CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

La cybersécurité, une protection de l'intérieur vers l'extérieur

LA CYBERSÉCURITÉ : UNE GUERRE DE TRANCHÉES (PARCE QUE LES INCIDENTS DE SÉCURITÉ SONT LA « NOUVELLE NORMALITÉ »)

par Claudiu Popa, CISSP, CIPP, PMP, CISA, CRISC

Vue d'ensemble

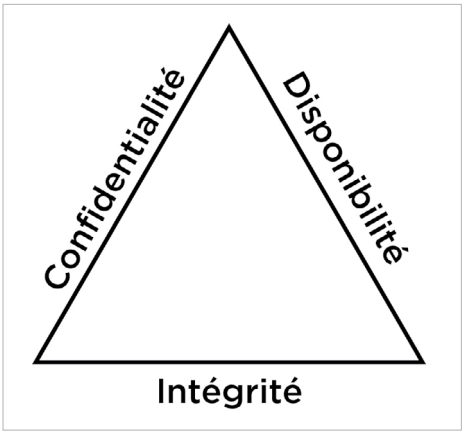
À en juger par les titres des journaux, on pourrait croire que les atteintes à la protection des données font inévitablement partie de la vie moderne. C'est pourquoi de nombreuses personnes et organisations s'étonnent quand on leur dit que tous les incidents de sécurité dommageables sont évitables. Si certains sont plus difficiles à anticiper, la plupart des cyberincidents semblent se produire selon un nombre limité de scénarios.

Le cas présenté ici s'inspire d'événements réels. L'entreprise, Fincharge Inc., est fictive. Ce cas illustre la façon dont les incidents se manifestent et la mesure dans laquelle l'adoption de la bonne approche (même s'il s'agit d'une approche réactive) peut faire toute la différence lorsqu'on veut désamorcer une attaque et permettre à l'entreprise de reprendre rapidement ses activités normales.

La mise en place de mesures de cybersécurité peut s'avérer difficile, mais, comme nous le verrons ici, il ne s'agit pas d'une mission impossible. Pour y parvenir, l'entreprise doit compter sur une direction compétente et des professionnels de qualité. Pensez-vous que vous avez ce qu'il faut? Qu'en est-il de vos équipes? Comment gérer ce type d'événement?

Étude de cas

C'est *toujours* une question d'incidence



Tout scénario de cyberattaque s'apparente à une guerre de tranchées. Au début de la dernière décennie, Fincharge a établi que la cybersécurité et la protection des renseignements personnels constituaient des objectifs clés, mais n'a pas réussi à investir dans des processus et des outils de sécurité pour rendre la protection des données efficace. À cause de ce manque de préparation, l'entreprise allait devoir se démener et s'adapter pour contrer les avancées de l'adversaire en cas d'attaque.

En l'espace de neuf mois, l'entreprise a survécu à trois cyberincidents relevant directement des trois composantes de la « triade CID ». Bien connues des spécialistes de la sécurité de l'information, ces composantes sont la confidentialité, l'intégrité et la disponibilité des données. Dans la présente étude de cas, l'entreprise a subi des attaques qui ont eu une incidence sur les trois objectifs en matière de sécurité de l'information :

- Confidentialité : des informations sensibles ont été exposées en permanence;
- Intégrité : les informations inactives ont été menacées par des logiciels malveillants;
- Disponibilité : pendant la pandémie, les systèmes ont été inutilisables durant une longue période.

Comment en est-on arrivé là?

Incidence sur la confidentialité : À l'insu de Fincharge, son fournisseur de services, EnterTrust, a subi une atteinte à la cybersécurité qui a exposé tous les dossiers de clients appartenant à Fincharge. Un employé a accédé aux données sur les clients et en a fait des copies dans l'espoir de tirer profit de leur vente. L'incident n'a été signalé à Fincharge que sept semaines plus tard, par l'intermédiaire de l'avocat d'EnterTrust. Ce délai a ébranlé la relation avec ce fournisseur, ce qui a obligé l'entreprise à informer immédiatement les personnes touchées et à s'adapter pour gérer l'afflux de demandes de clients inquiets.

