Fraudcast : histoires de tromperies et de trahisons

Épisode 7 : La question des rançongiciels

Jazz Clemente

Bonjour et merci d'écouter le balado Fraudcast de KPMG au cours duquel nous discutons des cas de fraude qui font la une de l'actualité pour comprendre ce qui s'est passé et en tirer des leçons. Je m'appelle Jazz Clemente.

Frédéric LeBlond

Et je suis Frédéric LeBlond.

Jazz Clemente

Nous sommes tous deux conseillers principaux au sein du groupe Juricomptabilité de KPMG au Canada.

Frédéric LeBlond

Les histoires dont il sera question dans cette série sont des cas réels, mais les noms ont été changés pour protéger pour la vie privée de toutes les personnes concernées. Bien que KPMG n'a pas travaillé sur ces affaires en particulier, nous nous penchons souvent sur des cas semblables à ceux dont il est question ici et qui sont connus du public.

Jazz Clemente

Dans cet épisode, nous présenterons des histoires décrivant ce qui se déroule lorsqu'un groupe de personnes qualifiées détient en otage des informations sensibles de l'entreprise au moyen d'un rançongiciel.

Tout d'abord, nous discuterons du cas d'une petite ville de l'Ontario qui a dépensé plus de 1,3 million de dollars pour enquêter sur un incident de cybersécurité et y réagir. Des fichiers et des serveurs ont été chiffrés dans une attaque impliquant le rançongiciel tristement célèbre LockBit 3.0. En plus de cette dépense, la Ville a également payé une rançon de près de 300 000 $ pour obtenir des clés de déchiffrement sur recommandation d'un cabinet tiers retenu par la ville, engagé pour l'aider à traverser l'incident.

Frédéric LeBlond

Waouh, donc ils ont payé la rançon? Je ne m'y attendais pas!

Jazz Clemente

Cela a dû être une décision difficile à prendre.

L'attaque par rançongiciel a d'abord été découverte par du personnel des TI de la Ville qui effectuait une sauvegarde routinière du système. Quand le personnel s'est rendu compte de l'attaque, il a rapidement débranché tous les serveurs, ce qui a permis d'éviter que d'autres systèmes ne soient touchés. En raison des actions rapides de l'équipe informatique, le rançongiciel n'a pas entièrement crypté tous les systèmes de la Ville. Aucun des services essentiels de la Ville n'a été touché. Deux cabinets externes ont été appelés au renfort. L'un agissait à titre de responsable technique et d'auditeur juricomptable de la Ville et l'autre, à titre de directeur de l'intervention face à l'incident. Il a été initialement noté que le portail du Web clandestin de LockBit affirmait qu'au moins 67 gigaoctets de données avaient été volés à la Ville, y compris des données confidentielles et des documents financiers. La Ville avait jusqu'à une semaine pour payer une rançon, ou les données seraient publiées.

Frédéric LeBlond

Donc d'abord ils volent vos données et vous font payer pour les récupérer, mais vous ne savez même pas s'ils honoreront cette promesse ou s'ils vous feront du chantage pour profiter de vous de nouveau? C'est trop.

Jazz Clemente

En effet. C'est une tactique connue sous le nom de « double extorsion ». On ne sait pas exactement ce que recherchaient à l'origine les personnes impliquées dans l'attaque. En fin de compte, la Ville a opté pour le maintien d'un négociateur tiers afin d'obtenir une rançon en échange des clés de déchiffrement pour débloquer les données.

Selon le rapport, une rançon équivalente à 200 000 dollars américains, ou environ 290 000 dollars canadiens, en bitcoins a été payée. Questionné à ce sujet, le maire de la Ville a dit que c'était une décision difficile à prendre, mais que c'était la recommandation des experts qui ont été engagés. Il a ajouté qu'il n'existe pas de guide pratique sur la façon de traiter chaque cas, car les circonstances varient chaque fois.

Frédéric LeBlond

Je pense que je comprends cette approche. Considérons la situation sous un autre angle : en tant qu'organisation, on se demande certainement combien les données valent. Peut-être que 290 000 $ est un faible coût par rapport à celui de tout reconstruire. Je comprends cela. J'espère que c'était la bonne décision, en fin de compte.

