récupère le futur plan marketing du territoire qui n’est pas encore public.

3 - 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 ».

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.

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

[1] Exemple Keepass : gestionnaire gratuit.

4 - Le smartphone

- Cas :

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

Il échange aussi des fichiers avec son ordinateur.

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

- Evénement de sécurité :

Ce dernier s'avère infecté et permet de récupérer des informations personnelles et bancaires transmises en toute discrétion.

4 - Le smartphone

- Question :

Combien les Apple Store ou Google Store diffusent d'applications vérolées ?

- Réponse :

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

Recommandation :

Le smartphone est comme 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.

5 - Les sauvegardes

- Cas :

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

Ce dernier s'active et cartographie le réseau interne, se déploie sur les stations et serveurs.

Quelques jours après il crypte l'ensemble des fichiers 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.

L'entreprise a été arrêté pendant une semaine.

5 - 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.

Et assurez-vous quelles sont récupérables.

6 - La gestion des droits utilisateurs

- Cas :

Le technicien informatique a donné les droits d'administrateurs à la plupart des utilisateurs pour qu'ils puissent en son absence installer des applications.

Beaucoup de personnes font de la veille et des tests fréquents, et la direction n'aime pas être restreinte dans ses usages.

Ainsi le serveur de fichier de l'entreprise comporte beaucoup de répertoire sans maîtrise.

Tout le monde croit dans l'OT qu'un fichier sensible est plus à l'abri sur son poste que sur le serveur.

- Evénement de sécurité :

Des données personnelles et sensibles sont aisément accessibles, même RH ou financière, et peuvent ainsi mettre en défaut le management comme l'entreprise.

6 - La gestion des droits utilisateurs

- Question :

Quelle proportion de petites entreprises gèrent mal ses données ?

- Réponse :

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

Recommandation :

Définir les données personnelles et sensibles dont chaque métier à besoin

N'autoriser que les personnes "ayant à en connaître" à y accéder.

Assurez-vous que votre gestionnaire informatique met en place l'organisation et les moyens techniques nécessaires, même sur votre poste, n'utiliser pas des droits supérieurs à ceux nécessaires.

7 - Le transfert sécurisé de données

- Cas :

Le directeur adjoint doit envoyer le rapport de saison à ses administrateurs.

Il l'envoi donc par email à une liste d’adresses prédéfinie.

Il se trompe de liste et l'envoie à un fichier presse.

- Evénement de sécurité :

La diffusion de ces informations sensibles à un mauvais public a eu un impact négatif et durable sur l’image de l'OT

7 - Le transfert sécurisé de données

- Question :

Comment échanger de manière simple par un partage de fichier public et sécurisé des documents sensibles ?

- Réponse :

- **Par une gestion électronique de document**
- Par email avec un accusé de réception
- Par une clé USB envoyé par la poste
- par un envoi postal d'une clé USB

- Recommandation :

la GED permet de déclarer et d'authentifier de manière fiable les participants aux échanges.

Ainsi le risque d'erreur sur des accès est limité et la traçabilité de l'application permet de suivre les accès légitimes ou illégitimes de manière précise.

8 - Les attaques au président

- Cas :

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

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 c'était fait pirater sa boîte email.

Le comptable effectue la transaction.

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

- Evénement de sécurité :

Une perte financière immédiate et irrécupérable.

8 - Les attaques 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 au donneur d'ordre et confirmation écrite**

- Recommandation :

Mettre en place une procédure incluant une vérification dans tous les cas, éventuellement de deux personnes différentes.

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

9 - 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.

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.

9 - Les réseaux sociaux

- Question :

Comment sécuriser les réseaux sociaux ?

- Réponse :

- En appelant le support du réseau social
- **En s'aidant d'un d'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

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

- Cas :

Un collaborateur administratif découvre un matin que son PC est anormalement lent.

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 transféré sur internet.

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

- Question :

Qu'est-ce que l'assistante aurais 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 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.

Mais au fait, qui sommes nous ?

Une approche conseil opérationnel globale pluridisciplinaire

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

Gouvernance et pilotage du SI

Construction du portefeuille de projets
Recherche de gains (coûts, productivité, compétitivité)
Pilotage des ressources
Tableaux de bords décisionnels

Gestion des projets SI

Audit, Conseils, Aide au choix de nouvelles solutions
Lancement des consultations
Pilotage des prestataires
Gestion du changement

RGPD

Mise en conformité
Certification de process
Formation
DPO externalisé

Cybersécurité

Politique de sécurité
Réduction des risques techniques
Amélioration des usages
Résilience (PRA/PCA)

Nos expertises RGPD

Des experts RGPD à votre service

3 juristes en protection des données personnelles
7 consultants sécurité des données

Membre AFCDP

Certification EUROPRIVACY

=> Plus de 200 collectivités, associations, PME accompagnées sur le RGPD

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

Aréches 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 Léman – 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 Rhône 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

Des questions ?

Consultante RGPD
DPO externalisé

Sophie BOREL

07 50 89 36 01 – sophie.borel@covateam.com

Directeur Général

Philippe DUJARDIN

06 77 40 23 80 - philippe.dujardin@covateam.com