Tietoverkkosodankäynti

Kurssin kesto:
3 päivää

Kurssin hinta:
2000 € + alv 24%

Tietoverkkosodankäynninkurssilla havainnollistetaan mikä kybersodassa on pelin henki –Mikäli et ymmärrä hyökkäystä, et pysty kunnolliseen puolustukseen. Finlaysonin tehdasrakennuksen pohjakerroksessa, vahvojen kiviseinien suojassa, on mahdollista simuloida aitoja tietoverkkohyökkäyksiä. Suljettu ympäristö ja rakenteellisesti todenmukaiset tietoliikenneverkot tarjoavat ainutlaatuisen mahdollisuuden harjoitella kyberuhkia vastaan puolustautumista käytännössä. Sodankäynti on jaoteltu kolmeen eri kategoriaan kohderyhmän mukaan; peruskurssi, jatkokurssi ja jatkokurssi viranomaisille. Lisäksi tarjoamme tietoliikenteen kertauspäivää johdatuksena varsinaiselle tietoverkkosodankäynninkurssille. Kurssia on järjestetty jo yli 10 vuoden ajan erikokoisten yritysten henkilöstöille aina viranomaistasoa myöden. Yrityskohtaisesti räätälöity tietoverkkosodankäynninkurssi mahdollistaa asiakkaan oman ympäristön uhkien käsittelyn. Asiakaskohtaisesti räätälöityjen kurssien hinnat neuvotellaan tapauskohtaisesti kurssihintoihin pohjautuen. Suuremmilla osalllistujamäärillä koulutuksen yksikkökustannukset ovat luonnollisesti matalammat, toteutukset alk. 3500 €/päivä (alv 0 %). Hanselin asiakkaille erikoishinnoittelu Sovelton puitesopimuksen pohjalta.

Kohderyhmä

Tietoverkkojen turvallisuudesta vastaavat, verkkoja ja järjestelmiä operoivat henkilöt.

Tavoite

Osallistujat saavat käsityksen siitä, mitä tietoverkkosodankäynti ja -hyökkäykset ovat. Suljetussa ympäristössä pystytään käytännössä harjoittelemaan tilanteita, joissa hyökkäys on käynnissä. Kurssilaiset pääsevät kokemaan tilanteita, joita ei voida toteuttaa tuotantoympäristössä ja oppimaan miten toimitaan erilaisissa virusten ja tunkeutujien aiheuttamissa ongelmatilanteissa.

Esitiedot

Tietoliikenteen kertauspäivä

Koulutuksen sisältö

Tietoturvan kehitysnäkymät

- Ympäristön muutokset
- Uudet uhkakuvat ja niiden analysointi
- Tietoverkkoterrorismi
- Strateginen isku tietoverkoissa

Tietoverkkosodankäynti

Kohteet
Keinot
Suomalaisen yhteiskunnan haavoittuvuudet

Internetin rooli

Tiedon lähteenä
Ohjelmistojen lähteenä

Virukset ja haittaohjelmat

Viruksia sietävät ympäristöt
Virukset poikkeusoloissa

Verkon aktiivilaiteet

Hyökkäyksen havaitseminen

IDS, palomuurit
Liikenteen profilointi

Toiminta puolustustilanteessa

Miten tunnistaa hyökkäys
Miten estää se

Varautuminen ja vastatoimenpiteet

Torjuntatyökalut ja niiden käyttö

Verkkoanalysaattorit
IDS-ohjelmistot

Hyökkäystyökalut ja niiden käyttö

Tietoverkkosodankäynnin harjoitus

Omien järjestelmien suojaaminen
Tiedon keruu
Salakuuntelu
Tiedustelu
Torjuntatoimenpiteet
Hyökkäys erilaisilla työkaluilla
Palvelunestohyökkäys
Virushyökkäys
Torjuntatoimenpiteet

Hyökkäysten simulointia ja tutkintaa

Hyökkäysten analysointi

Onnistuminen
Jäljet
Vahingot
Vastatoimet

Mitä opimme

Miten kehitämme organisaatiotamme

Kurssimyynti

kurssit@contrasec.fi
puh. 03 3123 7133