Pour l'avenir : Un balado de KPMG sur la cybersécurité

Série 1 : Destination : Identité numérique

Épisode 2 : La sécurité

Erik Berg

[extrait]

Jadis, le voleur de banque mettait sa vie en jeu. Le risque était élevé, la récompense aussi. Aujourd'hui, il est dans son sous-sol et joue au pirate pour s'amuser. Parce que c'est non seulement très lucratif, mais aussi relativement facile.

Yassir Bellout

[extrait]

Il est important de comprendre que l'identité numérique n'est pas une solution magique qui fera disparaître la cybercriminalité.

Narrateur :

Nos cartes d'identité, nos actifs et nos renseignements personnels sont des biens inestimables. Ils nous permettent d'accéder à des services, valident notre historique et prouvent qui nous sommes.

Et si elles tombent entre les mauvaises mains, les conséquences peuvent être terribles.

SFX – Fondu de la chanson thème

Hartaj Nijjar

Pour l'avenir, un balado sur la cybersécurité pour outiller les entreprises aujourd'hui, demain et pour l'avenir.

Je m'appelle Hartaj Nijjar et je suis le leader national du groupe Cybersécurité de KPMG au Canada.

Voyons ensemble comment les entreprises et les Canadiens peuvent collaborer pour protéger ce qui compte le plus dans un avenir axé sur le numérique.

SFX – Chanson thème en crescendo

Narrateur :

Et je suis Tamara Stanners, votre hôte. Merci de vous joindre à nous pour ce deuxième épisode de notre série de baladodiffusions intitulée Destination : Identité numérique

Aujourd'hui, nous naviguerons dans le paysage périlleux du vol d'identité, de la fraude et de la cybercriminalité. Nous verrons qui pourrait tirer profit de nos renseignements personnels et la façon dont nous pouvons travailler ensemble pour assurer la sécurité de nos actifs d'identité personnelle.

Cela peut sembler évident, mais réfléchissons un instant : **Pourquoi** est-il vital de protéger notre identité?

Erik Berg

L'identité doit être protégée parce qu'elle la source de vérité. Elle prouve que vous êtes bien qui vous affirmez être.

Narrateur :

Erik Berg, spécialiste en risque technologique chez KPMG, nous fait part de ses impressions.

Erik Berg

En accédant aux renseignements d'identité d'une personne, quelqu'un peut causer des préjudices graves, comme le vol et la fraude d'identité, la création de documents frauduleux, de passeports, de permis de conduire; la liste est longue. Cela peut nuire à votre cote de crédit, à votre dette fiscale, à votre casier judiciaire, et surtout, il y a les dommages émotionnels pour les victimes, en plus du temps qu'il faut pour réparer les dégâts à la réputation et au crédit.

Imaginez que vous mettez votre maison en vente et vous vous découvrez qu'il y a un prêt sur votre propriété, de sorte que vous ne pouvez pas la vendre. En essayant de comprendre ce qui s'est passé, vous apprenez que quelqu'un a utilisé votre identité à votre insu pour obtenir une hypothèque sur votre maison.

Narrateur :

Et ce n'est qu'un des nombreux scénarios possibles des conséquences que pourraient avoir un vol d'identité ou la perte de renseignements pouvant identifier une personne (PII) sur n'importe qui d'entre nous.

Personne n'est à l'abri.

Il est important de noter que la cybercriminalité est un crime. Et comme dans toute affaire criminelle, il y a des victimes et des fraudeurs. Alors, qui sont ces cyberfraudeurs? Quel est leur motif?

Erik Berg

There are many different types of bad actors out there, and they all have different motivations. So the first and foremost motivation for many cyber criminals is financial. So identifying, um, the easiest way between their hack and, um, monetizing the hack is, is critical for them. So there is, um, ways of, of

monetizing their hack on, on the dark web, typically records, credit card information, healthcare information. It can be sold for hundreds, if not thousands of dollars. And many times hacks include hundreds if not thousands of records at a time. So it's very, very profitable.

There are also political motivations or "hacktivism" as we refer to it, as where they want to promote or, um, uh, promote the interest of their ideology or to make something happen for an interested party.

Revenge, typically internal threats, uh, include attacking with the intent to harm as a payback.

So we talked about motivations and let's just briefly talk of about, uh, ways in which, uh, access to, uh, um, information is obtained.

So there are many different ways of gaining access. So through the dark web, uh, it's as easy as actually just purchasing credit card information or healthcare records on the dark web and buying exploit kits where you can exploit systems. Uh, social engineering is also one of the easiest ways to gather sensitive information.