Jazz Clemente

Le cabinet externe embauché a entrepris la conception et la reconstruction d'un nouveau réseau informatique pour la Ville. La Ville a suivi les lignes directrices et les recommandations des deux cabinets et a fait appel à un tiers pour surveiller les systèmes de façon continue. On ignore si la Ville a été ciblée intentionnellement. La plupart des attaques par rançongiciel sont perpétrées au hasard par l'intermédiaire de liens malveillants et de courriels d'hameçonnage, de profils de compétence compromis ou de vulnérabilités non corrigées sur les réseaux Internet. Les détails de l'attaque en elle-même sont encore inconnus, y compris la façon dont LockBit s'est introduit dans le réseau de la Ville, le nombre de dossiers pris et la possibilité que des données sensibles sur le personnel ou les résidents aient été volées.

Frédéric LeBlond

Jazz, je suis vraiment curieux. Peux-tu nous expliquer ce qu'est LockBit?

Jazz Clemente

Certainement. LockBit est à la fois un groupe de cyberattaques et le logiciel malveillant que ce groupe utilise pour mener des attaques criminelles. LockBit, en tant que groupe, fonctionne comme une entreprise de rançongiciel en tant que service (RaaS), où les équipes développent un maliciel qui est autorisé aux réseaux affiliés, qui l'utilisent ensuite pour mener des attaques, selon le directeur de l'innovation et des politiques dans une université canadienne. Selon le site web d'une société de logiciels de sécurité bien connue, le maliciel de LockBit infiltre ses réseaux cibles à travers des vulnérabilités non corrigées, d'accès d'initiés et des exploitations du jour zéro.

Frédéric LeBlond

Que sont les exploitations du jour zéro?

Jazz Clemente

Des attaques au cours desquelles les pirates tirent parti de défauts dans un logiciel qu'ils ont découverts avant que l'entreprise qui a créé le logiciel ne se rende compte du problème, ce qui lui donne « zéro jour » pour le résoudre. LockBit est alors en mesure de prendre le contrôle du système d'une victime, de recueillir des renseignements sur le réseau et de voler ou de chiffrer des données. Les attaques LockBit présentent généralement une tactique de double extorsion. Tout d'abord, LockBit encourage les victimes à payer pour retrouver l'accès à leurs fichiers chiffrés. On demande ensuite aux victimes de payer à nouveau pour empêcher que leurs données volées ne soient publiées.

Frédéric LeBlond

Ça a l'air horrible. À quel point LockBit est-il prolifique, en fait?

Jazz Clemente

LockBit a fait plus de 100 millions de dollars en demandes de rançon et extrait des dizaines de millions de dollars en paiements des victimes, selon un document de justice déposé dans un des États américains contre un membre présumé de LockBit. LockBit est apparu dès janvier 2020, et depuis, au moins 1 000 attaques ont été perpétrées à travers le monde.

Frédéric LeBlond

Savons-nous qui est derrière LockBit?

Jazz Clemente

Dur à dire, car ils opèrent dans un grand secret. Les membres de LockBit pourraient être situés n'importe où dans le monde. Deux des plus grandes victimes de LockBit au Canada seraient un hôpital et une librairie, ce qui nous mène à nos prochaines histoires.

Un hôpital dit qu'il n'a pas utilisé la clé de déchiffrement gratuite offerte par LockBit et n'a pas payé de rançon après une attaque de rançongiciel par le groupe.

Frédéric LeBlond

Quelle décision audacieuse!

