Trousse Entreprise

L’impact du télétravail sur les petites et moyennes entreprises

cyber eco

Table des matières

PRÉSENTATION DE L’ACTIVITÉ

Présentation de l’activité

OBJECTIFS

ANIMER

une discussion au sein de l'entreprise afin de partager les connaissances relatives au thème abordé.

ENCOURAGER

la prise de parole et le partage d’expériences relatives à des attaques utilisant les techniques abordées par le thème de la discussion.

DÉTAILS DE L’ACTIVITÉ

Durée	Objectif	Responsabilités de l’animateur	Responsabilités des employés	Matériel
10 - 20 minutes	Couvrir brièvement les points essentiels du thème abordé dans le guide	Présenter et commenter les réponses aux questions	Répondre aux questions	Projecteur Tableau interactif

QUESTIONS POUR LA DISCUSSION

Questions pour la discussion

1. Pourquoi le travail à distance facilite-t-il les cyberattaques?
2. Quelles sont les méthodes les plus courantes utilisées par les malfaiteurs depuis la prolifération de travailleurs à distance?
3. Quelles sont les activités à mettre en place pour protéger vos systèmes dans le cadre du télétravail?
4. Quelles pratiques sécuritaires pouvons-nous adopter lorsqu'on travaille de la maison?

Impacts du travail à distance

En propulsant un nombre jamais vu de travailleurs à la maison, le travail à distance a offert de nouvelles opportunités aux cybercriminels.

Parmi les différentes tentatives de cyberattaque, une grande majorité (80 %) a été réalisée par l'intermédiaire d'arnaques par courriel ou des tentatives **d'hameçonnage** et la moitié par des logiciels malveillants, selon un rapport de la Fédération canadienne de l'entreprise indépendante[1].

Le **rançongiciel** est un logiciel qui prend en otage les données que contient un appareil informatique en les cryptant. La personne malveillante exige que lui soit versée une rançon en échange du déverrouillage de l'appareil. Les liens malveillants se propagent souvent à l'intérieur de courriels.

Depuis mars 2020

- **2/3 des entreprises dans le monde**, et 63 % au Canada, ont constaté une augmentation des cyberattaques ciblées depuis qu'elles se sont tournées vers le télétravail[2].
- **Plus de 61 000 PME canadiennes** ont fait l'objet d'attaques informatiques au cours de l'année passée, dont 5 % qui en ont été victimes[3].

1. Avec l'accélération du virage numérique en temps de crise, les PME craignent de plus en plus les cyberattaques | FCEI (cfib-fcei.ca)
2. Les cyberattaques en hausse depuis l'avènement du télétravail, selon une enquête | Radio-Canada.ca
3. Ibid

Vulnérabilités du télétravail

De nouveaux risques émergent pour les organisations en raison de l'évolution des habitudes des utilisateurs

De nombreuses organisations ne fournissent pas un environnement à distance sécurisé. Elles n'offrent pas l'utilisation d'un VPN et les réseaux résidentiels sont moins sécuritaires que ceux d'un bureau.

Certaines entreprises adoptent l'approche : « Apportez votre propre appareil », ce qui signifie que les employés peuvent utiliser leurs appareils personnels (téléphones, tablettes ou ordinateurs portables) pour accéder aux informations de l'entreprise. Lorsque les employés utilisent un ordinateur personnel pour accéder aux fichiers et aux données de l'entreprise, celles-ci perdent le contrôle sur ce qui transite sur leurs systèmes et leurs réseaux si elles n'appliquent pas au minimum une certaine gestion sur ces appareils personnels.

Les organisations sont ainsi plus vulnérables aux attaques, car elles disposent d'une visibilité et d'une protection plus limitées sur des actifs personnels contentant des données sensibles de l'organisation.

Le saviez-vous? Si un appareil est branché à Internet, il est à risque.

Les êtres humains y sont aussi pour quelque chose…

L'erreur humaine est au cœur de la prolifération des cyberattaques

Les employés peuvent donner involontairement ou imprudemment accès aux mauvaises personnes.

Ils peuvent cliquer sur des liens malveillants et ils peuvent utiliser des mots de passe peu sécuritaires ou même les réutiliser sur plusieurs sites.

Le saviez-vous?