So one of the key takeaways is it's much easier than, than people think. So bank robbers before used to put their life on the line, um, robbing banks, and it was high risk, high reward. It has now shifted to someone being in their basement, uh, uh, hacking for fun because it's very lucrative and relatively easy to do.

Narrateur :
Les fraudeurs sont souvent dépeints comme des personnages mystérieux sans visage, cachés derrière un mur d'écrans, mais la plupart du temps, ce n'est pas le cas. Avec le changement de paradigme du risque et de la récompense, un cybercriminel peut être n'importe qui. Cela pourrait être votre voisin, votre chauffeur de taxi...ou peut-être même quelqu'un avec qui vous êtes allé à l'université.

Dramatisation 2.1 - Café avec un pirate

FONDU :

SFX - Tim Hortons très occupé. Des clients et des caissiers qui passent des commandes.

EMPLOYÉ DE TIM HORTONS
2 moyens, une rosette et un beigne aux pommes.

PIRATE
Merci

SFX - Elle prend les cafés et la nourriture et se dirige vers une table en passant près d'autres clients.

Elle s'assoit à une table avec un homme, lui donne un café et le sac contenant un beigne.

PIRATE
Tiens, ton café et ton beigne.

AMI (POURSUIT LA CONVERSATION ENTAMÉE PLUS TÔT)
Merci. Alors si je comprends bien, ton petit ami de l'UdeM est un pirate et tu t'y es mise aussi après avoir reçu ton diplôme?

SFX - Elle prend une gorgée de son café. Il déballe son beigne, prend une bouchée.

PIRATE (NONCHALAMMENT)
Oui. J'ai toujours été naturellement très douée pour coder et bâtir des programmes, donc ça m'est venu facilement.

Honnêtement, c'est beaucoup plus facile que ce que pensent la plupart des gens.

AMI (ABASOURDI)
Wow… (pause)donc, tu es vraiment un pirate hein? Honnêtement, j'imaginais plutôt un personnage sans visage dans un chandail à capuche.

PIRATE (RIRES)
Eh bien, j'en ai quelques-uns.

AMI
(rires)

Non, mais sérieusement.

Comment ça fonctionne exactement, que fais-tu?

PIRATE
Ok, j'essaie de t'expliquer.

SFX – Elle prend une bouchée de beigne et perd le fil pendant un instant.

Ils sont si bons!

Bon. Penses-y comme dans le monde physique. Tu as ta maison. Elle contient tous tes objets de valeur. Et il y a toujours une chance que quelqu'un essaie d'entrer chez toi pour les voler.

Alors que fais-tu? Tu fermes les portes à clé.

SFX – On entend les bruits ambiants tout au long de la scène.

Mais certaines personnes, eh bien, elles laissent des portes ouvertes. C'est là que j'entre en jeu : je vais de maison en maison pour les chercher.

SFX - Prend une gorgée de café.

J'utilise rarement la porte d'entrée. Trop évident. Mais la porte arrière ou une fenêtre, ça pourrait être une ouverture. Et si j'entre par là, il y a même une chance que personne ne le remarque.

Bien sûr, il y a des maisons qui ont des systèmes de sécurité. C'est la première chose que je vérifie. C'est trop risqué d'entrer dans une maison qui a une alarme, alors je les évite la plupart du temps.

Mais parfois (et tu serais surpris de voir combien de fois!), il n'y a pas de système de sécurité et une des portes ou des fenêtres n'est pas verrouillée. C'est alors que j'entre et que je recueille autant de données que possible. Ensuite, j'en fais ce que je veux. La plupart du temps, je les mets aux enchères pour les vendre au plus offrant.

AMI
C'est aussi simple que ça...

(pause, prend un verre de café)

Ça m'incite à renforcer la sécurité de ma maison.

(rit nerveusement)

Fin de la scène.

Narrateur :
Vous - Vérifiez que votre porte est verrouillée.

Société de sécurité – Installation d'un système d'alarme dans votre maison.

Votre voisin – Surveille votre maison pendant votre absence.

Police – Vient à votre secours s'il y a un soupçon d'intrusion.

Pour protéger une maison, il faut tout un village. Quand il s'agit de votre identité, cette responsabilité est également partagée.

Erik Berg
Dans ce paradigme où nous avons des fraudeurs, nous avons aussi des protecteurs, c'est-à-dire des gens qui travaillent sans relâche pour protéger les renseignements personnels.

En fin de compte, protéger l'identité, c'est la responsabilité de chacun, que ce soit des gouvernements, des entreprises ou des consommateurs – tout le monde a un rôle et tout le monde a sa place.

Le consommateur est responsable de la protection de son identité et aussi à qui il fournit des renseignements.

