Cybersécurité

Protéger les systèmes gérés par l'AOE

À titre de fournisseur de services d'approvisionnement en eau et de traitement des eaux usées, l'AOE a fait de la sécurité de son infrastructure technologique et de ses données une priorité.

L'AOE se base sur les principaux cadres de sécurité et les avis qu'un grand nombre d'experts lui fournissent régulièrement.

Nos experts en cybersécurité protègent les infrastructures de TI de l'AOE, les systèmes SCADA (supervision, contrôle et acquisition des données), l'infrastructure technologique et les données que nous gérons contre les cybermenaces.

Les mesures de protection du système de cybersécurité de l'AOE comprennent des technologies de pointe qui détectent les menaces à l'infrastructure et aux actifs de réseau de l'AOE et les protègent contre ces menaces. Elles protègent également les ordinateurs de l'AOE, les réseaux et d'autres biens faisant partie des installations des clients avant, pendant et après une cyberattaque. Par ailleurs, nous encourageons les clients à prendre des mesures de sécurité appropriées afin de protéger leurs installations et leurs biens.

Conformément aux exigences applicables aux organismes de la Couronne, nous mettons en œuvre les meilleures pratiques de l'industrie et des procédures supplémentaires, dont les suivantes :

- Embaucher des experts en TI afin de renforcer la sécurité et la résilience de l'infrastructure de notre réseau et de protéger les données des clients que nous gérons.
- Mettre en œuvre des mécanismes de défense à plusieurs couches et des contrôles de sécurité proactifs afin de contrecarrer et d'atténuer les cybermenaces en évolution constante et d'intervenir de façon efficace.
- Évaluer les risques régulièrement.
- Apporter continuellement des améliorations, mettre à niveau régulièrement les systèmes de sécurité, sensibiliser notre personnel à la sécurité et lui donner une formation dans ce domaine.

Pour plus de renseignements, communiquer avec :

Eric Dorman | vice-président, information et technologie de l'information, AOE
edorman@ocwa.com www.ocwa.com/fr

ONTARIO CLEAN WATER AGENCY
AGENCE ONTARIENNE DES EAUX

La sécurité au premier plan

Il est essentiel de connaître les caractéristiques importantes des systèmes et des outils de TI.

L'AOE analyse les applications et les mises à jour selon divers critères, y compris les contrôles logiques et physiques de cybersécurité. Des mesures de sécurité ont été intégrées à nos systèmes, y compris le système de traitement des données, le système de gestion du travail et les systèmes SCADA, dont les suivantes :

- Mise en œuvre d'un système de gestion de l'identité et de l'accès pour la durée complète du cycle de gestion des comptes. Les privilèges sont accordés aux utilisateurs selon le besoin de connaître. Les utilisateurs reçoivent uniquement les privilèges dont ils ont besoin pour faire leur travail.
- Retour à un état de sécurité par défaut. Si une application ou un système tombe en panne, les autres systèmes seront épargnés ou ne seront que légèrement touchés.
- Mise en œuvre de plusieurs mesures de défense, dont les suivantes :
  - systèmes de détection des intrusions qui surveillent constamment les flux de trafic (cadres);
  - pare-feux qui assurent un filtrage en temps réel;
  - cryptographie et authentification par couches (zones);
  - professionnels agréés assurant l'intégrité des systèmes (contrôleurs).
- Surveillance et suivi constants afin d'intervenir rapidement et de façon efficace lors d'une attaque.
- Analyses des vulnérabilités et évaluations des menaces effectuées régulièrement.
- Vérifications périodiques de la cybersécurité et de la conformité aux protocoles de gestion des risques.
- En cas d'intrusion externe dans nos systèmes, l'AOE utilise un centre de sauvegarde hors site de type « chambre forte » lui permettant de reprendre ses activités rapidement. Seuls certains employés de l'AOE y ont accès. Il permet d'effectuer des sauvegardes régulièrement et en toute sécurité afin de réduire les risques.

Communiquez avec nous pour en savoir plus.

Nos mesures de sécurité

Pare-feux périphériques
Dispositifs de pointe qui détectent et préviennent les intrusions dans les réseaux grâce à une analyse du trafic en temps réel et qui offrent une protection supérieure contre les logiciels malveillants.

Pare-feux du réseau de serveurs
Pare-feux pouvant déterminer si un fichier est sécuritaire et soumettre les fichiers inconnus à plusieurs couches de sécurité.

Réseau privé virtuel et pare-feux locaux
Réseau privé virtuel et pare-feux nous permettant de restreindre l'accès à l'échelle locale.

Barrières à l'accès
Points de contrôle de l'accès qui permettent d'accorder les droits d'accès aux comptes des utilisateurs de façon très détaillée et reposent sur le principe du moindre privilège. Les utilisateurs reçoivent le strict minimum en ce qui concerne leurs droits d'accès.

Privilège
Les utilisateurs reçoivent un ensemble de privilèges établi en fonction de leur accès aux données.

Conception
Conception sécurisée du système de traitement des données, du système Maximo et des systèmes SCADA.

Reprise après sinistre
Systèmes à plusieurs couches pour la reprise après sinistre dotés de systèmes auxiliaires automatiques et manuels.

Experts
Personnes qui contrôlent et surveillent les systèmes et les verrouillent si leur sécurité est menacée.

Engagement
Engagement de l'AOE en matière de sécurité.