UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Pourquoi protéger vos données

PROTÉGER LES DONNÉES PARTAGÉES

Depuis plusieurs années, les entreprises ont mis l'emphase et beaucoup d'énergie à mettre en place des filtres antipourriel, des pares-feux qui analysent les échanges réseau et des solutions de sécurité diverses afin de protéger l'organisation contre plusieurs types de cyberattaque. Ce sont tous des éléments dissuasifs qui ont pour but de protéger et de décourager un attaquant d'essayer de pénétrer dans l'organisation. Considérant la difficulté accrue d'une attaque réussie, les cybercriminels ont opté pour de nouveaux vecteurs d'intrusion : ce sont maintenant les employés et utilisateurs de l'organisation qui sont ciblés plutôt que les systèmes.

Bien que nous soyons maintenant dans l'ère numérique, la plupart des utilisateurs ne sont pas conscients de la portée et de l'impact qu'ont les informations qu'ils diffusent dans leurs activités quotidiennes. Ils ont entre leurs mains des données personnelles et des données corporatives qui sont d'une valeur incroyable aux yeux d'un acteur malveillant, et ces pirates sont de plus en plus ingénieux dans les méthodes qu'ils utilisent afin de s'en emparer.

QUELS SONT LES TYPES DE DONNÉES CIBLÉS PAR UN CYBERCRIMINEL ?

Plusieurs types différents de données qui sont de valeur pour un acteur malveillant. Chacun de ces types est utilisé pour des fins différentes, et peut poser un risque énorme pour un individu ou une organisation qui en serait victime. Il devient donc important pour un utilisateur de savoir s'il manipule des données sensibles. Voici donc les classements possibles de l'information sensible :

- **Information d'identification personnelle**

  Inclut le numéro d'assurance sociale, l'information de contact, la date de naissance, nom, prénom, identité de genre
- **Information financière**

  Inclut les numéros de cartes de crédit, dates d'expiration, numéros de compte, informations bancaires et transactions
- **Information médicale**

  Inclut les informations sur les prescriptions, état de santé, traitements et historique médical
- **Propriété intellectuelle**

  Inclut les logiciels propriétaires, dessins, documents de recherches, notes de cours, modélisations et formules scientifiques
- **Données de compétition**

  Incluent des données sur les compétiteurs, des études de marché et des plans d'affaires
- **Données légales**

  Contiennent l'information de la documentation sur les affaires judiciaires et détails d'acquisition
- **Données de sécurité informatique**

  Incluent les noms d'utilisateur, mots de passe, schémas du réseau, informations sur les solutions de défense

COMMENT PROTÉGER LES DONNÉES ?

Les cybercriminels ne manquent pas d'imagination afin d'obtenir ce qu'ils désirent. Les méthodes qu'ils utilisent sont variées, mais pas toujours transparentes. C'est pourquoi la vigilance est importante dans le travail quotidien pour s'assurer que nous ne diffusons pas de l'information sensible à un acteur malveillant.

Voici plusieurs ressources qui expliquent quels types d'attaque sont perpétrés par un cybercriminel, et les mesures que nous pouvons, en tant qu'utilisateur de différents systèmes informatiques, prévenir d'en devenir victime et ainsi protéger les données que nous manipulons.

Livre blanc sur la sensibilisation à la sécurité informatique (Kaspersky)

Un ouvrage très explicatif sur les différentes stratégies employées par les cybercriminels, et sur les types de mesure qu'on peut mettre en place dans les organisations afin de sensibiliser les utilisateurs sur leur existence.

Meilleures pratiques (UQAC)

Un tableau démontrant de bonnes pratiques pour chacun des aspects de l'utilisation des ressources technologiques.

Le piratage psychologique (Pensez cybersécurité)

Des illustrations qui démontrent la réalité du piratage psychologique, et comment nous pouvons tous en être victime.

Comment protéger l'information que vous envoyez par courriel (CSCUQ)

Un guide d'utilisation sur les outils de chiffrement dans Outlook. Des explications détaillées pour chacune des options disponibles.

Clés USB – Les dangers et bonnes pratiques

Un article qui décrit les risques associés avec les clés USB, et comment s'en protéger.

RÉVISIONS

Date	Action	Auteur	Ver.
2023-01-18	Ajustement du modèle du document	Jean-François Blais CESI de l'UQ	1.1
2021-11-01	Version courante	Jean-François Blais CESI de l'UQ	1.0