Une fois qu'une autre partie détient vos renseignements personnels, vous devez lui faire confiance un peu à l'aveugle et espérer qu'ils sont correctement stockés et sécurisés.

Ainsi, lorsque vous partagez des renseignements personnels identifiables avec des entreprises, vous vous attendez à ce qu'ils soient protégés jusqu'à un certain niveau ou selon certaines normes.

Narrateur :
Les entreprises et les gouvernements investissent déjà massivement dans la protection des renseignements personnels identifiables. Pourtant, selon le Centre antifraude du Canada, les pertes imputables à la fraude se sont élevées à 7,9 millions de dollars entre 2020 et 2021 seulement.

Et ce n'est pas tout. Selon Statistique Canada, sur 100 000 Canadiens, le nombre de personnes ayant été victimes de fraude d'identité est passé de 2 en 2009 à près de **60** en 2020. Et cette tendance pourrait très bien se maintenir. L'impact sur les victimes est considérable.

Alors, **pourquoi** notre système actuel laisse-t-il les citoyens si vulnérables?

Erik Berg
Une fois les pièces d'identité émises, c'est le citoyen qui doit les protéger. Toutefois, nous sommes tenus de fournir nos renseignements personnels en de nombreuses occasions. Que ce soit pour louer une voiture, réserver une chambre d'hôtel, ouvrir un compte bancaire ou demander un prêt, nous devons transmettre ces renseignements à des entreprises et à des tiers. S'il y a vol des données, c'est le citoyen qui subit les conséquences.

Narrateur :
À mesure que nous traversons différentes étapes de la vie, nous devons partager nos renseignements personnels des centaines de fois. Et, bien qu'il soit facile de se dire « ça ne m'arrivera jamais à **moi** », même les plus prudents ne sont pas à l'abri d'un vol d'identité.

Mais avoir des sources numériques sûres pour vérifier l'identité peut faire une grande différence.

Yassir Bellout
L'identité numérique changera le contexte du risque, car elle offrira un plus grand contrôle sur la protection des renseignements personnels. L'identité numérique sera surtout axée sur le partage de l'information, la façon de partager l'information, le type d'information à partager et avec qui elle est partagée. Cela offrira plus d'assurance sur la façon dont l'information est traitée, que ce soit dans le cadre d'une transaction commerciale, d'une interaction dans les médias sociaux ou en ligne.

Dans le cadre de transactions commerciales, les parties prenantes sont plus confiantes quant à l'identité des personnes et la légitimité de la transaction.

Narrateur :
L'enjeu, c'est le sentiment de sécurité - savoir que même si vos renseignements personnels sont d'une façon ou d'une autre volés, il existe un système qui détecte la violation et révoque l'accès au **bon** moment et limite les dommages

Imaginez un monde dans lequel votre assistant virtuel pourrait vous aider à repérer et à prévenir la fraude!

Dramatisation 2.2 – Demande de prêt hypothécaire

FONDU :

SFX – Décor de cuisine. De l'eau qui bout. Jazz instrumental en fond sonore. Yusuf coupe des légumes en préparation du repas.

Une notification d'IRIS (SIRI) retentit.

IRIS
Vous avez reçu un avis urgent.

YUSUF
Iris, lis l'avis.

IRIS
Ce message vise à vous informer que votre identité a été utilisée pour une demande de prêt hypothécaire.

SFX – Le couteau s'arrête.

YUSUF
Iris, résume les détails de la demande.

IRIS
Voici les détails :

Votre identité a été utilisée au 451, rue De la Montagne, à 16 h 03 aujourd'hui, le 15 avril.

La demande de prêt hypothécaire au montant de 745 000 $ a été présentée à la Banque ABC et nécessite votre approbation.

Pour accorder l'approbation, dites APPROUVÉ. Pour signaler une activité frauduleuse, dites ACTIVITÉ FRAUDULEUSE.

YUSUF (DANS SA TÊTE – CONFUS)
Quoi!? Ça n'a aucun sens!

Est-ce que ça pourrait être Aisha? Mais pourquoi? Non…

Maman? Elle est propriétaire de sa maison depuis 30 ans...

Khalid?

...Non, ce n'est certainement pas eux.

YUSUF (À VOIX HAUTE)
ACTIVITÉ FRAUDULEUSE.

SFX - Les pommes de terre sont mises dans l'eau bouillante. Le couvert est remis.

IRIS
Merci, j'ai bien reçu votre signalement d'activité frauduleuse.

IRIS
Veuillez confirmer votre identité au moyen d'un balayage rétinien.

SFX - Balayage et sons d'ordinateur.

IRIS

Balayage confirmé.

