# PASSION AFFAIRES et technologies

**Présentés ce mois-ci :**



Entreprise TI classée #1 à Québec en 2022 par **ThreeBest Rated®**

## « Grâce à l'intervention proactive de toute l'équipe d'ARS, nous avons évité le pire…

Nous avons récemment vécu un incident de sécurité. **ARS est intervenue très rapidement grâce à la cybersurveillance, avant même que nous en ayons pris conscience.** Par la suite, j'ai pu compter sur les techniciens pour régler rapidement certains **problèmes de changement de mots de passe** qui découlaient de l'incident. Après la fin de l'intervention, le bilan que m'a fourni ARS a fait en sorte que nous avons pu améliorer notre processus de gestion de crise.

**L'approche proactive d'ARS est très rassurante pour la cybersécurité de notre organisation.** Elle nous permet d'éviter des problèmes qui pourraient entraîner un long temps d'arrêt, une perte de confiance de nos membres et partenaires, et ainsi nuire à notre réputation.

Avec ARS comme partenaire TI, **nous avons l'esprit tranquille,** car nous savons que nos systèmes sont entre des mains expertes en tout temps. »

Louyse Trudel
**Agente d'administration à la direction générale AQCS**

## Guerre de l'information :
## Twitter lance une stratégie de contournement de la censure pour échapper à la surveillance russe

**Les entreprises touchées par la répression de la liberté d'expression en Russie à la suite de l'invasion de l'Ukraine ordonnée par Poutine, comme Twitter, Facebook et d'autres médias, réagissent en proposant des solutions technologiques sur le Dark Web pour contourner la censure.**

Le Kremlin a pris des **mesures pour réduire au silence le mouvement de protestation contre la guerre en Russie** en restreignant les médias indépendants locaux et internationaux, ainsi que Twitter et Facebook. Le parlement contrôlé par Poutine a adopté une **loi rendant la diffusion de ce qu'il considère comme des "fake news" sur l'armée russe passible d'une peine pouvant aller jusqu'à 15 ans de prison**.

SUITE PAGE 2

Cette répression a incité de grands médias internationaux, dont le New York Times et la BBC, à suspendre leurs activités d'information en Russie. **Twitter a lancé cette semaine une version officielle de son site de microblogging sur Tor, la principale porte d'entrée de l'Internet anonyme.** Les sites sur Tor se terminant par .onion au lieu de .com, permettent de dissimuler la localisation de l'utilisateur et son activité. Le réseau fonctionne « en oignon » avec plusieurs couches pour protéger les données (d'où le logo de Tor). **Cette stratégie permet donc aux utilisateurs en Russie de contourner la surveillance et la censure** en utilisant le réseau d'anonymat Tor pour accéder à la plateforme.

« **Rendre notre service plus accessible est une priorité permanente pour nous.** Nous avons connaissance de rapports pointant une difficulté croissante pour les utilisateurs à accéder à Twitter depuis la Russie. **Nous investiguons et travaillons à rétablir un accès total à notre service.** », a déclaré Trenton Kennedy, porte-parole de Twitter, dans un communiqué envoyé par courriel le 2 mars dernier. Le réseau social était effectivement limité en Russie depuis quelque temps. Plus précisément, **le 4 mars dernier, le régulateur russe de l'Internet, Roskomnadzor, a commencé à restreindre l'accès à Twitter** après avoir récemment bloqué Facebook. Cette décision était basée sur une **demande du Parquet national datant du 24 février, soit la même date que le début de l'invasion de l'Ukraine.**

La BBC a publié un message intitulé "Comment contourner le blocage de la BBC en Russie", indiquant le site "dédié" de la chaîne sur le navigateur Tor et **Psiphon, un outil pour contourner la censure**. La BBC a également lancé **2 fréquences d'ondes courtes diffusant des informations en anglais en Ukraine et dans certaines parties de la Russie** - ce qui avait été progressivement supprimé dans la plupart des endroits au cours de la dernière décennie. **« L'accès à des informations précises et indépendantes est un droit de l'homme fondamental qui ne doit pas être refusé au peuple russe »**, a déclaré la BBC.

Voice of America, le service de diffusion internationale par radio et télévision du gouvernement américain, que le Kremlin a menacé la semaine dernière de bloquer en raison de ses reportages indépendants sur l'invasion de la Russie, a déclaré un communiqué : **« VOA continuera de promouvoir et soutenir les outils et les ressources qui permettront à notre public de contourner les mesures de blocage imposées à nos sites en Russie. Nos journalistes poursuivront leurs reportages, un exemple de la liberté de la presse en action. »** Un groupe de financement participatif a d'ailleurs payé pour que les émissions soient placées sur une station privée et commerciale à ondes courtes.

Somme toute, bien que le **Dark Web**, aussi appelé le Web clandestin, soit utile pour les applications illégales, cette situation démontre qu'il peut tout aussi bien servir **pour préserver l'anonymat et la confidentialité des activités sur Internet par applications légales soutenant les droits fondamentaux.**

*Source : Rebecca Falconer et Marina Alcaraz*

# Conseils anti-hammeçonnage

Continuez de lutter contre la cybercriminalité! Inscrivez-vous pour recevoir nos **NOUVEAUX "conseils anti-hameçonnage" SANS FRAIS** et gardez vos employés alertes. **Vous recevrez ensuite un conseil à tous les mois par courriel.**

**Pour vous inscrire :**
www.ars-solutions.ca/conseils-anti-hameconnage-phase-2/
info@ars-solutions.ca • 418 872-4744 #233

