PASSION AFFAIRES et technologies

Nous aidons les entreprises à transformer leurs technologies en levier d'affaires

ARS solutions 25 ans

Mars 2018
Vol. 5 nº 2.

« Dans nos rencontres d'équipe, j'ai instauré la *minute informatique*, ce qui me permet de sensibiliser notre personnel à la sécurité informatique.

De nos jours, la cybercriminalité est une réalité et nous n'avons pas d'autre choix que de nous protéger.

Je consulte toutes les informations qu'ARS m'envoie, comme les bulletins et les rapports. Par la suite, je transmets aux employés les informations pertinentes pour les sensibiliser. Ils sont de plus en plus habiles à détecter les courriels frauduleux ou représentant un risque pour la sécurité de nos systèmes.

Ce sont de bonnes habitudes que nous n'avons plus le choix de combiner à une bonne protection antivirus et antipourriel ainsi qu'à une solution de sauvegarde et de relève robuste comme celle d'ARS. »

Louyse Trudel

Agente d'administration à la direction générale, AQCS

Suivez-nous

Développement d'applications mobiles :

TEMPS DE LECTURE 6:00

10 tendances à surveiller en 2018

Le développement d'applications a gagné du terrain en 2017 et pour cause. Les entreprises ont commencé à voir le concept non comme un choix, mais comme une nécessité. Les moyens les plus populaires de magasiner, naviguer et communiquer sont via les appareils mobiles et, par conséquent, investir dans une app mobile est l'un des meilleurs moyens d'augmenter les ventes.

1 INTERNET OF THINGS (IOT) ET APPLICATIONS PORTABLES

En 2017, le concept de maison intelligente et de santé intelligente a gagné en popularité. Cette année, les applications IoT se présenteront de plus en plus comme une tendance dominante. Quant aux apps portables, comme la montre Apple, elles seront en plein essor. Comme nous voyons une augmentation de la demande IoT, des applications seront nécessaires pour les appareils intelligents à la maison et au bureau.

2 ACCÉLÉRATION DU CHARGEMENT DES PAGES SUR MOBILES (AMP)

Qui veut attendre qu'une page Web se télécharge ? C'est pourquoi Google a présenté le projet AMP pour accélérer le temps de chargement.

SUITE À LA PAGE 2 ▼

SUITE DE LA PAGE 1 ▲

3 PAIEMENTS MOBILES

Les clients qui achètent en ligne via des applications mobiles utilisent généralement des services bancaires Web ou des cartes de crédit / débit pour effectuer des paiements. Mais avec l'introduction d'Apple Pay et de Google Wallet, les clients favorisent progressivement le m-commerce[1].

4 RÉALITÉ AUGMENTÉE (AR) / RÉALITÉ VIRTUELLE (VR)

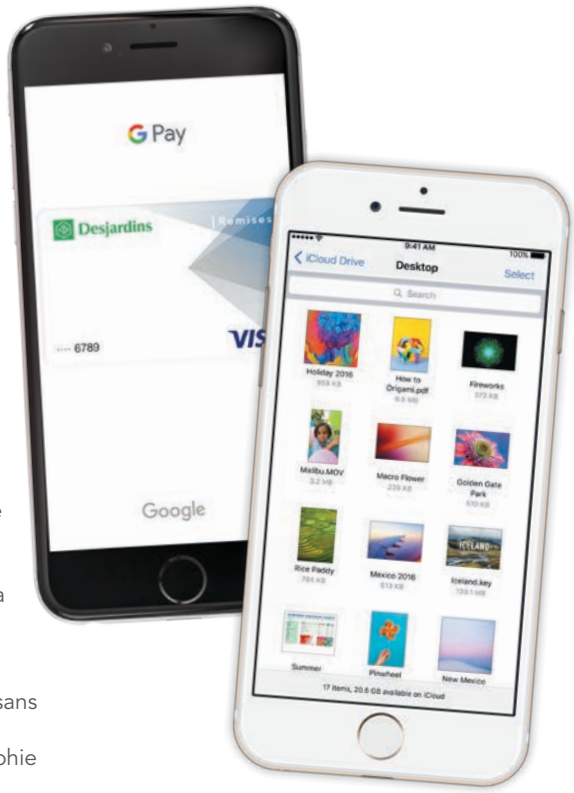
En 2018, AR et VR iront au-delà du divertissement et du jeu. Il y a un potentiel énorme pour l'AR et la VR en ce qui concerne la transformation de différents secteurs industriels. Le marché de la réalité augmentée sera largement dominé par les secteurs de la vente au détail, de la santé, de l'ingénierie et de l'immobilier tandis que les technologies de réalité virtuelle se concentreront sur le jeu et les événements.