Jazz Clemente

La cyberattaque a retardé les résultats de laboratoire et d'imagerie, a coupé les lignes téléphoniques et fermé le système de paie du personnel de l'hôpital. L'hôpital fonctionnait sous un code gris, ce qui signifie qu'il y a des défaillances dans le système, en réponse à la cyberattaque. Au moment présent, l'hôpital a indiqué qu'environ 80 % de ses systèmes prioritaires étaient rétablis après qu'une attaque par rançongiciel ait eu une incidence sur ses activités. Selon le président et chef de la direction, la cyberattaque a été traitée relativement rapidement, avec des perturbations minimales pour les patients et les familles. LockBit, l'un des groupes de rançongiciels les plus actifs et les plus destructeurs au monde, a publié de brèves excuses et offert à l'hôpital une clé de déchiffrement gratuite pour déverrouiller ses données. Selon les experts en cybersécurité, cette démarche est rare, voire sans précédent, pour le groupe tristement célèbre. Dans la déclaration du groupe, LockBit a prétendu avoir bloqué un associé responsable de l'attaque et a offert à l'hôpital une clé de déchiffrement gratuite pour déverrouiller ses données.

Même si l'hôpital décidait d'utiliser la clé de LockBit, les experts disent qu'il ferait encore face à un certain nombre d'obstacles. Les groupes de rançongiciels sont bons pour mélanger des fichiers, mais pas pour les démêler, selon un chercheur d'un cabinet de cybersécurité. Les organisations de soins de santé qui utilisent la clé d'un groupe de rançongiciels récupèrent en moyenne les deux tiers de leurs dossiers, selon un sondage auprès de centaines d'organisations. Le travail complexe de déchiffrement est également laissé à l'organisation elle-même. Pour l'hôpital, une question reste sans réponse concernant l'associé de LockBit. Le communiqué de LockBit indique que l'associé qui a attaqué l'hôpital ne fait plus partie de son programme, mais on ignore s'il détient toujours des fichiers volés. L'hôpital affirme que, jusqu'à présent, rien ne prouve que des renseignements personnels aient été compromis. Les excuses de LockBit semblent être une façon de gérer son image, car certains associés pourraient voir l'attaque d'un hôpital comme un pas de trop.

Frédéric LeBlond

D'accord, je sais que l'idée qu'un cybercriminel fasse des excuses semble un peu bizarre, mais j'ai une théorie là-dessus, à savoir pourquoi ils se soucient même de leur image. Je pourrais me tromper, mais j'ai l'impression que LockBit pourrait être un de ces groupes qui croient être en position de force sur le plan moral et qui ne ciblent que des groupes dans lesquels ils trouvent des défauts. Je pense qu'ils réalisent toutefois que nuire indirectement aux gens les plus vulnérables dépasse certainement les bornes. Personne n'aime les cybercriminels, mais je peux imaginer à quel point les gens pourraient être plus impliqués et déterminés à les arrêter s'ils continuaient à agir de la sorte. Ces groupes ne cherchent donc pas à polir leur image; ils veulent plutôt minimiser leurs risques. Heureux de voir qu'ils ont un certain sens de l'éthique.

Jazz Clemente

Ensuite, nous avons l'histoire de la façon dont une librairie canadienne a été touchée par une attaque impliquant LockBit. Ladite librairie refusait les demandes de paiement d'un groupe en ligne revendiquant son affiliation au site de rançongiciel LockBit en raison du risque de financement du terrorisme.

Frédéric LeBlond

Encore une fois, quelle audace. La librairie montre clairement ses valeurs. De plus, le risque de financement du terrorisme est très réel ici. Comme tu l'as mentionné précédemment, Jazz, LockBit est un rançongiciel en tant que service. Cela signifie que le groupe a des clients. Je ne sais pas pour toi, mais les organisations terroristes sont certainement en tête de la liste de groupes auxquels je pense qui demanderait ces services pour se remplir les poches. Il se peut également qu'un groupe revendique ce genre d'affiliation pour intimider les victimes. Ça s'est déjà vu. Ça pourrait aider LockBit à paraître plus menaçant qu'il ne l'est réellement.

