

Operaattoriverkkojen tietoturva

Kurssin kesto: 4 päivää

Kurssityyppi: Luento + laboratorioharjoituksia

Kurssikieli: Luennot suomeksi, materiaali suomeksi (tarvittaessa myös englanniksi)

Kurssikuvaus: Operaattoriverkon tietoturva on luonnollisesti vielä tärkeämpi kokonaisuus, kuin yksittäisen yritysverkon tietoturva. Kulkeehan operaattoriverkon kautta huomattavan monen yrityksen liikennettä. Tämän vuoksi tietoturvaan pitää kiinnittää asianmukainen huomio.

Operaattoriverkossa tietoturvan muodot ovat kuitenkin hyvin erilaisia verrattuna yritysverkon tietoturvaan. Vaikka uhat ovat periaatteessa samanlaisia, niitä vastaan varautuminen ja niiden torjunta on hyvinkin erilaista.

Kurssin aikana tarkastellaan intensiivisesti erilaisia hyökkäysmuotoja ja mitä niille voidaan tehdä operaattoriverkossa. Samoin käydään läpi operaattoriverkon laitteiden parhaita konfigurointi- ja ylläpitotapoja tietoturvan osalta. Tärkeä fokusalue on hallittu ja organisoitu toiminta erilaisten hyökkäysten, niin tunnistettujen, kuin tunnistamattomienkin aikana.

Kurssin sisällöstä esimerkit ja laboratorioharjoitukset on toteutettu Ciscon laitteilla. Suurin osa sisällöstä on kuitenkin geneeristä asiaa, joka sopii monen merkellisillä laitteilla toimiville operaattoreille.

Kurssin kohderyhmä: Operaattoriverkon suunnittelu-, ylläpito- ja hallintatehtävissä olevat henkilöt. Kurssin käyneillä henkilöillä on valmiudet torjua erilaisia uhkakuvia operaattoriverkossa itsenäisesti reaaliajassa.

Kurssin tavoite: Käydä läpi nykyisten operaattoriverkkojen tietoturvaan liittyviä skenaarioita sekä opettaa, miten uhkia voidaan ehkäistä ja torjua.

Kurssin sisältö:

Tietoturvan kokonaiskuva

- Mitä suojataan ja miksi?
- Operaattoriverkon tietoturvan toimenpidelista
- Erilaiset uhkakuvat, hyökkäysten kustannukset
- Uhkien globaali seuraaminen

- Valmistajien tietoturvalistat
- Geneeriset tietoturvaorganisaatiot

Pohja kuntoon I . reitityksen suojaaminen

- Miksi reititysprotokollia pitää suojata?
- Hyökkäykset reititystä vastaan
- IGP-reitityksen suojausmahdollisuudet
- EGP-reitityksen suojausmahdollisuudet

Pohja kuntoon II . reitittimien itsensä suojaaminen + lokit

- Mitä oikein suojataan?
- Pääsynhallinta
- Prosessien hoitaminen
- Reitittimen tilan tarkkailu
- Reitittimien suojaaminen eri valmistajien mekanismeilla

Suodatus verkon reunalla

- IETF:n säännökset suodattamisesta
- Kontrolliliikenteen suodatus
- Muun liikenteen suodatus
- Lähdeosoitteiden tarkistaminen

Datanvälityksen tietoturvamekanismit

- Liikenneviemärit (Sink Hole), takaisinsironta (Backscatter), jäljitys (Traceback), liikennesuntti (Black Hole Shunt) ja skruppaus (Scrubbing)
- Liikenneviemärien tehtävät
- Jätteen analysointi eri tekniikoilla
- Viemärien rakentaminen ja käyttö
- Takaisinsironnan toiminta

- Jäljityksen toiminta
- Liikennesuntti
- Skruppaus

Madot . hillitön kasvu vai lääkekuuri?

- Verkkomadon anatomia ja leviämistavat
- Matojen kaivaminen ja lääkitseminen
- Toiminta hyökkäyksen aikana

DoS ja DDoS . perusluokan työkaluja

- Tunnettuja (D)DoS-hyökkäyksiä
- Hyökkäyksen havaitseminen
- Toiminta hyökkäyksen aikana

Botnetit . vähän lisää haastetta

- Mikä on botnet? Miten se luodaan?
- Botnettien muodostama uhka
- Torjuntakeinoja botnettejä vastaan
- Toiminta hyökkäyksen aikana