Identification à deux facteurs requise.

YUSUF
Iris, envoie un NIP par message texte.

SFX - Signal d'arrivée du message texte. Code à quatre chiffres entrés.

SFX – Signal d'avis de confirmation

IRIS
Authentification réussie. L'accès à votre identité a été révoqué et la demande de prêt hypothécaire est annulée. Nous avons informé la banque ABC qu'il s'agit d'une activité frauduleuse.

YUSUF (SOULAGÉ)
Excellent. Maintenant que c'est réglé...

Iris, rappelle-moi de vérifier la cuisson des pommes de terre dans 20 minutes.

[Fin de la scène]

Narrateur :

Dans le futur écosystème pancanadien de l'identité numérique, l'identité sera vérifiée en temps réel, ce qui permettra aux Canadiens de résoudre rapidement des situations autrement très stressantes. En résumé, nous visons la tranquillité d'esprit.

Mais même avec des contrôles supplémentaires, une surveillance accrue et de solides défenses de cybersécurité, le système ne sera pas parfait. Cela veut dire que les fraudeurs sont infatigables. Ils deviennent plus intelligents et plus habiles chaque minute. Et... ils seront toujours là.

Yassir Bellout

Il est important de comprendre que l'identité numérique n'est pas une solution magique qui fera disparaître la cybercriminalité.

C'est plutôt un moyen de mieux protéger ce que nous avons maintenant. Les fraudeurs chercheront toujours des moyens de contourner le système, quelles que soient les mesures de protection mises en place. Que ce soit dans le monde numérique ou dans le monde réel, le crime a les mêmes motivations.

Il est important pour les organisations de concevoir des systèmes qui offrent des mesures de protection qui préviendront tout acte et comportement malveillants. Et c'est ce comportement malveillant qui est un moyen pour nous de savoir qu'il y a une atteinte à la sécurité ou une tentative de piratage.

Narrateur :

Comme Yassir le souligne, l'écosystème **entier** doit être protégé, pas seulement certains de ses éléments. La cybersécurité doit être intégrée au processus dès le début.

Le secret de la sécurité, ce sont les bonnes mesures de contrôle dans un environnement sûr. Pour bien faire les choses et assurer la création d'un écosystème pancanadien de l'identité numérique sécuritaire et résilient, les intervenants de partout au pays devront s'impliquer.

Yassir Bellout

Nous devons sécuriser la transformation de l'identité. C'est le premier défi. Cela dit, ce n'est pas la première fois que nous devons faire face à ce genre de défi. Tous les trois ou quatre ans, une transformation majeure survient dans notre façon de travailler et d'utiliser la technologie. Il y a 10 ans, les téléphones intelligents en étaient à leurs débuts et loin d'être aussi largement utilisés qu'ils le sont maintenant - ils ont changé notre vie. Même constat pour les technologies infonuagiques il y a 5 ans, et ainsi de suite. Prochain défi : l'identité numérique.

Nous devons d'abord rassembler toutes les parties prenantes. Donc, les gouvernements, les fournisseurs de la technologie, les législateurs et les consommateurs de première ligne, ce qui n'a pas vraiment été fait dans d'autres secteurs. Nous devons tous nous asseoir ensemble et nous assurer que nous concevons la bonne façon, une façon sûre et durable.

À mon avis, ce n'est pas un domaine où nous pouvons simplement laisser les fournisseurs de la technologie innover. Nous avons besoin qu'ils inventent et trouvent de nouvelles idées, mais nous devons nous assurer que ces innovations conviennent à tout le monde. Bien sûr, nous devons inclure un cadre réglementaire, veiller à ce qu'il soit élargi et adapté à la nouvelle réalité. Il doit également être viable à long terme.

Narrateur :

Il ne s'agit pas seulement d'adopter les plus récentes technologies au nom de l'innovation. Il s'agit de s'assurer que l'adoption de cette technologie est bien pensée, inclusive et sécuritaire.

Nos renseignements personnels sont extrêmement précieux et continueront d'être la cible d'attaques. À mesure que le Canada adoptera l'identité numérique, il sera crucial d'intégrer la protection de la vie privée et la sécurité aux fondements de notre écosystème d'identité numérique.

Merci encore de nous écouter et ne manquez pas le troisième épisode, au cours duquel nous explorerons en profondeur l'incidence de l'identité numérique sur les entreprises canadiennes ainsi que les principaux facteurs qui en assureront le succès aujourd'hui, demain et pour l'avenir.

Je suis Tamara Stanners, votre hôte, et vous venez d'écouter Pour l'avenir : Un balado de KPMG sur la cybersécurité. À bientôt.