EXPRESS
Bulletin du Syndicat des spécialistes et professionnels d'Hydro-Québec

Nouveau centre de surveillance électronique chez HQ : soyez vigilants!

Hydro-Québec, tout comme la majorité des compagnies de même envergure, se dote de nouveaux outils pour mieux protéger ses actifs dans le domaine de la technologie de l'information et des communications (TIC).

Elle vient en effet de mettre sur pied un centre de surveillance, le CSS, pour assurer sa sécurité en matière de TIC. L'un des buts visés est de surveiller et signaler tout acte pouvant être jugé malveillant et comportant un risque pour l'entreprise tels les attaques cybernétiques, les tentatives de DOS (*Denial of service*) ou l'intrusion de code pernicieux.

Ce centre a pour tâche de trouver, diagnostiquer et rapporter les situations à risque, qu'elles soient extérieures à l'entreprise ou internes. Il se peut donc que certains gestes posés, qui passaient inaperçus auparavant, soient désormais détectés.

Par exemple, si un employé utilisait un relai externe (*Proxy*) pour contourner le logiciel de filtrage d'entreprise (*Websense*) lui permettant d'accéder à des sites normalement bloqués, il mettrait alors à risque l'entreprise et s'exposerait à des réprimandes.

Nous vous rappelons que les outils de l'entreprise doivent être utilisés pour le travail seulement et non à des fins personnelles. Il faut surtout ne jamais tenter de contourner les règles de sécurité en place.

Tout ce que vous faites à partir de votre poste de travail est enregistré et pourrait servir contre vous en cas d'enquête.

Le rôle du CSS n'est pas de coincer les employés, mais bien de protéger les actifs de l'entreprise. Hydro-Québec est dans son droit d'agir ainsi car il a le devoir de le faire.

**Message du comité CTT (Changements techniques et technologiques*).