Note applicative

Sécurité des systèmes de gestion technique des bâtiments (GTB)

Résumé : les systèmes de gestion technique des bâtiments (GTB) de type SCADA permettent de centraliser la gestion des systèmes intégrés d'installations complexes. Ces dernières années, ils sont devenus une cible de choix des cyberattaques car ils sont considérés comme étant peu sécurisés du fait du manque d'outils de sécurité ad hoc. Spécialement conçue pour ces systèmes, la solution de sécurité de Radiflow regroupe des fonctions complètes de supervision et de mise en œuvre de la cybersécurité au sein d'une plateforme unique.

Les systèmes de gestion technique des bâtiments (GTB) gèrent des services indispensables à l'exploitation de bâtiments ou d'installations. On les trouve généralement dans les établissements bancaires, les data centers, les enceintes sportives, les campus universitaires, les hôpitaux et autres équipements dépendant de multiples services intégrés (alimentation en électricité et en eau, chauffage, ventilation et climatisation, contrôle des accès et alarmes incendie).

De nombreux systèmes GTB reposent sur un espace tampon entre le réseau normal et le réseau GTB. Si cette topologie est considérée comme sûre, elle ne l'est pas suffisamment pour empêcher les cybermenaces complexes comme les menaces internes (remise en service d'API contaminés lors de la maintenance, par exemple) ou externes (accès distant non sécurisé aux services).

Les réseaux GTB comprenant un grand nombre d'automates programmables, une des principales difficultés actuelles est de visualiser le trafic réseau en temps réel et de remonter les informations de sécurité. Avec un système avancé de surveillance du réseau GTB, il est possible de détecter les anomalies indiquant une attaque potentielle contre ses composants. Autre difficulté de la sécurisation des réseaux GTB : disposer d'un accès distant sécurisé pour les opérations de maintenance tout en veillant à ce que le technicien intervenant sur un appareil n'est pas accès aux autres dispositifs. À l'heure actuelle, les fournisseurs d'équipements pour réseaux GTB n'intègrent aucun mécanisme d'accès à leurs seuls matériels.

Autre tendance récente parmi les éditeurs de solutions GTB : la consolidation du réseau GTB et du réseau normal du bâtiment. Si cette consolidation présente de nombreux avantages, elle expose cependant le réseau GTB à davantage de cyberrisques.

Beaucoup d'administrateurs de réseaux utilisent les outils de protection des réseaux informatiques pour défendre leur réseau contre les cyberattaques potentielles. Ces produits sont excellents pour protéger les réseaux informatiques classiques. Cependant, ils ne conviennent pas à la protection des réseaux GTB parce qu'ils ne sont pas compatibles avec les protocoles utilisés sur ces réseaux (BACnet et Profibus, par exemple) et qu'ils ne modélisent pas leur topologie avec précision. En d'autres termes, les outils de sécurité pour réseaux informatiques n'ont aucune chance de détecter les anomalies et l'activité non autorisée des réseaux GTB.

RADIFLOW: SOLUTION DE SÉCURITÉ COMPLÈTE POUR SYSTÈMES SCADA

VISIBILITÉ

Notre système de détection d'intrusions (IDS) iSID apprend automatiquement la topologie du réseau (liaisons, protocoles et périphériques) par analyse passive. Toute nouvelle activité est mise en évidence dans l'interface du logiciel.

PROTECTION

Notre IDS et nos passerelles sécurisées protègent les réseaux SCADA contre les diverses menaces (exploration du réseau, infection des terminaux distants et activité des techniciens).

CONFORMITÉ

Nos produits permettent de mettre votre réseau en conformité avec les principales normes de sécurité : NERC CIP version 5, NIST SP 800-82 V2, ISA 99 et CEI 62443.