Que s'est-il vraiment passé?

Dès que Fincharge a eu connaissance de ce qui était arrivé, le responsable de la protection des données et le conseiller en cybersécurité de l'entreprise ont signalé l'incident au Commissariat à la protection de la vie privée du Canada (CPVP), l'organisme chargé du respect de la vie privée, qui a émis les recommandations suivantes :

1. Mettre en place une ligne téléphonique permettant de répondre aux questions des clients de Fincharge et de les orienter vers la ligne d'assistance d'EnterTrust;

2. Souscrire une assurance cyber-responsabilité pour éviter que l'exploitation éventuelle des données compromises ne devienne un grave problème de responsabilité pour Fincharge;
3. Aviser les clients, les informer de la gravité des conséquences et leur offrir de l'aide, des ressources et des conseils supplémentaires si nécessaire.

Incidence sur l'intégrité : Deux mois plus tard, Fincharge a fait l'objet d'une cyberattaque directe par courriel qui a donné lieu à l'installation d'un logiciel malveillant menaçant l'entreprise de chiffrer et de supprimer les données sur ses serveurs. Comme c'est souvent le cas, cette cyberattaque consistait à envoyer à une dizaine d'employés de Fincharge des courriels personnalisés qui semblaient provenir de collègues leur demandant d'ouvrir d'urgence une pièce jointe. Une fois ouverte, la pièce jointe analysait l'ordinateur local et le réseau environnant, à la recherche de vulnérabilités et d'un moyen de se connecter à son serveur d'origine pour télécharger d'autres logiciels malveillants. Le service informatique de Fincharge s'est efforcé d'agir rapidement pour tenter de devancer la menace invisible.

Que s'est-il vraiment passé?

L'objectif du logiciel malveillant était de localiser les données sensibles de Fincharge, de les voler et d'interrompre les activités suffisamment longtemps pour obtenir le paiement d'une rançon. L'équipe informatique de Fincharge a réussi à désamorcer cet incident en menant une série d'activités rapides et appropriées. Elle y est parvenue en réagissant dès la première atteinte à la protection des données.

La capacité à prévenir avec succès une atteinte potentielle avant qu'elle n'atteigne la phase d'extorsion repose sur un effort conjoint de l'équipe informatique de Fincharge et de son CPA, qui a été formé à la réponse aux incidents de cybersécurité. Relevant du directeur de l'information et du directeur financier, le CPA a réussi, dans le cadre de sa fonction consultative, à surmonter les obstacles et à déterminer les conséquences pour l'entreprise. Ces approches décisives ont permis à l'entreprise d'analyser et d'isoler rapidement les ordinateurs du réseau, de désactiver les appareils inutiles et d'enquêter individuellement sur tous les actifs qui avaient été en contact avec les systèmes infectés à l'origine. Cette approche de « traçage des contacts numériques » est différente dans chaque scénario, mais le résultat est le même : limiter efficacement une atteinte à la protection des données dès que possible avec des ressources informatiques limitées.

Incidence sur la disponibilité : Au début de la pandémie de COVID-19, Fincharge a pris la décision de mettre hors service ses serveurs pour réduire son exposition aux menaces.

Malheureusement, cette décision a également eu pour effet d'empêcher les utilisateurs légitimes d'accéder à leurs ressources de travail. Par conséquent, l'entreprise a dû faire des pieds et des mains pour distribuer aux employés des ordinateurs portables et des jetons de réseau privé virtuel non testés. Le travail qui se déroulait auparavant à l'intérieur du périmètre du réseau sécurisé devait désormais être effectué à domicile, une situation amenant presque chaque employé à agir comme son propre administrateur de système. Les difficultés liées à la prestation de soutien informatique à divers bureaux à domicile éloignés et les conséquences

de l'interruption des activités sur la productivité ont permis de comprendre à quel point de tels événements malveillants peuvent être perturbateurs.

