

# Intrusion dans le monde de la cybersécurité

L'exposition des Canadiens aux cybermenaces ne cesse d'augmenter en raison du nombre croissant d'appareils connectés à Internet, d'innovations numériques et de processus automatisés. Les systèmes immobiliers d'aujourd'hui, beaucoup plus connectés, peuvent aussi être une porte d'entrée vers le réseau d'entreprise et faire l'objet de cyberattaques.

## La cybersécurité en évolution

Les services à distance sont hébergés sur des serveurs sécurisés. Ainsi, les services et le serveur même doivent inspirer confiance à l'usager. Dans ce contexte, on parle souvent d'utilisation de certificats d'authentification. Mais de quoi s'agit-il? Comment fonctionnent-ils? Quels sont-ils?

Les certificats d'authentification servent à identifier exactement un serveur afin qu'une session sécurisée soit établie lors des échanges de données, et ils sont les garants de l'existence de l'organisation à laquelle ils appartiennent.

### Certificat SSL

Au départ, le certificat SSL (Secure Sockets Layer) était destiné à la sécurisation des données sensibles entre deux systèmes (par exemple, entre un serveur et un client, comme un site d'achat et un navigateur, ou entre un serveur et un autre serveur, comme une application avec des renseignements personnels identifiables) essentiellement dans le cadre des paiements en ligne. Par la suite, il est devenu la norme notamment pour protéger l'accès aux comptes utilisateurs, l'envoi de documents dématérialisés ou les déclarations fiscales. Même les réseaux sociaux ont adopté le protocole SSL.

Les principaux objectifs de SSL sont :

- 🔒 L'authentification du serveur
- 🔒 La confidentialité des données échangées (avec une clé cryptographique)
- 🔒 L'intégrité des données échangées

Installé sur un serveur, SSL autorise des connexions sécurisées sur le navigateur. Celles-ci sont signalées par la présence du protocole HTTPS dans l'URL du serveur, et par l'affichage d'un cadenas de sécurité dans la barre d'adresse (à gauche ou à droite, en fonction des navigateurs).

SSL permet ainsi de différencier un site sécurisé et légitime d'un site mal protégé, voire malveillant, comme en cas d'hameçonnage.

### Certificat TLS

À la dissolution de la société Netscape Communications, le groupe Internet Engineering Task Force (IETF) à l'origine de la plupart des normes Internet, a continué à développer et à améliorer SSL, le rebaptisant TLS (Transport Layer Security). Tout comme SSL, TLS assure la sécurité des données et le chiffrement, le code d'authentification des messages.

À la différence de SSL, TLS :

-  Est constitué de deux couches : le protocole TSL Record (enregistrement) qui fournit une connexion sécurisée et le protocole TSL Handshake, qui permet au serveur et à l'ordinateur de s'identifier l'un à l'autre, puis de choisir ensemble un algorithme de cryptage et des clés secrètes avant de s'envoyer des données ou des messages
-  Est immunisé contre les cyberattaques
-  Est activé par défaut dans tous les navigateurs
-  Prend en charge de nouvelles suites d'algorithmes de chiffrement plus forts et plus sécurisés
-  Prend en charge les suites d'algorithmes de code d'authentification de message (HMAC-SHA256 / 384 et AEAD)

Par conséquent, TLS remplit les objectifs de sécurité souhaités : il assure l'authentification mutuelle des acteurs, la confidentialité, l'intégrité spatiale et temporelle des transactions. On peut ainsi dire que TLS représente un protocole sûr dans sa construction et ses mécanismes. C'est pourquoi dans le cadre de son engagement envers la sécurité des renseignements personnels, Régulvar utilise désormais TLS, ainsi que le protocole BACnet/SC, une version améliorée et plus sécuritaire de BACnet/IP. En effet, TLS est une fonction essentielle pour une communication sécurisée, et la gestion des certificats fait désormais partie des exigences devant être satisfaites pour mettre en place un réseau BACnet/SC.

## Régulvar s'adapte

Il y a 20 ans, les sociétés n'étaient pas conscientes que des gens pourraient profiter de l'information dont elles disposent en utilisant des brèches dans le réseau. Mais qui n'a pas en mémoire la récente fuite de données chez Desjardins?