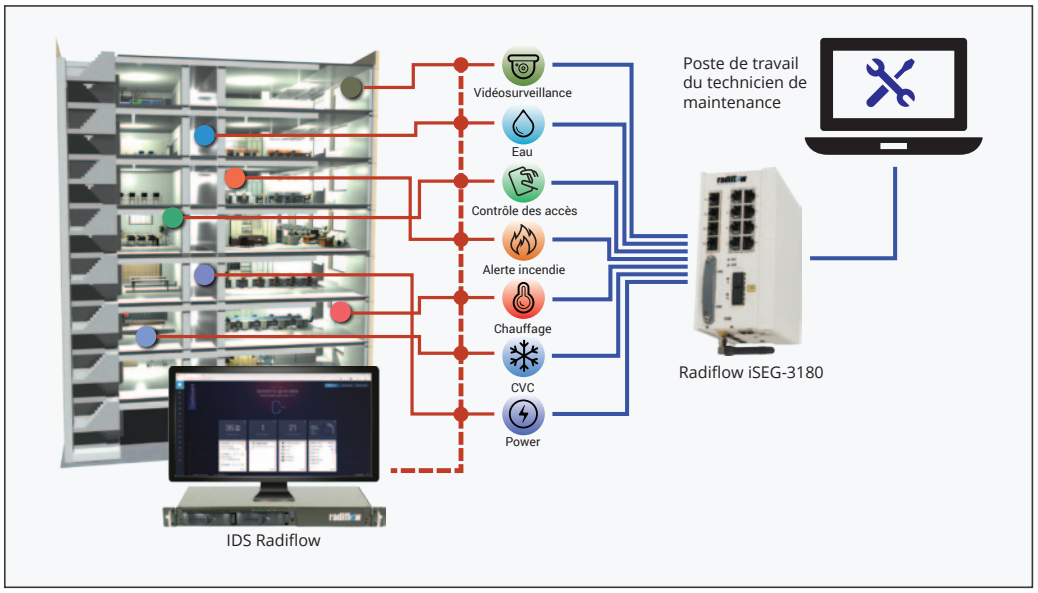
radiflow

La solution de sécurité de Radiflow a été conçue pour les systèmes SCADA/ICS, et notamment pour les systèmes GTB. Complète, elle comprend un système de détection d'intrusions (IDS) et des passerelles sécurisées. Non intrusif (sans effet sur le réseau GTB), l'IDS peut rapidement détecter et afficher toute activité anormale au sein du réseau GTB sitôt activé et garantir une protection totale.

L'accès sécurisé au réseau GTB est assuré par la passerelle sécurisée de Radiflow. Grâce à un accès par proxy d'authentification (Authentication Proxy Access - APA), l'administrateur réseau peut allouer une fenêtre temporelle spécifique pour limiter l'accès distant à un dispositif électronique donné en attente de maintenance. Cet APA est suffisamment souple pour lui permettre de planifier les tâches de télémaintenance sans courir le risque d'oublier de mettre fin à la session distante.

PRINCIPALES FONCTIONS

- Visibilité du réseau : par auto-apprentissage du réseau SCADA grâce à l'analyse passive (et active (en option)) de toutes les transactions de données.
- Détection des anomalies : détection de l'activité anormale (nouveaux appareils, modifications de la topologie, accès anormaux à la mémoire et modifications du microprogramme) par comparaison du modèle réseau normal créé par l'IDS.
- Gestion de la maintenance : processus APA (Authenticated Proxy Agent) pour la télégestion des opérations de maintenance.
- VPN : VPN IPsec de bout en bout pour la sécurisation des communications entre le centre de contrôle et l'installation protégée.
- Prise en charge des interfaces Ethernet et série des appareils récents et anciens, y compris de la norme PoE+.



À PROPOS DE RADIFLOW

Créé en 2009, Radiflow est un fournisseur de solutions de cybersécurité industrielle de confiance pour les opérations critiques. Notre gamme complète de solutions technologiques de pointe pour réseaux ICS/SCADA permet de conserver la visibilité et la maîtrise des réseaux OT, grâce notamment à un outil intelligent de détection des menaces à surveillance passive, capable d'identifier toutes les anomalies, et à des passerelles sécurisées de protection des réseaux OT contre tout écart par rapport aux politiques d'accès définies.Nos équipes sont constituées de professionnels aux profils les plus divers : experts en cybersécurité issus d'unités militaires d'élite et spécialistes en automatisation ayant travaillé chez les principaux opérateurs et fournisseurs de systèmes industriels. Nos solutions éprouvées sur le terrain et validées par les plus grands laboratoires de recherche protègent aujourd'hui des milliers d'installations.

US et Canada:
Tél: +1 (302) 547-6839
sales_NA@radiflow.com

EMEA:
Tél: +972 (77) 501-2702
sales@radiflow.com

UK:
Tél: +44 (0) 800 246-1963
sales_UK@radiflow.com

France:
Tél : +33 1 77 47 87 25
sales_FR@radiflow.com