

Yritysverkkojen tietoturva

Kurssin kesto: 3 päivää

Kurssityyppi: Luento

Kurssikuvaus: Yritykset käyttävät useita eri puolustusmekanismeja suojellakseen tietoverkoissa olevia järjestelmiään. Nämä mekanismit voivat olla joko teknisiä tai hallinnollisia. Kurssin aikana opiskelija tutustuu käytännön esimerkkien tai demojen avulla tietoturvan toteuttamiseen yritysverkoissa.

Kurssin kohderyhmä: Kurssi soveltuu henkilöille, jotka haluavat oppia yritysverkkojen tietoturvan perusteet konseptitasolla. Tämä kurssi on yleissivistävä ja soveltuu ensimmäiseksi kosketukseksi tietoturvaamisen maailmaan.

Kurssin tavoite: Tämän kurssin tarkoituksena on antaa opiskelijalle hyvät perustiedot yritysverkkojen tietoturvan toteuttamiseksi. Kurssilla käsitellään tietoturvaa useilla eri tasoilla, jotta opiskelija ymmärtää syy-yhteydet toimintamallien tai tekniikkojen käyttämiseen. Kurssin jälkeen opiskelija on hyvät edellytykset ymmärtää yritysverkkojen tietoturvatarpeita konseptitasolla ja ennen kaikkea antaa useita näkökulmia verkkotietoturvan käsittelemiseen.

Kurssin sisältö:

1. Päivä

Tietoturvan historiaa

- Aikajana
- Sodan tietoturvan vauhdittajana
- Nykypäivän tietoturva

Tietoturvallisuuden ulottuvuudet

- Yhteiskunta
- Maa
- Lainsäädäntö
- Yritys
- Käyttäjä

Hallinnollinen tietoturva

- Tietoturvan määritelmiä
- Tietoturvan eri tasot
- Identiteetin määrittely

- Tietoturvapoliitiikan perusteet
- Tietoturvariskien analysoiminen

Salaustekniikoiden perusteet

- Salaustekniikoiden historia
- Symmetrinen ja asymmetrinen salaus
- Salauksen vahvuus
- Salauksen käyttötapoja
- Tunnetuimmat salausalgoritmit lyhyesti
 - DES ja 3DES
 - AES
 - RC4
 - RSA
 - Diffe-Hellman
 - Blowfish

Tietoturvahyökkäykset

- Hyökkäyksien kohteet
- Hakkeroinnin historia
- Hakkeroinnin menetelmiä
- palvelunkieltohyökkäykset
- Haittaohjelmat
- Phishing
- Social Engineering

2. Päivä

Rajapintojen tietoturva

- Käyttäjä
- Käyttöjärjestelmä
- Rajapinnat oheislaitteisiin
 - Keyloggers
 - Infrapunayhteydet
 - Bluetooth
- Käyttöjärjestelmät
 - Käyttöjärjestelmien yleisiä heikkouksia
 - Microsoft Windows
 - Unix ja Linux
 - Novell
 - Symbian OS
 - Palm OS
- Verkon aktiivilaitteiden käyttöjärjestelmät

- TCP/IP-protokollan tietoturvan lyhyt tarkastelu
 - IP
 - ICMP
 - TCP
 - UDP
- IPv6 tietoturvan kannalta
- Reitityksen tietoturva
 - RIP ja RIPv2
 - OSPF
 - EIGRP
 - IGRP
 - BGPv4
- MPLS-tietoturva
- Sovellusten tietoturva

Tietoverkon tietoturvakomponentit

- Käyttäjärjestelmän toiminta
- Lähiverkkokytöiden tietoturva
- Palomuurijärjestelmät
- Reitittimien ja reitittävien kytkinten tietoturva
- IDP ja IPS-järjestelmät

Langattomien verkkojen tietoturva

- Oheislaitteiden tietoturva
 - Car Whispering
 - Bluesnarfing
- WLAN Standardit lyhyesti
- WEP
- WPA
- WPA2
- GSM Tietoturva
- GPRS/EDGE-tietoturva
- UTM-tietoturva

Etäyhteyksien tietoturva

- Etäyhteystarpeen määrittäminen
- Soittosarjat
- Modeemi
- ISDN
- VPN-konseptina
- PPTP
- IPSEC

- L2TP+IPSEC
- SSL
- MPLS-VPN

Todentaminen

- Todentamisen tarpeen määrittäminen
- Salasanamenetelmät
- Token-menetelmät
- Biometrinen tunnistaminen
- Todennuspalvelimen käyttäminen
- Radius
- Tacacs+
- Kerberos
- Digitaliset varmenteet
- PKI

3. Päivä

Datan sisällön suodattaminen

- Sisällön suodattamisen tarpeet
- Sisällön suodattamisen topologia
- Virukset
- Madot
- Muut haittaohjelmat
- WWW-suodatus
- URL-suodatus
- HTTP-suodattaminen
- SSL-liikenteen suodattaminen
- Roskapostin suodattaminen

Verkon hallinnan tietoturva

- Verkonhallinnan ulottuvuus
- Verkonhallinnan järjestäminen
- Verkonhallinnan työkalujen tietoturva
- SNMP ja RMON-tietoturvaa
- Lokitiedon kerääminen

Tietoturvan analysointi

- Tietoturva prosessina
- Tietoturvan kartoittaminen
- Haavoittuvuuksien hallinta
- BS7799 - Turvallisen tietojärjestelmän määritelmä

- Tietoverkon tietoturvan kartoittaminen
- Skannaukset
- IDP-analyysi
- Haavoittuvuuksien hallintaohjelmistot
- Lokitietojen analyysiin perustuvat järjestelmät