Chapitre 6

Sécurité des systèmes SCADA

La sécurisation des systèmes SCADA est d'une importance cruciale en raison des raisons suivantes :

1. **Critique pour l'Infrastructure Critique :** Les systèmes SCADA sont souvent utilisés pour contrôler des infrastructures critiques telles que les réseaux électriques, les usines chimiques, les systèmes d'eau et d'assainissement. Une compromission de ces systèmes pourrait avoir des conséquences graves sur la sécurité publique et l'économie.
2. **Risque d'Impact Élevé :** Les attaques réussies sur les systèmes SCADA peuvent entraîner des interruptions de service, des dommages matériels, des pertes financières importantes, voire des risques pour la vie humaine, selon le secteur d'application.
3. **Connectivité Croissante :** La connectivité accrue des systèmes SCADA avec des réseaux informatiques et l'utilisation de technologies Internet of Things (IoT) augmentent les surfaces d'attaque, rendant les systèmes plus vulnérables aux cyberattaques.
4. **Conséquences Économiques :** Les attaques sur les systèmes SCADA peuvent causer des arrêts de production, des pertes de revenus et des coûts de réparation importants, sans compter les répercussions sur la réputation des organisations touchées.
5. **Menaces Évoluées :** Les attaquants modernes, y compris les acteurs étatiques, les groupes de cybercriminels et les activistes, sont de plus en plus sophistiqués. Les attaques peuvent être lancées pour des motifs divers, notamment l'espionnage industriel, le sabotage, la cybercriminalité ou le terrorisme.

Attaques (Menaces et Dangers) contre les Systèmes SCADA :

1. **Attaques de Déni de Service (DoS) :** Surcharge du réseau ou des serveurs SCADA, entraînant une interruption de service.
2. **Intrusions et Accès Non Autorisé :** Tentatives d'infiltration par des acteurs malveillants cherchant à obtenir un accès non autorisé aux systèmes SCADA.
3. **Malware et Virus :** Introductions de logiciels malveillants visant à endommager ou à compromettre le fonctionnement des systèmes.
4. **Ingénierie Sociale :** Utilisation de techniques de manipulation psychologique pour tromper les utilisateurs autorisés et obtenir des informations sensibles.
5. **Attaques par Injection de Code :** Insertion de code malveillant dans les protocoles de communication pour manipuler les données ou contrôler les processus.

6. **Attaques de Manipulation de Données :** Altération non autorisée des données de capteurs ou d'instruments pour induire en erreur les opérateurs.

Risques et Évaluation :

1. **Évaluation des Vulnérabilités :** Identifier les faiblesses potentielles dans les systèmes SCADA, y compris les vulnérabilités logicielles, matérielles et humaines.
2. **Analyse des Risques :** Évaluer les conséquences potentielles des menaces identifiées et déterminer les probabilités d'occurrence.
3. **Gestion des Risques :** Mettre en œuvre des mesures pour atténuer les risques, y compris la mise en place de contrôles de sécurité, de mécanismes de détection et de plans de réponse aux incidents.

Scénarios des Incidents Possibles :

1. **Arrêt de Production :** Un attaquant peut causer un arrêt complet ou partiel des opérations de production.
2. **Manipulation de Données :** Les données de capteurs peuvent être modifiées pour afficher des informations incorrectes, entraînant des décisions erronées.
3. **Violation de la Confidentialité :** Des informations sensibles sur les opérations industrielles peuvent être compromises.
4. **Sabotage Physique :** Des attaquants peuvent accéder physiquement aux équipements SCADA pour les endommager.

Sources d'Incidents et Détection :

1. **Accès Non Autorisé :** Utilisation de pare-feu, de systèmes de détection d'intrusion (IDS) et de contrôles d'accès pour prévenir et détecter les accès non autorisés.
2. **Malwares :** Utilisation d'antivirus et de solutions de sécurité pour détecter et éliminer les logiciels malveillants.
3. **Surveillance du Trafic Réseau :** Analyse du trafic réseau pour détecter les anomalies, les tentatives d'intrusion et les comportements malveillants.

Politique de Sécurité :

1. **Développement de Politiques :** Élaboration de politiques de sécurité détaillées couvrant l'accès, l'utilisation des systèmes SCADA, la gestion des identités, etc.
2. **Formation et Sensibilisation :** Sensibilisation des utilisateurs et du personnel à la sécurité, avec des programmes de formation et des exercices de simulation d'attaques.
3. **Gestion des Mises à Jour :** Application régulière de correctifs de sécurité et de mises à jour logicielles pour remédier aux vulnérabilités connues.
4. **Surveillance Continue :** Mise en place de systèmes de surveillance continue pour détecter et répondre aux incidents en temps réel.

La sécurisation des systèmes SCADA nécessite une approche holistique intégrant la technologie, les politiques, la formation du personnel et une vigilance continue pour faire face à l'évolution des menaces. Une gestion proactive des risques et une réponse rapide en cas d'incident sont essentielles pour assurer la résilience des systèmes SCADA.