ÉTUDE DE CAS

MISE EN SITUATION

L'entreprise CoopR est une grande coopérative financière canadienne dont la mission est d'offrir des services financiers avantageux à ses quelques 6 millions de membres. Présente à travers toutes les provinces du Canada, elle dispose d'un réseau de plus de 500 points de services. Ses services sont également disponibles sur son site Internet et sur application mobile.

La coopérative CoopR emploie plus de 50 000 personnes à travers le Canada, dont environ 3000 personnes travaillant dans le département des technologies de l'information. Elle dispose également d'une équipe de sécurité informatique regroupant quelques 100 employés, dont une équipe responsable du programme de sensibilisation à la sécurité, une équipe de gestion des identités et des accès qui contrôle les accès et une équipe responsable de faire des tests de sécurité auprès des systèmes et des employés.

Le profil sociodémographique des employés est le suivant :

- Sexe :
    - Femmes : 75 %
    - Hommes : 25%
- Âge :
    - Moyenne : 45 ans
    - 20-30 ans : 15 %
    - 31-40 ans : 25 %
    - 41-50 ans : 40 %
    - 51-60 ans : 15 %
    - 61 et plus : 5 %
- Ancienneté moyenne : 10 ans
- Études :
    - Maîtrise : 10 %
    - Baccalauréat 35 %
    - Collégial 50 %
    - Secondaire 5 %
- Utilisation des technologies au travail
    - 95 % utilisent un ordinateur fourni par la coopérative, avec une adresse courriel corporative et un accès à Internet
    - 50 % ont un portable et travaillent en mobilité (sur la route ou de chez eux)

SES POLITIQUES DE SÉCURITÉ

CoopR a une politique corporative de sécurité qui définit les objectifs de sécurité de l'information et les rôles et responsabilités au sein de l'organisation.

Selon cette politique, le chef de la sécurité de l'information est responsable du programme de sécurité, incluant :

- L'élaboration du programme de sensibilisation et de formation à la sécurité de l'information pour tous les employés
- La définition des exigences de sécurité de l'information
- Le suivi du respect des exigences de sécurité de l'information
- La reddition de compte auprès de la haute direction en sécurité de l'information

Les gestionnaires ont les responsabilités suivantes :

- S'assurer que leurs employés suivent les formations obligatoires en sécurité de l'information
- S'assurer que leurs employés respectent les exigences de sécurité de l'information
- Demander le retrait des accès lorsqu'un employé quitte son emploi ou change de rôle au sein de l'entreprise

Les employés ont les responsabilités suivantes :

- Suivre les formations obligatoires en sécurité de l'information
- Respecter les exigences de sécurité de l'information, notamment lors de l'utilisation des technologies fournies par la coopérative. Ces exigences incluent :
    - L'obligation de protéger la confidentialité de l'information appartenant à l'entreprise ou à ses membres
    - L'interdiction d'utiliser son adresse corporative de courriel pour s'abonner à des sites ou échanger avec des personnes à des fins personnelles
    - L'interdiction d'utiliser son adresse de courriel personnelle pour échanger des informations relatives à l'entreprise ou ses membres
    - L'interdiction de diffuser de l'information ou des opinions relatives à l'entreprise sur les médias sociaux
    - Ne pas partager ses accès avec ses collègues
    - L'interdiction d'utiliser des sites publics de partage d'information pour échanger des informations relatives à l'entreprise ou ses membres
- Signaler immédiatement tout incident de sécurité de l'information à l'équipe de sécurité

La politique corporative de sécurité de l'information ne prévoit pas de conséquences explicites en cas de non-respect de ses exigences. Il est d'ailleurs très rare que des employés ou gestionnaires soient réprimandés ou sanctionnés pour avoir enfreint la politique de sécurité de l'information ou avoir utilisé à des fins personnelles l'équipement informatique qui leur est fourni.