Régulvar installe depuis près de 20 ans des systèmes de régulation IP, notamment BACnet/IP. Ce protocole a permis à l'industrie des systèmes de chauffage, de ventilation et de climatisation de fortement évoluer. En revanche, puisqu'il est ouvert, il peut constituer une brèche dans les réseaux. C'est pourquoi il est important de mettre en place des systèmes de protection adaptés et bien cadrés par le service informatique lorsqu'on l'utilise. De plus, il est basé sur des normes qui ne sont plus largement adoptées par la communauté informatique, surtout en ce qui concerne la sécurité.

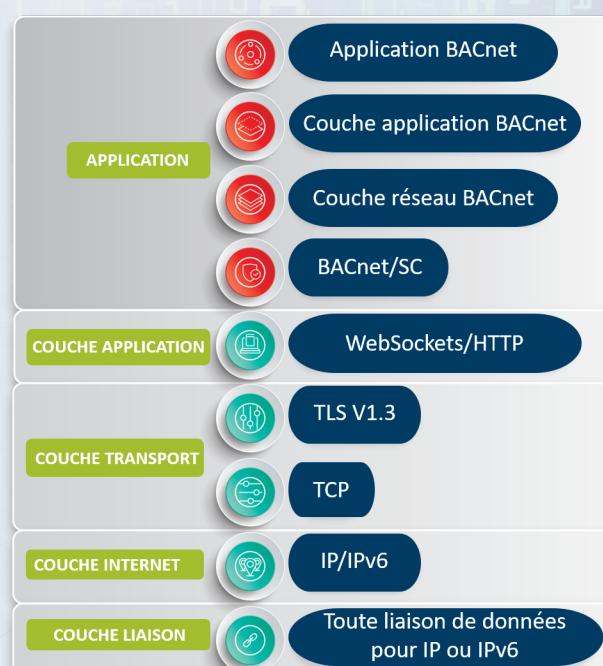
## BACnet/SC

Delta Controls a su s'adapter à la situation en mettant en place un programme de cybersécurité avec les politiques, les processus et les essais nécessaires, conformes aux normes OWASP, ISO et NIST, pour livrer des produits sécuritaires. Son objectif? Que les réseaux de bâtiments demeurent protégés grâce à des pratiques exemplaires d'intégration des technologies de l'information (TI), à une évaluation constante des produits et à des mises à jour de sécurité ponctuelles.

Ainsi, Delta Controls et Régulvar utilisent désormais [BACnet Secure Connect \(SC\)](#), un protocole BACnet sécurisé pour les réseaux TCP/IP conforme à la norme IEEE 802.1X, ainsi que les outils TLS.

Basé sur SSL et TLS, BACnet/SC est un protocole ouvert et fermé qui a ses propres mécanismes de sécurité des réseaux permettant d'authentifier un contrôleur ou logiciel et de l'autoriser à utiliser un réseau.

En outre, pour plus de sécurité, les appareils BACnet/SC peuvent être déployés dans des réseaux locaux virtuels (VLAN) ou des réseaux privés virtuels (VPN). BACnet/SC est aussi adapté aux méthodes, procédures et protocoles conventionnels des TI en matière de sécurité, ce qui le rend très convivial et plus sécuritaire.



Représentation des différentes couches BACnet dans le modèle OSI

Par ailleurs BACnet/SC est compatible avec tous les systèmes et appareils BACnet qui sont déjà installés. Rien ne doit être supprimé, aucune fonctionnalité n'est perdue.

En effet, la programmation et le langage client-serveur n'ont pas changé. Les utilisateurs n'ont pas besoin d'apprendre quoi que ce soit de nouveau. Ceux qui disposent déjà d'un système BACnet et qui souhaitent passer à la communication BACnet/SC utilisent simplement un routeur BACnet, car il s'agit d'une liaison de données différente. Ce même concept s'applique si l'utilisateur veut passer de BACnet MS/TP à BACnet/IP. Le message BACnet reste le même, seule l'enveloppe change.