Avantages de la réalité augmentée (AR) :

- Les produits et services peuvent être présentés en détail à l'aide d'une expérience visuelle pour les consommateurs.
- Les entreprises peuvent présenter la pertinence de leurs produits en temps réel.
- Les employés peuvent être formés à l'aide de cette technologie, ce qui augmentera ultimement la productivité.

Avantages de la réalité virtuelle (VR) :

- La capacité de présenter des produits en 3D dans des salles d'exposition virtuelles sans avoir besoin de beaucoup d'espace.
- La capacité de promouvoir les produits de manière interactive en utilisant la photographie et la technologie.
- Peut facilement être utilisé pour l'image de marque et le marketing.



5 APPLICATIONS SUR DEMANDE

Les applications sur demande gagnent en popularité. Elles rendent notre vie plus facile et offrent des solutions pratiques. Nous pouvons les utiliser de n'importe où et le paiement est facile. Voici quelques exemples : services d'entretien ménager, d'esthétique, de livraison de nourriture, de taxi…

6 LES APPS D'ENTREPRISE ET BYOD

De plus en plus d'organisations commencent à adopter le modèle « Bring Your Own Device ». Nous devrions donc voir une augmentation de la demande pour les applications hybrides (celles qui fonctionnent sous forme d'application, mais qui sont plus comme les sites Web mobiles). On estime que la moitié des employeurs du monde auront besoin du BYOD au cours de la prochaine année. **La sécurité demeurera donc un enjeu important.**

7 APPLICATIONS CLOUD

L'utilisation de la technologie Cloud connaît une forte augmentation. On parle ici d'une solution de stockage pour les photos, la musique – en fait, pour l'ensemble de notre utilisation personnelle des technologies. Il est devenu beaucoup plus facile d'obtenir des données sans impacter la mémoire interne de votre téléphone. Dropbox et Google Drive demeurent les outils les plus populaires, mais la solution de stockage Cloud d'Apple connaît également une popularité croissante. **Attention toutefois à l'excès de confiance. « Cloud » ne signifie pas « sécurité ». Il faut faire preuve de prudence sur ce qu'on y met.**

8 SÉCURITÉ DES APPLICATIONS

La sécurité des smartphones est plus importante que jamais en raison de la quantité de données stockées sur ceux-ci. Cependant, il est surprenant de constater que beaucoup de gens ne prennent pas encore la sécurité de leurs appareils mobiles aussi sérieusement qu'ils le devraient. Et il s'agit là d'une préoccupation pour les développeurs d'applications. Les applications avec des fonctions de sécurité intégrées peuvent faire une énorme différence et, par conséquent, les développeurs vont commencer à les utiliser davantage. Ultimement, il deviendra la norme d'offrir une garantie de sécurité pour chaque application développée.

9 MACHINE LEARNING, L'INTELLIGENCE ARTIFICIELLE (IA) ET LES CHATBOTS

Chatter en ligne avec les acheteurs reste très lucratif pour toutes les entreprises. Les applications intègrent continuellement les préférences de leurs utilisateurs et utilisent cette information à leur avantage. Les applications d'IA les plus populaires sont encore Prisma, Siri et Google Now. Cependant, du nouveau pourrait survenir en 2018.

10 *LAZY LOADING*

La dernière tendance surprenante est le *lazy loading* (chargement paresseux).

