SIEMENS

Inzicht in informatiebeveiliging technische installaties (ITSECIND)

Short Description

Het beveiligingsbewustzijn ontwikkelen van medewerkers die op enigerlei wijze betrokken zijn bij technische installaties.

Objectives

Het beveiligingsbewustzijn ontwikkelen van medewerkers die op enigerlei wijze betrokken zijn bij technische installaties.

Door een toenemende vraag uit de markt heeft er binnen de technische automatisering een verschuiving plaatsgevonden van gesloten naar open systemen. Werd voorheen gebruik gemaakt van propriëtaire "point to point" of stand-alone systemen, tegenwoordig worden er op grote schaal gestandaardiseerde systemen en applicaties ingezet

In de praktijk is gebleken dat onder andere UNIX, Linux, Windows, TCP/IP, OPC, webtechnologieën, Microsoft Acces, Microsoft Visual Basic, Java en C kwetsbaarheden kunnen bevatten die in strijd kunnen zijn met uw security policy. Daarnaast is de interconnectiviteit enorm toegenomen en is het mogelijk geworden systemen zowel binnen als buiten de locatie decentraal op te stellen waardoor door de verschillende communicatiemogelijkheden ook op dit punt de systemen kwetsbaarder geworden zijn.
Een onderbelicht nadelig gevolg is nu dat de tot voor kort in hoge mate immuun gebleken propriëtaire topologieën en systemen nu evenals de kantoorautomatisering kwetsbaar zijn geworden voor beveiligingsincidenten.

Vooral het bewustzijnsniveau van personeel speelt een belangrijke rol in het beveiligingsproces.
De ISA-99 norm is de basis geweest voor de huidige standaards ISA/IEC 62443 of NIST en zijn ontwikkeld om inhoud te geven aan de benodigde procedures en maatregelen die genomen moeten worden. technische systemen vragen door een andere prioriteitstelling en door een langere Life Cycle een andere aanpak dan de kantoorautomatisering.

Target Group

Deze cursus is bedoeld voor iedereen die inzicht wil krijgen in de kwetsbaarheid van technische installaties als het gaat om beschikbaarheid, integriteit en vertrouwelijkheid van informatie.
Bijvoorbeeld: adviseurs en consultants, systeem integratoren, projectleiders, quality managers, programmeurs, hardware engineers, servicetechnici, eindgebruikers en installateurs.

Content

De onderwerpen in deze cursus zijn:
- Bewustzijnscan aan de hand van een aantal stellingen
- Top 10 bedreigingen en "moderne" problemen
- Praktijkvoorbeelden noodzaak informatiebeveiliging
- Verschillen tussen ICT in kantoorautomatisering en technische automatisering
- Defense in Depth mechanism uitgaande van ISA-99 model
- Security policies en procedures
- Fysieke beveiliging
- Systeem- en netwerkbeheer
- Netwerktopologieën (Secure Cell)
- Netwerkbeveiliging (firewall en Intrustion Detection System)
- Systeemrobuustheid, Patch Management en anti virus
- Remote Access en encryptie (Virtual Private Networks)
- Back-up en herstelprocedures

Prerequisites

Cursist heeft kennis van technische automatiseringsystemen en de toepassingen daarvan.

Note

Deze cursus kan ook bij u in het bedrijf plaatsvinden, er is dan meer gelegenheid tot klantspecifieke invulling.
Docent : Nederlands,
Cursusdocumentatie : Engels
De geplande cursussen kunnen alleen doorgaan bij voldoende aanmeldingen.

Type

Face-to-face training

Duration

1 day

Language

nl