La transition difficile vers ce modèle « pandémique » inefficace a démontré l'urgence de planifier, de répéter, de former et d'avoir accès à des ressources fiables en un tournemain.

Que s'est-il vraiment passé?

Au premier trimestre de 2020, la pandémie de COVID-19 a obligé Fincharge à interrompre ses activités normales et à fermer ses portes au public.

Dès le début de ces perturbations, le service informatique de Fincharge a pris des mesures clés pour donner la priorité à l'assistance aux utilisateurs, en veillant à ce que le personnel dispose d'un accès sécurisé aux ressources de travail, d'une connexion sûre et de conseils pour les scénarios nécessitant des exceptions, des recherches supplémentaires et une exécution rapide. Dans toute PME, ce travail occuperait une personne à temps plein. Les capacités de l'équipe informatique de Fincharge ont été sollicitées jusqu'à leurs limites.

Conséquences et enseignements

Ces trois situations indépendantes les unes des autres se sont produites à au moins deux mois d'intervalle, ce qui a permis au service informatique de Fincharge de respirer un peu, car chacune d'entre elles a été traitée séparément.

L'entreprise a conclu que le dénominateur commun des trois situations était son faux sentiment de sécurité installé depuis longtemps. Pour façonner son approche en matière de protection des données, l'organisation s'était appuyée sur un modèle de politique de protection des renseignements personnels peu pertinent pour les activités actuelles. Les capacités de surveillance et de détection déjà faibles de l'entreprise laissaient présager des contrôles préventifs inadéquats. Cependant, le succès des actions correctives a été rendu possible grâce aux efforts héroïques de l'équipe informatique.

Une évaluation des risques a révélé que l'entreprise n'était pas, comme prévu, dans le peloton de tête des organisations conscientes des risques. En fait, Fincharge a obtenu une note légèrement inférieure à 2 sur une échelle de 1 à 5.

Modèle de maturité [1 à 5]	Préparation aux risques
1. Efforts héroïques, non structurés et réactifs	Pratiques de sécurité ponctuelles et réactives
2. Mesures propres aux tâches et aux projets	Application de certains contrôles techniques
3. Réponse définie et standardisée de manière proactive	Processus et politiques documentés
4. Programme mesuré, contrôlé et géré	Mesures et preuves systématiques

Modèle de maturité [1 à 5]	Préparation aux risques
5. Amélioration continue et optimisée	Solutions innovantes et optimisées en matière de risques

Cette approche – consistant à mesurer la performance depuis les processus jusqu'aux préparatifs de sécurité – est basée sur le modèle de maturité des capacités, qui est une mesure standard du secteur d'activité. Il s'agit d'un processus qualitatif que toute PME peut suivre dans le cadre d'une autoévaluation. Bien qu'il ne s'agisse pas d'une science exacte, cette approche offre un aperçu utile du degré de préparation de l'entreprise. Lorsqu'ils y ont accès, le CPA et le personnel informatique peuvent se servir d'outils de test de sécurité pour évaluer approximativement leurs résultats sur une échelle de 1 à 5. Avec ces informations, les PME et les organismes à but non lucratif peuvent planifier leurs investissements en matière de sécurité et classer les activités de gestion des risques par ordre de priorité avec plus de confiance et de clarté.

