Sécurité Internet

Objectifs pédagogiques

- Identifier et décrire les applications et spécificités des systèmes industriels
- Décrire les architectures de référence ISA-IEC 62443 et ANSSI
- Définir le processus analyse des risques et mettre en place une gestion de risques
- Identifier les vulnérabilités sur les différentes couches d'une architecture industrielle
- Décrire les principes et les applications de défense en profondeur

Prérequis

- Utiliser et réinvestir des connaissances générales en informatique et en sécurité des systèmes d'information
- Expliquer le protocole TCP/IP et mettre en oeuvre des notions sur les architectures de sécurité
- Mettre en oeuvre des notions sur les protocoles réseaux filaires et sans fil
- Aucune connaissance préalable sur les systèmes industriels n'est indispensable.

Programme détaillé

Introduction aux domaines industriels, architectures et applications associées (7 heures)

- IoT, objets connectés, smart city, industrie 4.0, …
- Composants d'un système industriel (PLC, capteurs, actionneurs, RTU, IED, …)
- Les serveurs et applications (SCADA, MES, BMS, EMS, PCS, Historian, …)
- Les protocoles industriels (Modbus, DNP3, PI, EtherNet/IP, OPC UA, …)
- Les 4 niveaux du modèle CIM (Computer Integrated Manufacturing)
- Le modèle ISA99

Présentation et démonstration des vecteurs d'attaques (10 heures)

- Protocoles liés aux réseaux sans-fil (Wifi, Bluetooth, 802.15.4, Zigbee, …)
- Protocoles industriels (Modbus, OPC, CIP, ...)
- Applications industrielles (MES, SCADA, Développement, …)
- Interconnexions avec des réseaux de sensibilité différentes (gestion, Internet, partenaires, intégrateurs, …)
- Exposition d'IHM sur Internet
- Média amovible USB/DVD
- Equipements de terrain (API/PLC, sondes, capteurs, …)

Mesures de sécurité (11 heures)

- Solutions techniques de filtrage, de cloisonnement et de détection d'intrusion
  - Firewall industriel
  - Diode et passerelle unidirectionnelle industrielle
  - Chiffrement IPSEC/SSL
  - Sondes de détection d'intrusion
  - Analyse passive de trafic

- Honeypot
- Solutions techniques de durcissement système
  - Automates de nouvelle génération certifiés CSPN (Siemens S7_1500 et Schneider M580)
  - Commutateurs Ethernet (bureautique et industriel)
  - Systèmes d'exploitation Windows et Linux
  - Applications
  - Automates programmables
- Guides ANSSI et référentiels de sécurité pour le domaine industriel (LPM, NIST, ISA/IEC, NERC, ISO 27000 …)

Sécurité Internet