La **technique du bourrage**[1] d'information consiste à utiliser des noms d'usagers et des mots de passe trouvés sur des sites illégaux et les essayer sur plusieurs sites Web. La trousse #2 de Cybereco traite de l'importance à accorder aux mots de passe.

Pour plus de détails, consultez la trousse #2 : **Mot de passe - Cybereco**

1. Bourrage d'information (« credential stuffing ») Impact du COVID-19 sur la cybersécurité (deloitte.com)

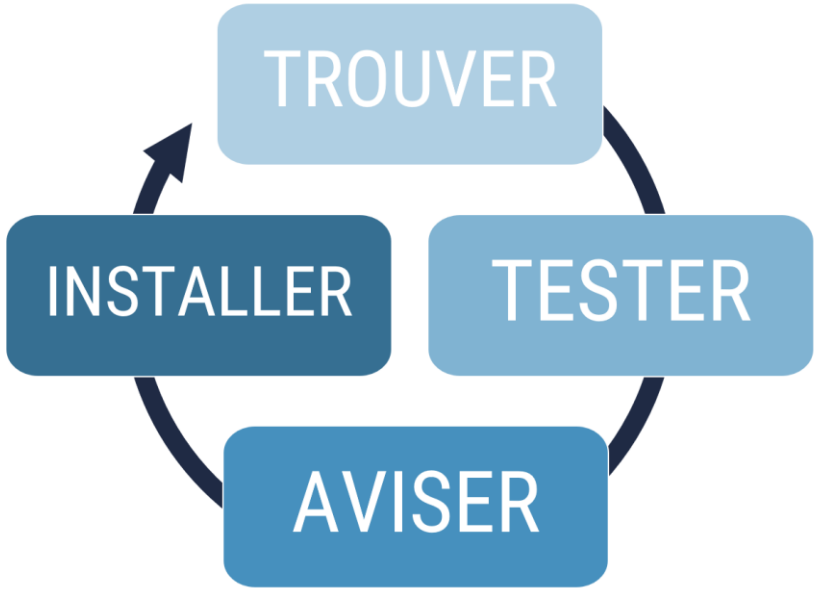
Comment se protéger?

Mettre à jour ses appareils

La mise à jour régulière des actifs de l'organisation est essentielle à la protection de vos appareils et des données qu'ils contiennent dans le cadre du télétravail.

Votre organisation peut utiliser des outils de détection des vulnérabilités pour **trouver** les correctifs manquants parmi vos actifs. La mise en place d'un *processus de vigie* des vulnérabilités est également utile pour les organisations ainsi que la tenue d'un *inventaire des actifs* à jour au sein de l'organisation.

De plus, des **tests** des correctifs devraient être effectués dans des environnements hors production avant le déploiement de ceux-ci sur les actifs clés afin d'évaluer les impacts potentiels.



Enfin, **avisez** toutes les personnes concernées que des correctifs sont disponibles et qu'ils devront être **installés**.

Le saviez-vous?

L'objectif premier des **mises à jour** est de **colmater les vulnérabilités** ou les faiblesses liées à la sécurité d'un système.

« **Une vulnérabilité** est une lacune ou une faiblesse liée à la sécurité. Il peut y avoir des vulnérabilités techniques dans la conception, la mise en œuvre, l'exploitation ou la gestion d'un système, d'un appareil ou d'un service informatique[1]. »

1. Application des mises à jour sur les dispositifs (ITSAP.10.096) - Centre canadien pour la cybersécurité

Comment se protéger?

Sauvegarder vos documents dans le nuage

Les sauvegardes visent à protéger les données sensibles de votre entreprise notamment face à une attaque par rançongiciel

Les systèmes et les données utilisés par les entreprises doivent être sauvegardés régulièrement et les copies de sauvegardes ne devraient pas être sur le même appareil que celui utilisé pour le travail. Il est conseillé d'utiliser un service infonuagique reconnu dans l'industrie qui, entre autres, permet de chiffrer les données sauvegardées, d'avoir une politique de mots de passe robuste et de requérir l'authentification à double facteur.

Il est également pertinent d'effectuer des sauvegardes à une fréquence définie. Le délai entre deux sauvegardes ne devrait pas excéder le temps dont vous auriez besoin pour restaurer vos données advenant un cyberincident.

Pourquoi sauvegarder vos documents?