Analyse de l'incident

En bref, les problèmes mis au jour lors de l'attaque par les logiciels malveillants sont issus de la convergence de plusieurs facteurs :

1. **Prévention : contrôles insuffisants pour protéger les utilisateurs contre l'attaque**
   Les organisations qui ont subi des atteintes à la protection des données découvrent souvent que leurs outils de sécurité n'ont pas été correctement configurés ni entretenus. Un faux sentiment de sécurité peut entraver les efforts visant à limiter une atteinte à la sécurité. Dans le cas de Fincharge, les tentatives de structuration d'un ancien programme de sécurité n'étaient pas prioritaires. Si de telles activités avaient eu lieu, le service informatique aurait pu contribuer à accroître la capacité de l'organisation à répondre aux risques.
2. **Détection : manque de cohérence pendant la cyberattaque**
   Plusieurs employés ont remarqué les communications inhabituelles par courriel, mais ne les ont pas signalées sur-le-champ, tandis que d'autres se sont sentis mal à l'aise d'en parler à la direction. Une approche cohérente fondée sur un simple formulaire de signalement servira dorénavant à consigner les incidents dès qu'ils se produisent et à sensibiliser les employés à la situation.

   Un système basé sur les rôles et propre aux types de situations vécues par les employés au sein des différents services doit les aider à surveiller, à détecter et à identifier de manière uniforme les incidents potentiels. Les entreprises devraient utiliser des outils comme un inventaire des actifs et un registre des risques afin de consigner les actifs qui nécessitent une surveillance active pour des motifs de sécurité.

3. **Réaction : manque de communications préparées et de directives claires pour les employés**
   Fincharge a dû rapidement attribuer des rôles fonctionnels aux membres de l'équipe informatique, créer des communications à l'échelle de l'entreprise et prendre des décisions pour contenir la brèche. Il faudrait préparer des mesures réactives, de sorte que les membres de l'équipe soient prêts à accomplir une série de tâches et que les employés sachent qu'ils pourraient recevoir des communications approuvées leur demandant de prendre des mesures bien précises pour leur poste de travail.

L'atteinte à la protection des données subie par le fournisseur de services tiers de Fincharge, EnterTrust, peut être présentée en des termes similaires :

1. **Prévention : les ententes de gestion des niveaux de services devraient inclure l'utilisation de contrôles de sécurité**
   Tout fournisseur de services ayant accès aux données de Fincharge, en particulier aux renseignements personnels, doit accepter de se conformer aux pratiques de transfert et de stockage sécurisés des données. Les informations doivent être chiffrées lors de leur transfert à des personnes déterminées, et Fincharge doit procéder à un examen annuel de ses procédures de sécurité.
2. **Détection : des contrôles doivent être mis en place pour détecter les brèches de données lorsqu'elles se produisent**
   La capacité de détecter et d'identifier les incidents de sécurité subis par des tiers dépend en grande partie de l'efficacité de leurs contrôles de sécurité et de l'application de toute obligation de divulguer cette information à Fincharge. Il faudrait adopter des contrôles de détection et de compensation (c.-à-d. des entrées de base de données exclusives et des activités d'inventaire récurrentes) pour garantir que si ces pratiques ne sont pas suivies, Fincharge en sera informée.
3. **Réaction : la réponse et le signalement doivent suivre immédiatement la détection**
   Pendant la phase de réaction, l'équipe de réponse aux incidents devrait être prête à signaler aux autorités compétentes l'atteinte à la protection des données dès qu'elle est détectée. Une telle mesure contribue à atténuer le risque de réaction négative de la part des personnes concernées relativement à des retards risqués, à des conséquences prévues, à une responsabilité potentielle et à des manquements en matière de conformité.

Ces événements ont donné lieu à un certain nombre d'améliorations en matière de cybersécurité, notamment la création, au sein de l'équipe informatique, d'un sous-groupe spécialement chargé de la cybersécurité défensive. Ce sous-groupe est responsable de la gestion des activités préventives liées à la protection des données, des systèmes et des applications, telles que la gestion des correctifs et la surveillance des événements. Cette protection est un élément fondamental des capacités de Fincharge en matière de gestion des risques liés à l'information.

Les événements de l'année dernière ont démontré la nécessité pour Fincharge de procéder à des tests de sécurité proactifs. Ces exercices comprennent des tests de pénétration visant à mettre au jour des faiblesses inconnues, la recherche de vulnérabilités, des examens des risques, des

évaluations des menaces et des risques, ainsi que des examens de protection des données et de conformité appelés « évaluations des facteurs relatifs à la vie privée ».