Jazz Clemente

Le groupe de pirates a menacé de publier toutes les informations volées et a affiché un compte à rebours sur plusieurs versions du forum de LockBit sur le Web clandestin. À la fin du compte à rebours, le forum LockBit a déclaré que les données avaient été publiées. Toutefois, ni les journalistes ni l'analyste indépendant de la sécurité n'ont pu trouver les données fuitées. Selon un défenseur de la protection des renseignements personnels et un analyste de la cybersécurité, cela ne signifie pas qu'il y a moins de risques pour les Canadiens touchés par cette atteinte à la protection des données. Cela ne veut certainement pas dire que les données ne seront pas publiées à l'avenir. Certaines

données sur les employés ont été volées dans l'attaque de rançongiciel, dit maintenant la librairie. De nombreux travailleurs actuels et anciens s'inquiètent de ce qui se passerait si des renseignements comme leur adresse courriel, leur adresse domiciliaire, leur numéro d'assurance sociale et leurs coordonnées bancaires étaient rendus publics. La librairie offre depuis deux ans un service de protection du crédit à certains employés actuels et anciens. Elle a affirmé qu'elle continuerait de répondre aux préoccupations qui pourraient apparaître.

La librairie a déjà dit qu'elle ne connaissait pas l'identité du groupe derrière l'attaque. Lorsque la cyberattaque a frappé la librairie, son site web s'est entièrement déconnecté et les magasins physiques de la chaîne n'ont pas pu traiter les transactions par carte de crédit, carte de débit ou carte-cadeau. Les magasins physiques avaient rouvert leurs portes le week-end suivant. Le site a repris graduellement ses activités transactionnelles peu après. Être touché par une attaque par rançongiciel est vraiment dévastateur. Chaque scénario est unique et il n'y a aucune instruction universelle pour répondre aux attaques. Il faut absolument prendre des mesures de prévention et avoir la capacité de détecter toute menace et de réagir rapidement, au besoin.

Jazz Clemente

Paul Sammut, associé au sein du groupe Cybersécurité de KPMG à Ottawa, sera notre invité spécial aujourd'hui. Paul compte plus de 22 ans d'expérience en technologies et en sécurité de l'information. Il offre des services-conseils en certification à des clients de divers secteurs, dont ceux de la technologie, des services financiers, des télécommunications, des marchés de consommation et des organismes sans but lucratif. Paul dirige l'équipe de cybersécurité de la région Est de KPMG au Canada et travaille à Ottawa depuis 2018, après avoir passé sept ans chez KPMG au Royaume-Uni. Il est également un leader mondial en matière d'ISO 27001, la norme internationale de gestion de la sécurité de l'information.

Paul Sammut

Bonjour Jazz! Merci pour la présentation. Je suis heureux d'être avec vous.

Jazz Clemente

Voici notre première question : quelle devrait être la réponse initiale une fois que l'on a découvert que son entreprise a été victime d'une attaque par rançongiciel?

Paul Sammut

Eh bien, la première réaction que nous voyons généralement chez les organisations est une sorte de choc, de panique et d'incrédulité; on peine à croire que sa propre organisation a été ciblée. Ces premières heures de découverte sont souvent le moment le plus critique où une attaque par rançongiciel se produit. Je m'adresse aux auditeurs : si vous n'avez jamais été victimes de ce genre d'attaque, sachez qu'il y a quelques mesures que vous pouvez prendre pour mieux préparer votre organisation.

Tout d'abord, il est préférable de prévoir une provision sur honoraires d'intervention en cas d'incident, ce qui signifie que des experts sur appel 24/7 peuvent vous répondre en moins d'une heure, fera une énorme différence. Si vous pensez que votre organisation est frappée par un rançongiciel, pouvoir communiquer avec quelqu'un qui a déjà traité ce genre de situations avant, régulièrement, qui a la capacité d'accéder à vos systèmes et de vérifier si l'attaquant est toujours sur vos systèmes, et qui saura vous aider tout au long du processus fait une si grande différence en ces temps de panique et de scénario catastrophe. Les experts peuvent aussi aider à assurer la liaison avec un conseiller en cas d'intrusion, c'est-à-dire un avocat qui a de l'expérience dans les négociations de rançon.

Deuxièmement, il faut tester votre intervention lors d'un exercice de simulation. Cela fait en sorte qu'en cas d'attaque, votre équipe de gestion de crise connaît son rôle, vous savez déjà combien de temps il faut pour récupérer vos sauvegardes et vous avez des idées pour traiter vos communications internes, et externes si votre entreprise faisait les manchettes, par exemple. Faire ce genre d'exercice, à la façon d'un exercice d'incendie, vous place dans une bien meilleure position pour gérer une attaque par rançongiciel et aide à atténuer son impact.

