AB inter NET work

Formation réseau Ethernet Industriel

INGENIERIE MISE EN SERVICE AUDIT FORMATION

EiS – la Sécurité en environnement industriel

Votre formateur (20 ans d'expérience dans les réseaux Hirschmann) vous présente dans ce cours refondu en 2018, les principes autour de la cybersécurité industrielle. Ce cours est destiné pour des participants devant prendre en compte les risques et les contraintes de la sécurité sur les réseaux industriels ainsi que les moyens de protection et les conséquences de leur mise en œuvre. Il peut aussi être un bon outil de sensibilisation (en version allégée) sur les menaces qui pèsent sur votre réseau de production. Dans ce cours, les participants apprendront les bases théoriques et tous les fondamentaux liés à la sécurité des réseaux : menaces, attaquants, depuis l'analyse de risques jusqu'aux logiciels et matériels pour se protéger. Un module est dédié aux exigences de la LPM de 2013, aux recommandations de l'ANSSI et de l'Europe en environnement industriel ainsi que les risques qui ciblent ce milieu.

Objectif du cours

Comprendre les concepts inhérents à la sécurité industrielle : menaces, cibles et attaquants, le fonctionnement de la cryptographie. Focus sur la spécificité française, ANSSI & LPM. Connaître les différents moyens de protection du réseau.

Profil des participants

Utilisateur du réseau (sensibilisation), chef de projet, ingénieur de production ou études, décideurs…

En situation de handicap ? nous contacter

Prérequis

EiB & EiA recommandé (ou équivalent)

Matériels utilisés

Fourni : switchs/routeurs & pare-feu Hirschmann (1 pour 2 pers.)

Le **PC est impératif** et à la **charge des participants** (min. 1 pour 2 pers.) avec droit admin. local (installation de logiciels et désactivation de pare-feu)

Formateur

Il intervient aussi sur le terrain (60% / 40%) - exclusivement en Hirschmann ; plus de 10 ans de compétences dans les réseaux industriels ; formateur officiel Hirschmann et certifié :

HiNE HiSE HiSP

Pédagogie / Évaluations

- Majoritairement théorique (80%) avec applications pratiques (20%)
- Quizz en fin de session pour vérification des acquis – 20 questions

Support de cours : **720 slides** couleur

Durée : **- 5 - jours** x 7 heures

Max : 10 pers. – *idéal* : 4-6pers.

Contenu – réactualisé en juillet 2023

I : Enjeux dans les réseaux industriels (291p)

A – Contexte
Différences Réseau OT vs IT. Sécurité vs Sûreté. Statistiques et les attaques dans l'actualité. La sécurité dans l'industrie ?

B – Protéger quoi contre qui ?
Attaquants et motivations. Menaces. Objectifs & Mécanismes à protéger. Cibles des attaques. Méthodologie typique d'une attaque et Anatomie de 3 attaques. Protocoles réseau fragiles / sécurisés.

C – Architecture des réseaux industriels
Architectures anciennes, actuelles, et recommandées. Modèle CIM. Industrie 4.0. Ne pas être connecté : une protection efficace ? Défense en profondeur : zones et conduites. Exemple de zones dans un système ferroviaire

D – Attaques sur les mécanismes réseau
Attaques de déni de services. Attaque du modèle OSI. Spoofing : usurpation ARP / DHCP / DNS. MAC flooding. Attaques via boucle cuivre ; sur les redondances MRP / HR /RC/RSTP ; de vlans ; de routage (RIP, OSPF, VRRP). Sur protocole automatisme.

E – Base de Cryptographie
Définitions - Notion et utilité du chiffrement. Chiffrement symétrique / asymétrique. Authentifier et sécuriser. Clé de sessions.
Fonction de hachage. Empreintes et signatures numériques. Chiffrement des échanges. Certificat numérique et utilisation. Vérification. Certificat PGP et X509. Certificats autosignés. Classes de certificats. Encodage X509. Chiffrement et Métadonnées

II : Mettre en œuvre la sécurité (243p)

A – Analyse des risques et Normes. (119p)
Cycle de vie de la sécurité. Niveaux. Stratégie de base. Evaluation des risques. Construire/évaluer son modèle d'analyse des risques. EBIOS et EBIOS RM. Normes : IEC 62443 – ISA 99 – ANSSI – Directive NIS et NIS2. Autres réglementations (Résilience des Entités Critiques, CLOUD ACT, DORA, CRA…) – les assurances cyber – Audit cyber sécurité AB inter NET work

B – Classifications des systèmes d'information industriels (60p)
Réglementation française ; Définitions. Désignation d'un OIV et liste des OIV. Arrêtés sectoriels. Obligations des OIV. Classes 1, 2 & 3. Classification des SII : Exposition, Vraisemblance, Impact. Documents importants sur le site de l'ANSSI.

C – Recommandations de l'ANSSI (64p)
13 Bonnes pratiques pour les systèmes industriels. Règles d'hygiène informatique. Renforcer la sécurité de son SI en 42 points.
Règles de mise en sécurité : profils SCADA / switch / HiOS vs Classic / pare-feu

III : Se protéger en environnement industriel (173p)

A – Protection logicielle
Mot de passe et 2FA. Chiffrement. Choix d'un VPN. Désactivez les ports USB et SMB1. Vos identifiants sont-ils diffusés? RDP. Déchiffrer les attaques de certains ransomwares. OS cloisonnés

B - Protection matérielle
Clés USB : préservatifs et inspection.
Isolation des échanges : pare-feu, tap optique, diode, passerelles. Pare-feux vs ACL. Stateful/Stateless. DPI. Comment écrire les règles ? OPC DA. UTM Stormshield. Surveillance des évènements : Syslog/SIEM. Surveillance du trafic : sFlow/Sondes passives. IDS – IPS – honeypots

C - Gouvernance
NOC-SOC-MOC. PDIS. PCA & PRA. Zero-trust. Assurances. Réagir en cas d'attaque.

En Pratique (exercices)

- Démo de RAZ d'un switch via Ethernet/IP sans droit.
- Démo d'une attaque de type ARP spoofing. Scan d'un réseau.
- Vérification d'une empreinte SHA.
- Mise en place d'OpenGPG pour chiffrer des documents et des emails. Zed! Encrypt.
- Générer un certificat X509.
- Calculer la classe OIV d'un site industriel.

Besoin d'un tarif pour une formation INTER entreprise : voir notre site web pour agenda & tarif – en INTRA entreprise, prix journalier pour 1 à 5pers. ou 6 à 10pers.

formations@abinternetwork.com – www.abinternetwork.com/formations – +33 9 72 450 350

AB inter NET work – SARL au capital de 10 000€ - SIREN 479 853 186 - RCS de Bourg en Bresse – TVA intracom : FR30 479853186 - APE 6202A
Organisme de formation **certifié Qualiopi** et déclaré sous le n° 82 01 01356 01 – DREETS de Lyon – version 2023