Mesures correctives prises

Voici certaines des principales activités qui ont eu lieu chez Fincharge pendant et immédiatement après ces événements :

- sensibiliser les utilisateurs à la bonne façon de signaler les incidents;
- amener les employés à participer aux mesures de sécurité informatique et à les soutenir pour réduire les effets négatifs des incidents;
- apprendre à connaître la situation générale de Fincharge en matière de cybersécurité, de manière à déterminer quelles mesures ponctuelles fonctionnent, quelle documentation existe et quelles compétences d'équipe peuvent être axées sur les activités de défense par rapport aux activités d'enquête concernant la réaction aux incidents.

Fincharge peut améliorer sa situation en matière de cybersécurité en réalisant un inventaire de ses données sensibles, y compris de tous ses lieux de stockage. Il est très risqué pour l'organisation de ne pas savoir où se trouvent les données et quelle est la quantité d'informations stockées en raison du manque d'uniformité dans l'attribution des contrôles et des mesures standardisées visant à déterminer l'efficacité des mesures de sécurité.

Afin de présenter une image plus claire de la bonne gestion des risques liés à l'information, nous avons illustré l'approche globale de Fincharge en fonction de six catégories (ou piliers) de risques :

1. Gestion des actifs : dresser un inventaire et faire une classification des actifs informationnels de Fincharge;
2. Sécurité opérationnelle : améliorer la protection contre les pertes et les fuites de données;
3. Gestion des vulnérabilités : introduire une analyse systématique des vulnérabilités (et évaluer le risque relatif des menaces relevées);
4. Sécurité administrative : présenter la formation sectorielle en cybersécurité à l'ensemble du personnel (en mettant l'accent sur la gestion des incidents et la connaissance de la situation);
5. Gestion de la vie privée : soumettre les processus, les systèmes et les applications qui contiennent des informations sensibles à une évaluation préliminaire des facteurs relatifs à la vie privée;

6. Gestion des risques : sélectionner et tester une police d'assurance cyber-responsabilité appropriée pour Fincharge.

Bien que Fincharge ne possède pas actuellement de documentation détaillée sur ses pratiques et ses configurations, la capacité de l'équipe de sécurité informatique à effectuer les tâches critiques suivantes a permis à l'entreprise de se défendre contre les cyberattaques qu'elle a subies :

- dresser rapidement la liste des systèmes soupçonnés d'être infectés;
- trouver la cause fondamentale de l'infection (c.-à-d. déterminer le « patient zéro » au sein de l'entreprise);
- retirer du réseau les machines soupçonnées d'être infectées;
- inoculer et surveiller temporairement les postes de travail suspects;
- mettre à jour la technologie de filtrage des courriels pour bloquer les attaques par cette voie;
- mettre à jour le filtrage du pare-feu pour empêcher toute communication avec le serveur d'origine;
- effectuer plusieurs couches d'analyse antivirus pour éviter les faux négatifs;
- déployer de nouveaux antimaliciels sur les serveurs;
- tester les logiciels de rançon pour déterminer si les systèmes peuvent les détecter et les arrêter;
- mettre en œuvre des mesures visant à fermer les machines le soir et la fin de semaine afin de réduire les risques.

Cet ensemble de mesures permet d'optimiser l'utilisation du temps et des ressources en période de grande urgence; toutefois, des contrôles systématiques pour l'analyse proactive des réseaux, l'analyse comportementale et la prévention des fuites de données – autant d'éléments qui permettraient d'améliorer grandement la situation sur le plan de la sécurité opérationnelle – font toujours défaut.