Jazz Clemente

Y a-t-il des secteurs ou des types d'entreprises qui sont plus susceptibles d'être visés par une attaque par rançongiciel?

Paul Sammut

Actuellement, les attaquants ciblent des organisations moins matures, qui ont moins investi dans la cybersécurité et dans leur technologie tout simplement parce que ce sont des cibles vulnérables. En fait, Microsoft a publié son rapport sur la cyberdéfense le mois dernier, en octobre 2023, et l'une des statistiques y figurant est que 70 % des organisations qui ont rencontré des rançongiciels opérés par des humains

avaient moins de 500 employés. Il s'agissait évidemment d'organisations de petite ou moyenne taille, et quand on y pense, il est beaucoup plus facile pour un attaquant de cibler une organisation de cette taille qui emploie probablement une ou deux personnes à la sécurité, par opposition à une banque qui peut compter 100 ou 200 employés qui protègent l'organisation.

L'année dernière, là où je travaille en Ontario, l'un des deux secteurs les plus ciblés était la fabrication. En général, ce sont des organisations de plus petite taille qui n'emploient que quelques personnes à la sécurité informatique, et qui dépendent également de ces systèmes pour être en mesure de poursuivre leurs processus de fabrication. Une attaque par rançongiciel, par exemple, peut avoir un effet dévastateur, entraîner la perte de semaines de production et causer des perturbations majeures. C'est certainement l'un des secteurs les plus touchés, en partie parce que les entreprises sont généralement moins matures dans leur technologie. Malheureusement, le deuxième secteur le plus visé est les soins de santé et les hôpitaux. Jazz, tu as mentionné quelques exemples plus tôt et nous avons vu un certain nombre de cas très médiatisés d'attaque par rançongiciel, qui peuvent avoir des effets dévastateurs sur un hôpital, comme la fermeture des services d'urgence, l'annulation des rendez-vous chirurgicaux et la fermeture des salles. Un certain nombre d'hôpitaux ont été frappés et ces histoires font les manchettes à cause des perturbations et de l'importance des services qu'ils fournissent. Des attaques de ce genre peuvent avoir un impact très grave sur la vie quotidienne des gens.

Jazz Clemente

Est-ce une bonne idée de payer la rançon aux attaquants afin d'accéder à nos systèmes ou de déchiffrer des données et des fichiers?

Paul Sammut

Eh bien, c'est la question à un million de dollars ou, parfois, à plusieurs millions de dollars. Quand je fais des présentations à des conférences et des séminaires, c'est souvent l'une des premières questions qu'on me pose. Il y a un certain nombre de questions et de considérations éthiques en jeu aussi. En règle générale, quand on paie la rançon, on perpétue le modèle d'affaires du rançongiciel. Si personne ne payait jamais de rançon à la suite d'une attaque par rançongiciel, les attaquants cesseraient rapidement de le faire. De plus, on ne sait pas où va l'argent; il peut servir à financer d'autres activités liées au crime organisé, d'autres attaques par rançongiciel, comme le trafic humain ou le terrorisme. C'est une véritable considération quand vient le temps de payer un demi-million ou un million de dollars à des cybercriminels. Toutefois, la décision d'affaires peut se baser sur la comparaison entre le coût, le risque et les avantages.

Dans le cas d'un hôpital, on fait face à un scénario de vie ou de mort parce qu'il s'agit de maintenir les services et les activités. Maintenant, il faut en discuter en tant qu'organisation, donc avec l'équipe de direction et le conseil d'administration, dans le but de déterminer d'avance qui serait responsable d'autoriser une décision de payer une rançon, de savoir quelles approbations internes il faudrait et de vérifier s'il existe une politique générale de non-paiement, par exemple. Mais il existe d'autres considérations. On peut se demander si l'on veut payer la rançon et obtenir les clés de déchiffrement pour récupérer les données, si cela fonctionne vraiment. En général, les organisations croient qu'elles récupéreront leurs données; autrement, pourquoi payer la rançon? Cependant, nous avons vu des scénarios catastrophiques où les organisations ont payé la rançon, mais n'ont jamais récupéré leurs données. Elles ont dû reconstruire complètement leur environnement. C'est le genre de situation dans laquelle on ne veut pas risquer de se retrouver.