## Différences entre BACnet/IP et BACnet/SC

	<b>BACnet/IP</b>	<b>BACnet/SC</b>
Protocole de transport	UDP	TCP
Communication cryptée	Non	Oui (avec TLS)
Authentification des appareils	Non	Oui (avec TLS)
Adresses IP	Statique en général	Statique ou dynamique
Système d'adressage par domaines	Non utilisé	Utilisé par certains fabricants
Tolérance aux conversions d'adresse de réseau	Avec appareils spéciaux	Oui
Type de connexion au bâtiment	BACnet/IP BBMD	Concentrateur BACnet/SC

## Avantages de BACnet/SC

- 🔒 Convivialité : adapté au domaine des TI
- 🔒 Utilisation des technologies standards de sécurité (protocole TLS) des réseaux TCP/IP
- 🔒 Cryptage des messages
- 🔒 Authentification des appareils avec des certificats
- 🔒 Compatibilité avec les installations BACnet
- 🔒 Prise en charge des réseaux IPv4 et IPv6

La révolution numérique a apporté de nombreux avantages, mais son lot de risques supplémentaires. Aujourd'hui, diverses approches sont utilisées pour sécuriser l'infrastructure BACnet; cependant, ces solutions peuvent être difficiles à mettre en place et elles constituent une charge pour les groupes informatiques. BACnet/SC facilite grandement la création d'une infrastructure BACnet sécurisée et normalisée entièrement compatible avec les déploiements BACnet déjà en place.

La cybersécurité ne représente pas un problème portant uniquement sur la technologie de l'information, il s'agit d'un problème d'entreprise qui exige une approche interdisciplinaire et un vaste engagement en matière de gouvernance pour faire en sorte que tous les volets de l'entreprise soient bien alignés pour appuyer des pratiques efficaces de cybersécurité.

Régulvar a toujours concentré ses efforts sur l'offre de solutions novatrices, adaptées et faciles à mettre en œuvre, et son programme de cybersécurité n'est pas différent.



# Un projet d'envergure



Qui n'a pas entendu parler du projet du REM? Ce vaste chantier, lancé il y a plus d'un an, représente actuellement le plus grand projet de transport collectif au Québec. L'objectif du REM? Desservir la grande région de Montréal sur 67 km (Rive-Sud, aéroport International Pierre-Elliott-Trudeau de Montréal, Sainte-Anne-de-Bellevue, Deux-Montagnes) grâce à un réseau de 26 stations.

Régulvar est heureuse d'annoncer qu'elle a été mandatée pour participer à ce prestigieux projet. Elle va ainsi concevoir et installer le système immotique BACnet/SC du REM dans les stations, les deux centres d'entretien et dans le bâtiment administratif. Au total, elle installera près de 2 700 contrôleurs (eBMGR, eBM404, eBM440, eBM800, 03-DIN-SRC, 03-DIN-CPU, 03-DIN-8XP) sur un réseau industriel hautement sécurisé. Les travaux de Régulvar ont commencé le 25 février dernier.

**Quels seront les défis relevés?  
La suite dans un autre bulletin une fois les travaux terminés. Restez à l'affût!**

Rédaction  
Caroline Gras, trad. a.,  
[cgras@regulvar.com](mailto:cgras@regulvar.com)

Graphisme  
Stéphanie Harel  
[sharel@regulvar.com](mailto:sharel@regulvar.com)

Source  
Marc Dugré  
Président, ing., CSO, Régulvar inc.



- MANIPULATION D'OBJETS BACNET**
- OBJETS AVANCÉS ET CONTRÔLEURS**
- PROGRAMMATION GCL**
- CRÉATION D'INTERFACE GRAPHIQUE avec Illustrator**
- CRÉATION D'INTERFACE GRAPHIQUE avec enteliviz**
- INTRODUCTION AU CONTRÔLE SANS FIL**

**À Laval** (français)

**À Gatineau** (anglais)

14 - 15 septembre	Sur demande
16 - 17 septembre	Sur demande
22- 23 - 24 septembre	Sur demande
29 - 30 septembre	Sur demande
Sur demande	Sur demande
Sur demande	Sur demande

Pour plus de renseignements,  
consultez notre site Web

[www.regulvar.com](http://www.regulvar.com)

ou communiquez avec le  
service de la formation  
au 450 629-0435, poste 1777  
[formation@regulvar.com](mailto:formation@regulvar.com)