



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

Série 1 : Destination : Identité numérique

Épisode 4 : D'aujourd'hui à demain



Imraan Bashir

[extrait]

C'est un espace dynamique qui évolue. Même les normes évoluent, mais cela ne veut pas dire que nous devons attendre que tout se règle tout seul.

Katie Bolla

[extrait]

Nous pouvons nous attendre à un avenir pratique, transparent, personnalisé et beaucoup plus sûr pour les consommateurs.

Marc Chaput

[extrait]

Rome n'a pas été construite en un jour. Ce sera donc un processus itératif. Il n'est pas trop tard pour commencer.

Narrateur :

Un ancien proverbe chinois dit : « Un voyage de mille milles commence par un pas. » Qu'il s'agisse de trouver le courage d'agir ou de nous assurer qu'il s'agit d'un pas dans la bonne direction, nous clôturons notre discussion sur l'identité numérique en mettant l'accent sur l'action.

[SFX – Chanson thème]

Hartaj Nijjar

Voici le balado « Pour l'avenir », qui explore la cybersécurité dans les entreprises d'aujourd'hui, de demain et de l'avenir.

Je m'appelle Hartaj Nijjar et je suis le leader national du groupe Cybersécurité de KPMG au Canada. Parcourez avec moi le monde de la cybersécurité pour comprendre le rôle crucial qu'elle jouera dans la protection de notre avenir.

[SFX – Chanson thème]

Narrateur :

Je m'appelle Tamara Stanners et suis votre hôte. Aujourd'hui, nous terminons notre exploration de l'identité numérique.

Nous avons fait un voyage audio dans l'avenir. Vous, notre auditeur, devriez maintenant savoir ce qu'est l'identité numérique, comment elle peut changer de nombreuses facettes de nos processus actuels de vérification de l'identité, et ce qu'il faut faire pour protéger ce système nouvellement créé. Maintenant que notre voyage approche de son terme, nous revenons au présent.

Dans cet épisode, vous aurez l'occasion d'entendre une fois de

plus nos conférenciers, qui présenteront quelques points clés à retenir pour les citoyens, les gouvernements et les entreprises du Canada.

Par exemple, s'il y a un message que nos auditeurs devraient retenir, c'est qu'aucun groupe ne pourra donner vie à l'identité numérique par lui-même. Il faudra des actions **concertées** entre les citoyens, les gouvernements et les entreprises.

Parlons du premier de ces trois groupes d'intervenants – les citoyens. Que pouvons-nous faire aujourd'hui pour protéger notre identité?

Erik Berg

Il est essentiel que les consommateurs comprennent d'abord où se trouvent leurs données.

Narrateur :

Voici Erik Berg, spécialiste des risques technologiques chez KPMG.

Erik Berg

Les données se trouvent sur nos différents appareils mobiles, ordinateurs portables, elles sont à la fois sur des supports physiques (papier) et numériques, et elles sont dispersées un peu partout. Il est essentiel de comprendre où se trouve cette information et quel type de contrôle de sécurité vous avez sur cette information. Vous ne laisseriez pas votre passeport dans une boîte aux lettres ouverte à l'extérieur de votre maison? C'est la même chose pour les données numériques. Vous devriez pouvoir les sécuriser. Elles devraient être chiffrées.

Deuxièmement, vous devez surveiller de près les renseignements personnels que vous transmettez. Certains fournisseurs n'en ont pas besoin. Vous devriez les fournir sur une base « besoin de savoir », c'est-à-dire en fonction d'un besoin opérationnel et fonctionnel précis. Malheureusement, plusieurs organisations demandent souvent plus de renseignements qu'elles n'en ont réellement besoin, et les consommateurs n'hésitent pas à les transmettre. Je pense donc qu'une prise de conscience, de part et d'autre, est primordiale.

Narrateur :

Même si les citoyens devront encore attendre avant qu'un écosystème pancanadien d'identité numérique ne soit mis en place, nous pouvons faire notre part pour protéger nos identités dès aujourd'hui. Soyez vigilants, attentifs et prudents. Pas seulement pour votre propre protection, mais aussi celle de vos proches.

Yassir Bellout

Nous oublions souvent que dans notre monde, les jeunes, nos enfants, ont aussi accès à Internet. Et une des choses que nous (je suis moi-même père de trois enfants) devrions faire de plus en plus, c'est de les protéger. Non seulement en utilisant Internet de façon sécuritaire à l'aide d'identifiants numériques, mais en l'enseignant à nos enfants. De meilleures solutions sont à venir, je n'ai aucun doute là-dessus. Mais en attendant, protéger l'identité et les données des jeunes est très important.