Remarque concernant les tests de sécurité fréquents

Au-delà de la mise en œuvre et de la détermination de ces contrôles à plusieurs couches (souvent appelés « défense en profondeur »), il est important de fournir aux parties prenantes l'assurance de l'efficacité du contrôle en effectuant des tests standardisés. L'un des principaux avantages d'une méthodologie de test rigoureuse est sa capacité à produire une image claire de l'ensemble des actifs de l'organisation, qui est nécessaire pour de nombreuses activités opérationnelles, stratégiques et de conformité, y compris la classification des données, la formation de la main-d'œuvre sur la cybersécurité, la budgétisation des investissements informatiques et l'admissibilité à l'assurance cyber-responsabilité.

Résumé

Cette étude de cas sert à rappeler aux professionnels de la comptabilité et aux autres conseillers de confiance que les organisations peuvent compenser un manque de contrôles par un niveau correspondant de sensibilisation et de vigilance des employés.

La nécessité de respecter les règles et de veiller à leur application est fonction des mesures prises pour responsabiliser et éduquer les employés. La meilleure façon d'y parvenir est d'utiliser des statistiques pertinentes, des exemples basés sur des rôles et des possibilités structurées d'apprentissage et d'échange d'informations.

Grâce à la combinaison de mesures de protection harmonieuses, d'un leadership responsable et d'une attention constante portée aux intérêts des parties prenantes, les organisations peuvent bénéficier de la retombée la plus précieuse de leur investissement : la confiance méritée des clients, des partenaires et des employés.

Ressources

Aussi de Claudiu Popa :

- *Guide sur la protection des renseignements personnels et la sécurité des données au Canada* (1re et 2e éd., CPA Canada, 2015)
- *Managing Personal Information for Privacy-Savvy Organizations* (Carswell, 2012)
- *The Canadian Cyberfraud Handbook* (Thomson Reuters, 2017)
- *Tendance technologique : Cybersécurité et protection des données* (CPA Canada, 2019)
- *Tendance technologique : Protégez votre marque et votre réputation sur les médias sociaux* (CPA Canada, 2019)

Autres publications

- CPA Canada, *Lignes directrices sur la comptabilité de gestion – Pour passer des données aux décisions : Les cinq étapes du processus décisionnel fondé sur des données* (2020)
- AICPA, Controls Mapping Documents (2017)
- Industrie Canada, Le cadre de contrôle de CyberSécuritaire Canada (2021)
- NIST, Cybersecurity Framework (2020)
- Centre canadien pour la cybersécurité, En route vers la sécurité d'entreprise (2020)

À propos de l'auteur

Claudiu Popa, CISSP, CIPP, PMP, CISA, CRISC, est un professionnel agréé en sécurité de l'information et protection de la vie privée. Il traite dans les médias de questions comme la gestion des risques d'entreprise, la sécurité informatique et la protection des données. Fort de plus de 25 années d'expérience internationale dans les domaines de l'audit de sécurité, des normes internationales et des services-conseils en matière de risques auprès des conseils d'administration, M. Popa est un conseiller en gestion de confiance pour les entreprises canadiennes et leurs parties prenantes. Il soutient la mise en œuvre de stratégies liées à la sécurité, qui revêtent une importance cruciale, et la prise de décisions portant sur la conformité en matière de sécurité et de respect de la vie privée, la protection des données et la prévention de la cybercriminalité.

Il est l'auteur de quatre ouvrages, de nombreux articles et de multiples publications universitaires sur la protection de l'information, la conformité et la gouvernance des risques, fondés sur la recherche primaire en matière de cybersécurité. En tant que professionnel agréé, M. Popa demeure un ardent défenseur de la sécurité de l'information et un coach d'entreprise de confiance pour les organisations canadiennes qui sont déterminées à améliorer leur sécurité et la protection de leurs clients.

AVERTISSEMENT

La présente publication, préparée par Comptables professionnels agréés du Canada (CPA Canada), fournit des indications ne faisant pas autorité.

CPA Canada et l'auteur déclinent toute responsabilité ou obligation pouvant découler, directement ou indirectement, de l'utilisation ou de l'application de cette publication.