SES STRATÉGIES ACTUELLES

L'entreprise a recours a trois stratégies principales pour prévenir les brèches de sécurité de l'information :

1. Le programme de sensibilisation et de formation à la sécurité de l'information

   CoopR a un programme de sensibilisation qui vise tant les employés que ses membres et le grand public. Il inclut des campagnes de sensibilisation ciblées qui visent à influencer les comportements de chaque individu. Il vise à développer chez l'individu le réflexe de garder pour soi toute information confidentielle ou personnelle et réfléchir avant de cliquer sur un courriel dont la provenance est inconnue. La formation théorique est sous forme de capsule d'auto-formation d'une durée de 20 minutes. Elle explique le stratagème d'hameçonnage et ses principaux indices et informe sur la procédure de signalement d'un incident de sécurité de l'information.

   Cette formation est faite une seule fois, i.e. les employés n'ont pas à la refaire périodiquement. Tout nouvel employé doit suivre la formation, mais il n'y a pas de vérification systématique et l'employé obtient son ordinateur qu'il ait ou non suivi la formation. C'est à chaque gestionnaire de s'assurer que ses employés suivent la formation.

2. La surveillance des systèmes informatiques

   Compte tenu de la vitesse à laquelle les technologies et les nouvelles menaces évoluent, une des stratégies sur laquelle mise la coopérative est la surveillance de ses systèmes informatiques. Cette surveillance vise à prévenir et surtout détecter le plus rapidement possible toute brèche ou compromission de la sécurité de ses systèmes afin de pouvoir prendre les mesures nécessaires pour minimiser les dommages. Une équipe surveille durant les heures normales de travail l'état des systèmes et les alertes qui sont générées par les systèmes de détection d'intrusion, l'anti-spam et l'anti-virus. Des balayages des systèmes sont également effectués chaque mois afin d'identifier si toutes les configurations et correctifs de sécurité sont adéquatement déployées sur les systèmes informatiques de l'entreprise.

   Le filtrage web bloque l'accès à plusieurs sites dont les sites publics d'échanges d'information.

3. La vigie et le partage d'information sur les menaces avec d'autres institutions financières et organisations du secteur public.

L'équipe de sécurité fait une vigie sur les nouvelles menaces et participe à des groupes de partage d'information sur les menaces, que ce soit des groupes d'industrie tel l'Association canadienne des banquiers ou le Financial Services – ISAC ou encore des fils d'information tel celui du Centre canadien de réponse aux incidents cybernétiques (CCRIC) et le Canadian Cyber Threat Exchange (CCTX). Des abonnements à des sources d'information automatisées permettent également d'alimenter les systèmes de surveillance avec les nouvelles signatures de virus ou autres logiciels malicieux.

4. Une gestion des identités et des accès centralisés

   L'équipe de Gestion des identités et des accès (GIA) gère une dizaine d'outils pour réaliser les demandes d'ajout, de modification ou de retrait d'accès. Toutes ces demandent entrent via un guichet unique. Lors d'un départ, le gestionnaire doit informer l'équipe de GIA pour que les accès de l'employé soient retirés. Cette équipe est aussi responsable de l'expérience utilisateur. Elle doit répondre rapidement aux demandes et aux problèmes liés aux accès. L'équipe de GIA peut aussi produire des rapports sur demande. Par exemple, elle est capable de produire un rapport au gestionnaire sur les droits d'accès de ses employés.

SES OUTILS ET CAPACITÉS TECHNOLOGIQUES

L'entreprise a implanté les outils suivants visant à se prémunir contre la fuite d'information, les attaques par déni de service ou les rançongiciels :

- Un anti-spam
- Un anti-virus
- Un système de filtrage web (*web filtering*)
- Un système de détection d'intrusion (*Intrusion detection system*)
- Une segmentation et un coupe-feu réseau (*firewall*)
- Un coupe-feu applicatif (*web application firewall*)
- Le chiffrement du disque dur des postes de travail

L'entreprise a aussi implanté les outils suivants visant à mieux gérer les identité et accès des employés :

- Une source autoritaire pour les identités (i.e. *Active Directory*)
- Solutions pour ajouter, modifier et supprimer des utilisateurs
- Solution d'authentification unique (*Single Sign on*)
- Gestionnaire de mot de passe
- Outil en libre-Service pour la réinitialisation des mots de passe Windows
- Solution de gestion des comptes à hauts privilèges
- Système de journalisation et de surveillance des accès

INSTRUCTIONS DE TRAVAIL

CoopR a été victime en 2018 d'une fuite de données qui a causé des dommages directs et indirect de plus de 5 millions de dollars. À l'aide d'un compte non désactivé d'un ancien collègue, un employé en intelligence d'affaires a extrait des données de la base de données membres et les a déposées sur un serveur externe. Les données extraites contenaient des renseignements personnels des membres (nom, prénom, adresse, numéro de téléphone) et des données sur leur détention (niveau de richesse, total des actifs, dettes). Une fois déposées sur ses propres serveurs, il les a revendues sur Internet.