Si nous lisons un article avec de grandes images, nous ne pouvons parfois ni ouvrir, ni lire jusqu'à ce que ces images soient téléchargées. Or, les utilisateurs ferment souvent la page en faveur d'une autre plus rapide et plus facile à utiliser. Le taux de rebond des pages a donc connu une forte augmentation. Les experts en la matière ont inventé le *lazy loading* qui consiste à attendre une action du visiteur pour charger certaines portions de la page : images, boutons de partage sociaux, etc. Cela permettra de réduire considérablement le temps de chargement et devrait entraîner une réduction du nombre de pages rebondies.

Le développement des applications mobiles poursuivra sans aucun doute sa croissance en 2018 et les utilisateurs devront faire preuve de vigilance quant à la sécurité de leurs informations.

[1] *M-commerce désigne l'ensemble des transactions commerciales effectuées par le biais des terminaux mobiles, en particulier les smartphones et tablettes (les ordinateurs portables traditionnels ne sont pas inclus dans cette catégorie).*

Simon Fontaine, Président
simon.fontaine@ars-solutions.ca

Nous rendons les entreprises plus efficaces et performantes en transforma

4 *hacks* majeurs qui ont marqué 2017

Comment votre entreprise devrait se protéger ?

TEMPS DE LECTURE 7:00

Il est parfois difficile de distinguer une fausse nouvelle ou une histoire sensationnelle d'un réel danger. Quelles sont les menaces réelles auxquelles sont confrontées les PME aujourd'hui ? Après tout, Target, Home Depot et d'autres bannières connues sont toujours celles présentées aux nouvelles. Pourtant, ***81 % des brèches de sécurité se produisent dans les PME*** *- peut-être parce qu'elles n'ont pas accès à des solutions de sécurité robustes ou parce qu'elles choisissent de ne pas investir en sécurité…*

CES 4 *HACKS* ONT PROUVÉ QU'AUCUNE ENTREPRISE N'EST À L'ABRI DES CYBERATTAQUES...

Equifax

En septembre 2017, Equifax a annoncé une brèche de données massive qui **a compromis les données personnelles de 143 millions de clients**.

L'attaque s'est produite à travers une faille dans l'application de développement Web *Apache Struts*. Equifax a pris connaissance de la vulnérabilité plusieurs mois avant l'attaque, mais n'a pas agi assez rapidement pour appliquer un correctif de sécurité au logiciel. En conséquence, **les pirates ont eu accès aux noms, NAS, dates de naissance et adresses** de millions de clients entre le 13 mai et le 30 juillet 2017.

Equifax a été largement critiqué pour avoir attendu plus d'un mois avant d'alerter les clients et actionnaires à propos du piratage.

Wanna Cry

Une souche de rançongiciel appelée WannaCry a touché **plus de 230 000 ordinateurs dans 150 pays en mai 2017**. Le virus a infecté les ordinateurs Windows via une vulnérabilité appelée EternalBlue. Windows a déployé un correctif pour EternalBlue en mars, mais de nombreux systèmes n'étaient toujours pas protégés lorsque le virus a commencé à se propager deux mois plus tard.

Petya/NotPetya

Un mois après WannaCry, un nouveau virus connu sous le nom de Petya a paralysé des systèmes informatiques **dans plus de 60 pays**. Petya a fonctionné de manière similaire à l'attaque WannaCry, utilisant la vulnérabilité Windows EternalBlue pour infecter les ordinateurs et demander **une rançon de 300 $ en Bitcoin aux utilisateurs**.

Uber

En novembre dernier, Uber a avoué avoir été victime d'un piratage en 2016. L'incident a touché **les informations personnelles de 57 millions d'utilisateurs et les numéros de permis de conduire de 600 000 conducteurs d'Uber**.

Les pirates informatiques auraient accédé aux données d'Uber via un service Cloud tiers. Ils ont réussi à s'infiltrer dans le compte GitHub d'Uber et ont découvert les identifiants de connexion pour accéder à ses données stockées dans le serveur d'Amazon.