# Outils de collaboration : une porte d'entrée supplémentaire pour les cybercriminels

**Depuis que le télétravail s'est normalisé, les outils de collaboration sont également devenus la norme au sein des entreprises. Il s'agit toutefois d'une porte d'entrée supplémentaire pour les cybercriminels...**

La semaine dernière, chez ARS Solutions, certains de **nos employés ont reçu un courriel de Connexion Affaires de TELUS**, l'outil de collaboration et de téléphonie IP que nous utilisons à l'interne, et **celui-ci semblait très légitime**. Voici le courriel en question :

**Objet: Message important concernant votre service Connexion Affaires de TELUS**

TELUS

Connexion Affaires de TELUS

Bonjour Mario Lessard,

En raison de plusieurs tentatives de connexion infructueuses, votre connexion à Connexion Affaires de TELUS sera vérrouillée pendant 60 minutes. Si vous avez oublié votre mot de passe, veuillez cliquer ici pour le réinitaliser.

Vos services ne seront pas interrompus durant cette période.

Merci d'avoir choisi Connexion Affaires de TELUS.

Avis légaux | Modalité de service
©2022TELUS Communications Inc.

Il s'agissait d'un **avis de verrouillage de connexion suite à plusieurs tentatives de connexion infructueuses**. Heureusement, **nos employés nous l'ont signalé rapidement** donc nous avons pu avertir le reste de l'équipe qu'il s'agissait d'un courriel frauduleux et qu'il ne fallait pas cliquer sur le lien. Il serait toutefois **très intuitif pour certains de croire que quelqu'un a réellement tenté de se connecter à leur compte** et donc qu'il faut modifier leur mot de passe au plus vite. **Mais le simple fait de cliquer sur le lien pourrait être bien dommageable pour l'entreprise et infecter l'ensemble du réseau.**

En cybersécurité, **un seul clic peut être fatal**. On doit se méfier d'absolument tout pour éviter le pire, car **il vaut mieux être paranoïaque que piraté...** N'hésitez pas à nous contacter pour obtenir de l'aide à ce sujet ou pour vérifier la légitimité d'un courriel reçu.

# Cybersécurité : SIEM ou MDR?

Il y a beaucoup de confusion entre le **MDR (Managed Detection and Response) et le SIEM (Security Information and Event Management)**. Alors que le MDR est plutôt un outil automatisé de détection des menaces les plus probables de survenir, le SIEM quant à lui vise plus large afin d'intercepter tout incident potentiel pouvant mettre une organisation à risque, et ce, autant de l'interne que de l'externe. Il collecte les journaux de tous les dispositifs présents sur le réseau et effectue des corrélations afin d'identifier les tentatives d'attaques. En somme, **le SIEM est beaucoup plus complet qu'un MDR dont l'action est limitée**. Toute entreprise se spécialisant en cybersécurité aura tout avantage à travailler avec un SIEM si elle veut protéger adéquatement ses clients des attaques. **Voici un tableau comparatif permettant de mieux différencier les deux services. Tout est une question de culture d'entreprise et de gestion de risques.**

| SIEM | MDR |
|---|---|
| **Approche globale permettant d'identifier tout incident potentiel.** | **Approche ciblée sur les menaces les plus probables.** |
| **Cueillette d'informations globale à des fins d'analyse d'éventuels incidents grâce à une vision plus large.** *Par exemple, la détection d'utilisation de services non autorisés et/ou anormaux tels que les copies de sauvegardes.* | **Identification des journaux significatifs uniquement** *(vision plus restreinte).* |
| **Savoir qui fait quoi et quand (et a accès à quoi).** *Ex. : Un employé qui a accès aux dossiers de paie ou qui exporte des données clients (Desjardins).* | ✗ |
| **Détecte les changements humains de configuration/sécurité, que ce soit dans le Cloud ou local** *(modification des groupes de sécurité, ajout de nouveaux équipements, etc.)* | ✗ |
| **Détection des mauvaises pratiques** *(comptes modifiés sans autorisation, erreurs techniques, interventions sur le réseau par les administrateurs sans justification).* | ✗ |
| **Collecte d'informations à des fins légales. Les données du SIEM sont recevables en cour.** *Le SIEM a la capacité de collecter et de conserver l'ensemble des journaux.* | ✗ *Le MDR n'est pas en mesure de collecter et de conserver l'ensemble des journaux. Il conserve ce qui lui semble significatif.* |
| **Un humain avec expérience et ayant la connaissance des particularités de son client détecte les anomalies et anticipe les éventuelles attaques.** *Possibilité de juger du niveau de criticité et d'insister pour la résolution de l'incident.* | **Outil automatisé, une intervention humaine se fait uniquement lorsqu'une menace est détectée.** |
| **Travail à temps plein par plusieurs ressources.** | **Travail à la demande.** |

De nos jours, il est essentiel d'avoir une **vision globale de la sécurité** ainsi qu'une **forte culture d'entreprise**, car **les employés imitent la direction.** La gestion de la sécurité doit suivre les **meilleures pratiques en la matière recommandées par les autorités telles que la CISA (Certified Information Systems Auditor), la NSA (National Security Agency) et le FBI (Federal Bureau of Investigation).** Votre département ou fournisseur TI doit non seulement être **dédié, compétent et expérimenté,** mais il doit aussi utiliser les **meilleurs outils spécialisés pour gérer la sécurité TI** dans son ensemble, incluant les problèmes comportementaux humains. Une **approche d'amélioration continue** au niveau des processus concernant la sécurité est également de mise. N'hésitez pas à nous contacter pour obtenir de l'aide à ce sujet.

*Source : Foresite*