Narrateur :

Les jeunes générations sont nées dans l'ère numérique. L'essentiel de leur éducation, de leur vie sociale et de leurs passe-temps se fait dans le monde numérique, de sorte qu'il est essentiel de développer une expertise sur la façon et le moment de partager en toute sécurité de l'information personnelle identifiable en ligne.

Dramatisation 4.1 – hameçonnage perdu

FONDU :

SFX –Aréna. Un tournoi de jeux en ligne se déroule. Un père et son fils arrivent à leurs sièges. Papa regarde le tournoi pendant que le fils regarde sa tablette.

PAPA

Ok Sam, qu'est-ce qu'on regarde ici?

FILS

Seulement le plus grand tournoi de jeux de tous les temps : le tournoi de mi-saison de la Ligue des Lords! Ces gens là-bas, ce sont les joueurs et tu peux voir ce qu'ils font sur le grand écran.

PAPA (IGNORE SA QUESTION)

Il fait si sombre ici... où est le vendeur de hot dogs?

(vérifie ses poches)

Ah mon Dieu, j'ai oublié mon argent!

FILS (EMBARRASSÉ)

Papa. Voyons. Nous ne sommes pas en 1904. Tu peux tout commander avec ton téléphone maintenant.

(Change de sujet)

Puis-je avoir ta carte de crédit?

PAPA

Peux-tu le demander plus poliment, s'il te plaît? Et pour faire quoi?

FILS

Puis-je avoir ta carte de crédit, s'il te plaît?

Kurt vient de m'envoyer un message pour télécharger un nouveau jeu. Il dit que c'est vraiment malade. On se promène en capturant des royaumes et en gagnant des armures de bijoux.

Il est déjà au niveau 4 et je dois l'avoir avant qu'il ne devienne intouchable.

PAPA

Montre-moi ce message une seconde.

SFX – Lui tend le téléphone.

D'abord, ça me semble un peu louche. Regarde toutes ces fautes

d'orthographe. Et il a même mal écrit ton nom. Tu ne penses pas qu'il est étrange que Kurt te demande directement des renseignements sur ta carte de crédit?

Pourquoi tu ne lui envoies pas un texto? Demande-lui s'il t'a envoyé ce message.

FILS

Ah papa, franchement!

Papa

Non, il n'y a pas de « ah, papa, franchement ». Pas de message, pas de carte de crédit.

FILS (À CONTRECŒUR)

D'accord.

SFX –Tape sur le téléphone. Notification sonore d'envoi, puis de réception de message.

FILS (SURPRIS)

Hum.

PAPA

Alors? J'avais raison?

FILS (À CONTRECŒUR)

... Kurt n'a jamais entendu parler de ce jeu.

[Fin de la scène]

Narrateur :

Ce n'est pas parce que quelqu'un demande de l'information qu'il a le droit de le faire. Nous devons tous demeurer vigilants et poser constamment les bonnes questions **avant** de permettre à quiconque, en personne ou en ligne, d'accéder à nos renseignements personnels.

Et comme nous tentons de protéger notre identité aujourd'hui, l'avenir est prometteur.

Katie Bolla

Avec la mise en œuvre de l'identité numérique, le pouvoir et le contrôle seront entre les mains des consommateurs. Nous pouvons nous attendre à un avenir commode, transparent, personnalisé et beaucoup plus sûr. Nous pouvons maintenant décider qui accède à nos renseignements – personne ou organisation – et savoir pourquoi. Nous pouvons nous sentir plus en sécurité et plus en confiance en ce qui concerne notre identité.

Narrateur :

Il n'est donc pas surprenant que, dans la mise en place d'un écosystème pancanadien de l'identité numérique, les gouvernements – les émetteurs fondamentaux de l'identité – jouent un rôle essentiel.

Marc Chaput

L'établissement de cette nouvelle identité numérique et de cette nouvelle infrastructure nécessitera des efforts de la part des secteurs public et privé. Ces acteurs doivent donc travailler ensemble afin d'offrir un cadre d'identité numérique solide.

Narrateur :

Voici Marc Chaput, spécialiste, Gestion des identités et des accès de KPMG.

Marc Chaput

Je pense que notre pays est un peu en retard. Il n'est pas trop tard, mais d'autres pays sont loin devant nous à cet égard. Nous avons donc besoin que notre gouvernement commence à travailler sur les normes, la gouvernance et la législation sur la conformité qui doivent être mises en place.

