PUBLI INFO

COMMENT PROTÉGER LES INFRASTRUCTURES CRITIQUES (SCADA) DE FAÇON PROGRESSIVE ET OPTIMALE ?

Stéphane AYACHE, Responsable Radiflow France

Radiflow dispose de plus de 10 ans d'expérience en matière de détection et d'analyse des menaces persistantes avancées (APT) et des attaques ciblées sur les infrastructures industrielles (SCADA). Radiflow bénéficie de nombreux retours d'expérience dans différents secteurs : énergie électrique, traitement de l'eau, pétrole & gaz, transport, industries chimiques.

GS Mag : Quels sont les principaux défis et enjeux inhérents aujourd'hui aux systèmes SCADA ?

NE RIEN FAIRE N'EST PAS UNE OPTION. En effet, les systèmes de supervision industrielle (ICS) sont vulnérables aux cyberattaques pour un certain nombre de raisons qui leur sont propres :

- Technologies réseaux et systèmes hérités ;
- Vulnérabilités non corrigées pour éviter d'interrompre la production (parfaitement connues des cybercriminels) ;
- Droits d'accès et paramètres laissés par défaut, existence de comptes génériques ;
- Vulnérabilités propres aux logiciels industriels, comme des mots de passe en clair dans les codes sources, dans les procédures d'exploitation qui datent du temps où les systèmes ICS n'étaient pas connectés au réseau et connaissaient peu de problèmes de faille logicielle (Modbus, BACnet, S7...).

Les principaux défis sont donc :

- La visibilité des composants de l'infrastructure OT de façon fine ;
- La traduction des vulnérabilités techniques en risques et impacts business ;
- La capacité à déployer rapidement des mécanismes de protection sans perturber le fonctionnement ;
- La gestion du multi-sites ;
- Et un « business model » adapté à cette industrie : service de bout en bout en mode SAAS.

GS Mag : Quelles sont les clés, selon vous, pour sécuriser de tels systèmes ?

Les clés de réussite d'une protection adaptée au contexte client, permettant une augmentation de la robustesse de l'infrastructure, nécessitent plusieurs ingrédients :

- Une double expertise pointue en automatisme et cybersécurité ICS SCADA ;
- Une méthodologie sur la base processus structuré et normalisé (ISA/CEI-62443) ;
- Une efficacité basée sur la capitalisation de nombreux retours d'expérience mondiale dans l'OT.

GS Mag : De quelle manière accompagnez-vous les entreprises dans cette démarche et comment votre offre est-elle amenée à évoluer dans ce domaine ?

Radiflow aide à protéger les entreprises de façon progressive et optimale afin d'augmenter la robustesse et la fiabilité des infrastructures. Pour cela Radiflow permet :

- D'auto-découvrir la topologie et le comportement opérationnel (non intrusif) ;
- D'analyser le trafic réseau par inspection approfondie des paquets des protocoles SCADA ;
- De bénéficier d'une solution de protection à valeur ajoutée sans avoir forcément à « patcher » tous leurs équipements ;
- De fournir un « business model » flexible et adapté : paiement à l'usage ;
- De surveiller les événements et la gestion des systèmes de contrôles de sécurité de l'environnement via des services partagés : centres de sécurité (SOC).

En lien avec nos partenaires intégrateurs, comme KALIS consulting, SEGULA..., nous proposons des services à valeur ajoutée en mode achat ou location (outils + service en mode SAAS) sur 2 axes :

1/ Protection des systèmes de Gestion Technique des Bâtiments (GTB) ;

2/ Protection des infrastructures industrielles (SCADA).

Enfin, la solution Radiflow est en cours de certification CSPN auprès de l'ANSSI. ■■■

INFORMATIONS PRATIQUES

➔Solution phare

Détection des menaces industrielles iSID

Modules de sécurité pour une détection complète des menaces :

1. Visibilité du réseau : iSID crée un modèle de réseau visuel de tous les périphériques, protocoles, sessions, et émet des alertes en cas de détection de modification de la topologie.
2. Gestion des vulnérabilités (CVE) : Gestion des menaces utilisées par les vulnérabilités du réseau SCADA, notamment celles contre les automates programmables et les protocoles industriels, en s'appuyant sur les sources de données publiques et sur le laboratoire de recherche de Radiflow.
3. Monitoring de la stratégie de sécurité : Définir et gérer les règles de sécurité de chaque liaison du réseau, et valider des commandes spécifiques (« écrire sur le contrôleur », p. ex.) et des plages de valeurs opérationnelles (« ne pas régler la turbine à plus de 800 tours/minute », p. ex.).
4. Gestion de la maintenance : Limiter l'exposition du réseau lors des opérations de maintenance planifiées en créant des ordres de travail pour des périphériques spécifiques pendant des fenêtres temporelles définies. À la fin de la session, un rapport détaillant toutes les activités de maintenance est généré.
5. Détection des anomalies : Création d'un modèle de réseau comportemental à l'aide d'une multitude de paramètres, comme le temps d'échantillonnage de la séquence des périphériques, la fréquence des valeurs opérationnelles, etc., pour détecter les anomalies.

➔Contact
Stéphane AYACHE
➔Téléphone
+33 (0)1 77 47 87 25
➔Courriel
stephane_a@radiflow.com
➔Web
www.radiflow.com

radiflow
Secure your Assets