Lorsque l'incident a été identifié, l'entreprise a dû dédommager des milliers de membres en plus d'assumer le temps supplémentaire des employés et des consultants qui ont travaillé plusieurs semaines à rétablir la situation et répondre aux questions des membres touchés. Deux cabinets d'avocats ont lancé des procédures d'actions collectives contre CoopR pour négligence en matière de protection de la vie privée de leurs clients.

À l'aide d'un outil de visualisation d'accès, l'entreprise a constaté que plusieurs de ses employés peuvent accéder à une quantité importante d'information classifiée confidentielle (ex. : renseignements personnels des membres, numéro de carte de crédit, données financières, mot de passe, code source) dans des bases de données. Plusieurs employés qui ont quitté l'entreprise depuis plusieurs années avaient encore leurs accès activés. CoopR souhaite renforcer le niveau de responsabilisation des gestionnaires sur qui le processus de retrait des accès repose.

Vous êtes engagé à titre de consultant afin de recommander à CoopR un programme de responsabilisation des gestionnaires sur la menace interne et la sécurité des accès. Le programme doit inclure des actions à court (< 3 mois), moyen (+/- 6 mois) et long terme (> 12 mois). Ce programme doit prendre en considération l'impact sur les gestionnaires visés, les employés et l'organisation dans son ensemble.

On vous demande aussi de poser un diagnostic sur les 1) politiques, 2) les stratégies et 3) les solutions technologiques actuellement en place et recommander des ajustements permettant d'éliminer l'accès inadéquat à des données confidentielles.

Les recommandations doivent tenir compte du budget alloué par les dirigeants de CoopR pour le programme de responsabilisation qui est de 6 millions sur trois ans incluant les ressources, le matériel et les frais de consultation pour l'accompagnement.

Pour vous aider dans l'estimation de vos recommandations, voici une estimation de coûts des différentes ressources :

- Rémunération globale annuelle d'un employé à temps plein : 170 000$
- Taux horaire d'un consultant externe senior : 400$
- Coût annuel par utilisateur pour une solution de GIA : 1000$
- Coût annuel du support 24/7 pour une solution de GIA : 180 000$

- Coût de formation sur une solution : 10 000$

Afin d'évaluer l'efficacité du programme, un ou plusieurs indicateurs de suivi du programme devront être proposés.

Appuyé d'une revue de littératures, d'études comparatives, de sondages et de statistiques, analysez d'un point de vue critique chaque volet de son approche de sécurité. Votre analyse pourra par exemple faire ressortir les éléments suivants :

a. Est-ce aligné avec les tendances de l'industrie ?
b. Est-ce que l'approche s'est avérée efficace pour d'autres entreprises ?
c. Quelles seraient les approches alternatives ou complémentaires ?

Les sous-questions auxquelles les étudiants devraient réfléchir dans le travail de session :

- Quelle stratégie de responsabilisation est la plus efficace dans un programme de sensibilisation destiné aux gestionnaires ?
- Quelle est la proportion des solutions technologiques versus des stratégies visant à changer les comportements humains dans la résolution de la problématique ?
- Une approche individuelle a-t-elle plus d'impact qu'une approche collective dans l'apprentissage des gestionnaires ?

Il est attendu des étudiants qu'ils se positionnent sur les trois volets (politiques, stratégies et outils) en justifiant leur position selon :

- Les menaces et attaques les plus courantes
- Une revue de la littérature sur les types de stratégie et leur efficacité
- Un balisage des mesures de réponses envisageables pour les employés malveillants
- Une vigie sur les produits et services disponibles sur le marché (en gestion des identités et des accès spécifiquement)