- Un **rançongiciel** bloque l'accès à vos données. L'attaquant exige une rançon importante pour les déverrouiller.
- Si un imprévu se produit, les sauvegardes permettent la **disponibilité** de vos données.
- Les sauvegardes permettent également la **récupération** de vos données si vous avez besoin de restaurer vos systèmes.

Le saviez-vous?

Le Centre canadien pour la cybersécurité recommande également que les organisations conservent leurs copies de sauvegarde chiffrées dans un endroit sécurisé et que seuls les employés disposant des privilèges nécessaires doivent pouvoir accéder aux copies de sauvegarde[1].

Dans le cadre d'une attaque par rançongiciel, les copies de sauvegardes peuvent permettre de récupérer rapidement vos données si elles n'ont pas été corrompues.

1. Application des mises à jour sur les dispositifs (ITSAP.10.096) - Centre canadien pour la cybersécurité

Comment se protéger?

Adopter l’authentification à double facteur

L’authentification à double facteur atténue le risque de vulnérabilité des entreprises ou des utilisateurs privés aux cyberattaques par force brute ou hameçonnage

Pour ajouter une couche de protection supplémentaire, les organisations devraient instaurer l’authentification à double facteurs. Ce protocole de sécurité oblige les usagers à utiliser une seconde méthode d’authentification en plus du mot de passe.

L’utilisation d’un code à usage unique envoyé par SMS est probablement la méthode la plus répandue, mais d’autres méthodes sont plus sécures :

- **Application tierce** générant un code à usage unique
- **Clé physique**
- **Identification biométrique**
- **Appel téléphonique**

Votre organisation doit déterminer quelle stratégie lui convient le mieux et, une fois implantée, s’assurer d’en informer tous les utilisateurs. L’utilisation d’un *système d’authentification unique* (SSO) pour plusieurs applications peut permettre de faciliter ce processus pour les utilisateurs et peut donc être envisagée par votre organisation.

Le saviez-vous?

L'authentification double facteur devrait être offerte à vos employés pour les connexions internes, mais elle devrait également l’être pour vos clients qui doivent ouvrir une session sur votre site Web; elle renforcerait ainsi la sécurité dans l’accès à leur compte.

L’authentification double facteur est validée par la conjugaison de deux facteurs. Elle est parfois appelée « authentification à deux étapes[1] ».

1. Glossaire - Centre canadien pour la cybersécurité

D’autres éléments à considérer

En plus de modifier nos habitudes et d’adopter de bonnes pratiques, le travail à domicile exige une vigilance de tous les instants. Le Centre pour la cybersécurité du Canada recommande les initiatives suivantes :

- **Protéger** votre routeur sans fil domiciliaire à l’aide de phrases de passe robustes
- **Désactiver** les services de réseautage Wi-Fi et Bluetooth, lorsque vous ne les utilisez pas
- **Utiliser** les antivirus et antimaliciels de fournisseurs de confiance (versions payantes)
- **Signaler** toutes activités suspectes à votre équipe de sécurité des TI
- **Implanter** un réseau privé virtuel (VPN) à votre organisation. Ils ajoutent une couche supplémentaire de protection pour le travail à distance.

N’oubliez pas…

Changez régulièrement vos mots de passe et assurez-vous qu’ils sont uniques et qu’ils ne sont pas réutilisés sur d’autres sites.

Méfiez-vous de l’hameçonnage et portez une attention particulière aux courriels qui proviennent de l’extérieur de votre organisation.

La sensibilisation : une tactique gagnante

- Il est plus que jamais nécessaire d'offrir des sessions d'information en matière de cybersécurité à l'intention des employés et du public en général.
- C'est la répétition des messages qui parviendra à faire diminuer les attaques fructueuses et qui convaincra les utilisateurs à adopter de saines pratiques.

S'il n'est pas possible d'éliminer l'ensemble des menaces et d'assurer qu'un système ne soit jamais attaqué, l'utilisation de meilleures pratiques et l'éducation des utilisateurs permettent de réduire considérablement les risques et assurent l'une des meilleures protections.

Recommandations

Regardez la **vidéo de Cybereco** pour en apprendre davantage.

Testez vos connaissances et vos réflexes à l'aide du **quiz Cybereco**.

N'OUBLIEZ PAS !

Vous êtes une ligne de **défense importante** pour protéger l'entreprise.