Et puis nous avons le secteur privé qui va aider à construire l'infrastructure réelle pour soutenir ces nouvelles identités numériques. Il y a donc beaucoup de secteurs impliqués, et ils devront tous participer.

Bien sûr, ça prendra du temps. Rome n'a pas été construite en un jour. Ce sera donc un processus itératif pour nous. Il n'est pas trop tard pour commencer, alors commençons et construisons ce nouveau paradigme d'identité passionnant.

Narrateur :

Là où Marc encourage l'action rapide, Sylvia Kingsmill, leader mondiale, Cybersécurité chez KPMG, qui a participé à l'épisode 3, préconise une réforme législative.

Sylvia Kingsmill

Un des appels à l'action est la réforme législative. Nous avons encore beaucoup de chemin à faire pour que les exigences entourant l'expérience client et la protection de la vie privée soient en place. La confiance, la minimisation des données transmises, tout ce qui est nécessaire pour faire de l'identité numérique une réalité pour le gouvernement, passe par une réforme juridique.

Nous n'avons toujours pas de cadre législatif ni de règles d'engagement pour les sociétés fermées et les entreprises partout au Canada, ni pour les entités sous réglementation fédérale. Nous disposons d'un cadre législatif provincial qui permet que certains de ces éléments se concrétisent dans le cadre du projet de Loi 64 au Québec, mais les autres provinces sont toujours en consultation auprès du gouvernement pour savoir à quoi ressemblera leur législation respective.

Donc, pour les citoyens, les entreprises et tous ceux qui se fieront à l'identité numérique dans un proche avenir, nous avons besoin de quelques règles. Nous avons besoin de règles d'engagement. Rien n'a encore été établi de façon harmonisée à travers le Canada.

Narrateur :

Dans le cadre de cet effort d'équipe visant à établir un cadre d'identité numérique, les entreprises doivent aussi garder la confidentialité au premier plan.

Sylvia Kingsmill

Réfléchissez-y du point de vue de la confidentialité.

Narrateur :

Encore une fois, Sylvia s'adresse aux entreprises canadiennes.

Sylvia Kingsmill

C'est un changement de culture. C'est adopter une pensée fondée sur la confidentialité. Il faut évaluer les technologies émergentes avant de se lancer sur le marché, réfléchir à ce que devrait être le paramètre de confidentialité par défaut, afin que nous puissions obtenir une identité numérique sûre de manière efficace.

Et comme nous n'avons pas de cadre juridique harmonisé avec lequel travailler, je pense qu'il nous incombe de nous tourner

vers les solutions de marché, les normes de l'industrie et les meilleures pratiques pour prendre une longueur d'avance sur la législation. Parce que ça pourrait prendre un certain temps avant que nous ne voyions des changements législatifs. Nous ne voulons donc pas attendre que les lois dictent l'avenir du nouveau paysage numérique. Nous voulons commencer à adopter les meilleures pratiques et aller plus vite.

Narrateur :

Il existe un sentiment d'urgence réel quant à la nécessité de faire les bons premiers pas, ce qui n'est pas surprenant étant donné les avantages potentiels de l'identité numérique.

En ce qui concerne les premières étapes, si vous êtes un dirigeant d'entreprise canadien et écoutez cet épisode, que devriez-vous faire pour être parmi les premiers à profiter des avantages de l'identité numérique?

Imraan Bashir, leader, Identité numérique chez KPMG, poursuit.

Imraan Bashir

Comprenez vos clients avant même de vous lancer dans le parcours d'identité numérique. Quels sont leurs plus grands irritants? Quels sont vos cas d'utilisation pour interagir avec eux? Comment l'identité peut-elle même aider à résoudre les problèmes? Il y a des cas où l'identité n'est pas un problème. De nombreuses transactions sont anonymes. Peut-être qu'elles n'ont pas besoin d'utiliser l'identité numérique, et c'est bien. La priorité numéro un doit être de déterminer les cas où l'identité numérique est nécessaire dans votre entreprise, là où aujourd'hui, vous acceptez une preuve d'identité papier ou analogique, ou que vous procédez à une sorte de vérification manuelle en arrière-plan. Cette vérification pourrait être rendue plus efficace et plus fiable.

Un autre élément important de la mise en œuvre d'une identité numérique est de comprendre votre place dans l'écosystème. Êtes-vous un fournisseur d'identité? Êtes-vous un consommateur d'identité?

Comprenez-vous où vous vous situez dans cet écosystème pancanadien?