Au lieu de rapporter la brèche de données aux autorités et d'alerter les utilisateurs, **Uber a payé 100 000 $ aux *hackers* pour acheter le silence et détruire les données**. Uber sera probablement confrontée à des sanctions juridiques sévères pour avoir omis de signaler cette violation de données.

Les cyberattaques sont en hausse et **les coûts des dommages associés aux rançongiciels ont dépassé 5 milliards de dollars en 2017, soit quinze fois plus qu'en 2015**. Les attaques par rançongiciels ciblent les entreprises de toute taille, laissant des millions de données personnelles à risques et des équipes TI qui s'acharnent à récupérer les données.

SUITE À LA PAGE 4 ▼

SUITE DE LA PAGE 3 ▲

5 précautions à prendre pour réduire vos risques

1 FORMATION EN SÉCURITÉ

La plupart des employés ne sont pas familiers avec les meilleures pratiques de base en sécurité et peuvent involontairement créer des failles. Les employés peuvent stocker des données confidentielles de l'entreprise sur leurs appareils mobiles ou être susceptibles d'ouvrir des courriels d'hameçonnage.

Formez vos employés à détecter les courriels et fichiers suspects et apprenez-leur à sécuriser leurs comptes et à renforcer leurs mots de passe.

2 GESTION DE CORRECTIFS (PATCHS)

La gestion des correctifs est une mesure préventive qui adresse et corrige les vulnérabilités découvertes dans les logiciels au fil du temps. Les pirates ciblent souvent ces faiblesses.

L'attaque WannaCry a profité d'une vulnérabilité dans les anciens systèmes d'exploitation Windows. Microsoft a déployé un correctif quelques mois avant l'attaque, mais nombreux sont ceux qui ne l'avaient pas installé.

3 SCAN DU *DARK WEB*

Si les données de votre entreprise sont compromises, vous voudrez savoir où circulent vos informations. Les pirates achètent et vendent fréquemment des données volées sur le Web sombre (*dark Web*) à des fins de vol d'identité et de fraudes.

Un scan du *dark Web* surveille les forums de discussion criminels, les réseaux privés et autres sites cachés pour rechercher vos informations volées. **Le système vous avertit lorsqu'il détecte que vos données sont compromises.**

Même si un scan ne peut pas supprimer vos données une fois qu'elles ont été publiées, **il vous permet de prendre des précautions pour doubler la sécurité et vous protéger contre le vol d'identité**.

4 POLITIQUES CLAIRES

Chaque employé devrait être informé des politiques de sécurité dans votre entreprise. Créez des exigences claires en ce qui concerne la sécurité des mots de passe et des identifiants. Si vous proposez un programme **BYOD** (Bring Your Own Device), assurez-vous de l'installation obligatoire d'un logiciel de sécurité. **Clarifiez quelles informations de l'entreprise peuvent ou ne peuvent pas être consultées via des dispositifs personnels.**

5 DÉLÉGUER LA SÉCURITÉ

Embauchez un expert du domaine que vous ayez ou non une ressource technique à l'interne. **Vous bénéficierez d'une équipe de spécialistes possédant non seulement un ensemble de compétences, mais également des outils performants** qui sont nécessaires pour vous aider à protéger ce qui compte réellement pour votre entreprise. **La sécurité est un processus à maintenir en continu.**

Sécurité

81% des brèches de sécurité se produisent dans les PME

Pour en savoir davantage sur votre **niveau de risque** et obtenir un **plan d'action clair** sur les mesures à prendre, ARS vous offre **3 forfaits d'audit de sécurité** selon vos besoins :

1 Le Sommaire
Une évaluation générale de votre niveau de risque

2 L'Avancé
Une évaluation plus en profondeur combinée à des tests d'intrusion

3 Le Premium
Le monitoring se greffe à l'audit pour une détection supérieure

Contactez-nous pour obtenir une proposition sur mesure en fonction de votre situation.

ARS solutions affaires et technologies
6655, boul. Pierre-Bertrand, bureau 301, Québec (Québec) G2K 1M1
www.ars-solutions.ca | info@ars-solutions.ca | 418 872-4744