Jazz Clemente

Que peuvent faire les entreprises pour éviter d'être victimes d'une attaque par rançongiciel?

Paul Sammut

Excellente question. D'abord, il faut avoir de bonnes pratiques de sécurité informatique, ce qui peut au moins réduire la probabilité d'une attaque par rançongiciel, mais si votre organisation est touchée, cela peut atténuer les répercussions. L'une des choses les plus importantes est de corriger les vulnérabilités de vos systèmes. Tenir vos serveurs informatiques à jour. Tout ce qui n'est pas à jour est potentiellement exploitable par un attaquant qui cherche à obtenir un accès supplémentaire. Nous avons vu des cas où les organisations tenaient à jour la grande majorité de leurs systèmes, mais avaient oublié de corriger un serveur, ou tardé à déployer les correctifs, et c'était la seule porte d'entrée dont un attaquant a eu besoin pour accéder à leur réseau et déclencher le rançongiciel.

Ensuite, on doit investir dans la surveillance active, que ce soit par l'entremise de sa propre équipe informatique ou d'un

fournisseur de services qui surveille les systèmes à la recherche d'activités suspectes et de signes potentiels d'intrusion. Ce qui passe habituellement dans les attaques par rançongiciel est que l'attaquant obtient l'accès à l'environnement, puis effectue une reconnaissance, en apprend sur le réseau et la façon dont l'entreprise fonctionne, et attend le meilleur moment pour déployer le rançongiciel afin de provoquer une perturbation et une panique maximale. Si votre organisation surveille de façon proactive les comportements suspects, alors vous avez la meilleure chance de détecter l'attaquant, peut-être même avant qu'il ait la chance de déployer le rançongiciel, ce qui serait le scénario idéal.

J'ajoute trois éléments à considérer. Il faut effectuer régulièrement des tests de pénétration des systèmes. Il s'agit de permettre à un fournisseur de services externes de tester vos systèmes, de chercher des façons de les exploiter ou de les compromettre, en particulier vos systèmes externes, comme le service de RPV, qui sont souvent des moyens d'accéder à votre réseau et à votre environnement; il est donc primordial de les tester. Il faut aussi faire des tests d'hameçonnage. Souvent, un attaquant obtient l'accès par un courriel d'hameçonnage très ciblé qui vise un employé en particulier, par exemple en les faisant cliquer sur un lien et fournir leurs identifiants de connexion. Quand vous effectuez des tests réels sur vos employés, idéalement chaque mois, ceux-ci deviennent plus vigilants face aux attaques par hameçonnage parce qu'ils ne veulent pas échouer à vos propres tests. Ils font généralement plus attention quand des courriels d'hameçonnage potentiels arrivent et la sensibilisation s'en trouve grandement améliorée.

Enfin, faites un exercice de simulation. Comme je l'ai mentionné plus tôt, cela peut vraiment réduire l'incidence d'une attaque et mieux préparer votre personnel. Nous faisons tous des exercices au cas où un incendie se produisait, mais de nos jours, nous avons plus de probabilités de vivre une attaque par rançongiciel qu'un incendie. Les organisations devraient s'y préparer, car cela pourrait avoir une incidence dévastatrice sur leurs activités.

Jazz Clemente

J'ai une dernière question. Étant donné le risque d'attaques par rançongiciel et les exigences et la réglementation en matière de confidentialité, qu'est-ce que les organisations doivent savoir aujourd'hui?