Nous rêvons ici de sources fiables, qui émettent une identité de confiance à des parties ou à des personnes qui comptent sur ces renseignements. Il existe peut-être un endroit où vous jouez un rôle sur plusieurs plans, donc il est important de mieux comprendre le rôle de votre organisation dans cet écosystème. Et aussi comprendre les normes dont vous auriez besoin, quel cadre de règles vous devez respecter pour faire partie de cet écosystème.

Narrateur :

Il s'agit de voir les cas de valeur réelle et d'utilisation au-delà de l'engouement, mais d'équilibrer cette analyse avec des mesures prises en temps opportun.

Imraan Bashir

J'encourage les organisations à adopter une culture d'expérimentation dans ce domaine aussi. C'est un espace dynamique qui évolue. Même les normes évoluent, mais cela ne veut pas dire que nous devons attendre que tout se règle. J'ai peur qu'en attendant trop longtemps, nous perdrons l'intérêt de la clientèle, et les entreprises du secteur risqueront de devenir désuètes parce que nous n'avons pas évolué assez rapidement.

Narrateur :

L'un des principaux défis de toute transformation numérique consiste à s'assurer que la rapidité de mise en marché ne compromette pas la sécurité. Comme il s'agit d'un balado sur la façon de **protéger** un avenir numérique, il faut souligner l'importance de garder une longueur **d'avance** sur les menaces.

Dramatisation 3.2 – Le pirate éthique

FONDU :

SFX –Lancement de la réunion Zoom. Un pirate informatique éthique rencontre un chef de la gestion des risques pour discuter d'un test de pénétration récent.

CONSTANCE

Bonjour Ria.

RIA

Salut Constance.

CONSTANCE

Comment allez-vous aujourd'hui?

RIA

Super. Trois cafés de pris. J'ai fait des tests d'intrusion toute la matinée, donc je me sens assez productive pour un lundi.

CONSTANCE

Contente d'entendre ça.

Ok, nous devons parler de ce contrôle du trafic et de la passerelle d'application aujourd'hui. Mais avant, pouvez-vous me faire part des résultats des tests de pénétration que vous avez effectués? J'espère que...

SFX –sons d'interférence web

RIA

Constance, je vous ai perdue pendant un moment.

CONSTANCE

Oh désolée, je disais juste que j'espérais de bonnes nouvelles aujourd'hui.

Je sais que les tests que nous avons menés au début de l'année étaient tous très solides, ce n'est donc qu'une formalité. Quoi qu'il en soit, quels sont les résultats?

RIA (RÉTICENTE)

Eh bien... hum... en fait, pour cette ronde, j'ai trouvé un moyen d'entrer dans votre dépôt de données par un trou dans le pare-feu.

CONSTANCE (CHOQUÉE)

Ah oui? Mais nous avons récemment corrigé un tas de trous et nous avons procédé à un exercice d'optimisation l'année dernière!

RIA

Je sais, mais le contexte des menaces évolue constamment. Il ne prend pas de pause.

(pause)

CONSTANCE (SONGEUSE)

C'est vrai...

(pause)

RIA

Écoutez Constance, vous et votre équipe êtes déjà en avance parce que vous consacrez du temps et des ressources pour renforcer vos défenses.

Mais, venant de quelqu'un qui fait ça dans la vie, croyez-moi quand je dis que ces exercices ne peuvent pas être faits seulement une fois par année. Les criminels ne prennent pas de pause et nous ne pouvons pas le faire non plus.

CONSTANCE (AVEC ASSURANCE)

En effet. Demain, notre équipe étudiera la question et formera un groupe de travail.

RIA (SUGGÉRANT)

Ou peut-être cet après-midi?

CONSTANCE (CONFIRME)

Ou peut-être cet après-midi.

[Fin de la scène]

Narrateur :

N'oubliez pas : Le cybercrime est facile. La protection est difficile.

Les attaques seront toujours un risque, et quelle que soit la complexité de vos défenses, un faux sentiment d'immunité ne peut que provoquer un désastre.

Si nous voulons assurer la sécurité d'un avenir axé sur la technologie et donner vie à l'identité numérique, nous devons intégrer la sécurité dans les fondements de nos systèmes d'identité et être proactifs dans le maintien de solides défenses aujourd'hui, demain et pour l'avenir.

Je suis Tamara Stanners, votre hôte. Nous vous remercions d'avoir fait ce voyage avec nous. Nous espérons que vous vous joindrez à nous en octobre 2022 pour la prochaine série de balados sur l'avenir. D'ici là, portez-vous bien et au revoir.