Paul Sammut

Il est certain qu'au Canada, la grande chose à savoir est la Loi 25, qui provient du Québec et dont les plus récentes dispositions sont entrées en vigueur récemment. Elle véhicule un principe général de transparence par rapport à la façon dont une organisation s'occupe des informations de ses clients, donc leurs renseignements personnels. Avez-vous entendu parler du « RGPD », qui est le règlement général de l'UE sur la protection des données? La Loi 25 s'aligne beaucoup sur ce dernier. Elle nous protège beaucoup plus en tant que consommateurs, mais il est important pour les entreprises de s'assurer qu'elles se conforment elles aussi à la Loi et qu'elles protègent les données de leurs clients de la façon prescrite par la loi. L'un des grands principes est que, si une personne consent à partager ses renseignements personnels avec vous en tant qu'organisation, elle peut consentir à une fin particulière, et c'est à vous en tant qu'organisation de veiller à ce que le consentement soit géré en fonction de la façon dont ces données seront utilisées, communiquées et possiblement partagées avec des tiers.

Les organisations doivent faire très attention aux données sur les consommateurs qu'elles détiennent, surtout au Québec, évidemment, à leur utilisation et au consentement qui les accompagne. Ils doivent également savoir que ce consentement peut être retiré par les consommateurs qui ne veulent plus que votre organisation détienne leurs données personnelles. Il est vraiment essentiel de mettre en place des pratiques bien définies. Avec la Loi 25, nous nous attendons à ce que les organisations qui ne s'y conforment pas ou qui utilisent les données de leurs clients à mauvais escient se voient imposer de très lourdes amendes. Vous ne voulez pas ignorer ce genre de chose, et vous devez vraiment être proactifs maintenant que c'est une loi au Québec. Nous nous attendons à ce que d'autres provinces canadiennes emboîtent le pas au Québec. C'est vraiment important d'agir de façon proactive.

Jazz Clemente

Merci beaucoup pour ton temps et pour toutes ces informations précieuses, Paul.

Paul Sammut

Merci de m'avoir invité, Jazz.

Frédéric LeBlond

Nous aimerions lors de chacun de nos épisodes vous proposer des conseils pour mieux vous sensibiliser à la

fraude. Voici Jazz avec notre stratagème de fraude de la semaine, le rançongiciel.

Jazz Clemente

Les rançongiciels continuent de faire les manchettes, et on en voit de plus en plus dans les médias. C'est vraiment effrayant et stressant que tous vos fichiers et données soient chiffrés jusqu'à ce que vous payiez une rançon. Un rançongiciel est un logiciel malveillant qui prend en otage des fichiers d'un ordinateur ou d'un réseau, empêchant son utilisateur d'y avoir accès à moins de verser une rançon. Il ne fait donc pas partie de la même catégorie de maliciel qu'un virus. Les premières variantes de rançongiciels exigeaient que les paiements soient envoyés par courrier. Aujourd'hui, les auteurs de rançongiciels exigent que les paiements soient versés en cryptomonnaie ou par carte de crédit. Les attaquants ciblent des individus, des entreprises et des organisations de toutes sortes. Certains auteurs de rançongiciels vendent même le service à d'autres criminels, ce qu'on appelle le rançongiciel en tant que service.

Frédéric LeBlond

Comment pouvons-nous gérer cela?

Jazz Clemente

La meilleure façon d'éviter d'être exposé à un rançongiciel ou à un maliciel en général, en tant qu'utilisateur, est de faire preuve de prudence. Faites attention à ce que vous téléchargez sur votre ordinateur ou votre téléphone. D'autres moyens s'offrent à vous pour vous protéger; mentionnons la mise à jour des systèmes d'exploitation, des logiciels et des applications, la mise à jour automatique et le contrôle régulier des logiciels antivirus et des antimaliciels ainsi que la sauvegarde régulière des données et la vérification que ces sauvegardes ont bien été complétées. Enfin, il faut sécuriser les sauvegardes et créer un plan de continuité au cas où l'entreprise ou l'organisation serait victime d'une attaque par rançongiciel.

Frédéric LeBlond

Les professionnels en juricomptabilité chez KPMG transforment la façon dont les clients cernent et atténuent les risques et économisent temps et argent. Nous aidons les particuliers et les organisations à se tenir au fait de la fraude, et nous serions ravis de vous aider. Au nom de toute l'équipe de Juricomptabilité de KPMG au Canada, je vous remercie d'avoir écouté cet épisode du balado Fraudcast de KPMG.

Jazz Clemente

Nous espérons vous retrouver bientôt.