KIBERNETINIO SAUGUMO PAGRINDAI ORGANIZACIJOJE

Kibernetinio saugumo pagrindų organizacijoje mokymai susideda iš teorinių paskaitų ir praktinių užsiėmimų.

Kursų esmė - pažinti kibernetinio saugumo svarbą, grėsmes ir priežastis ir pasirengti praktiškai atremti kibernetines atakas.

Pirmosios dienos mokymų turinys universalus, jis skirtas bendram kibernetinio saugumo suvokimui, grėsmių ir priežasčių išsiaiškinimui. Dalyvauti geriausiai tinka įmonių vadovams, IT padalinių vadovams bei informacinių sistemų administratoriams.

Antrosios dienos mokymų metu kibernetinio saugumo teorija kombinuojama su praktine demonstracija ir individualių užduočių atlikimu laboratorijoje. Numatytos užduotys nesudėtingos, specialus pasirengimas nėra būtinas. Dalyvauti geriausiai tinka IT padalinių vadovams ar informacinių sistemų administratoriams.

Po mokymų visiems dalyviams išduodami dalyvavimą patvirtinantys pažymėjimai.

TRUKMĖ: 1-2 dienos
(Galima dalyvauti visomis arba tik pasirinktą dieną)

KAINA: 400-750 EUR/dalyviui
(kaina vienai dienai – 400 EUR/dalyviui, kaina už abi dienas – 750 EUR/dalyviui)

DĖSTYMO KALBA: lietuvių

Kibernetinio saugumo mokymai
Tel.: +370 621 19419
Justas@cyberdefence.lt
https://cyberdefence.lt

mitas.lt

Pirmos dienos tema:
„Internetas kaip kritinė infrastruktūra, Lietuvos kibernetinių grėsmių žemėlapis, Kibernetinių incidentų metodai“

Potemės:

1. Internetas ir kibernetinio saugumo perspektyva
- Internetas kaip kritinė infrastruktūra;
- Prielaidos kibernetinėms grėsmėms;
- LT interneto tarptautinis junglumas;
- Incidentų mastas Lietuvoje (CERT-LT, LITNET);

2. “Pasižymėję”, naujausi kibernetiniai incidentai ir jų metodai
- Lietuvos kibernetinių grėsmių žemėlapis; (***Laboratorinis***)
- „WannaCry“ Lietuvoje;
- 1.35 Tbps DDOS ataka prieš Github;
- Valstybinių įstaigų puslapiai „skirti“ kriptovaliutoms kasti !?;
- Stuxnet virusas ir jo atmainos;
- Spamhaus DDOS metodai;

3. Interneto protokolų saugumo spragos
- Tinkamas IP adresų dalinimas užkerta kelią kibernetinei atakai!?
- Apsauga nuo TCP atakų;
- DNS įrašų keitimas;

4. Kibernetinių atakų tipai (*Gyva demonstracija*). Botnet rinka.
- Brute force; SQL injection;
- Cross Site Scripting;
- Man-in-the-midle;
- Botnet tinklo kūrimas, rinka, kainos, panaudojimas atakoms;

5. Saugumo priemonių taikymas
- Simetrinis, Asimetrinis šifravimas ir algoritmų spartos;
- Sertifikatas, PKI, elektroninis parašas;
- Autentifikacija, Challenge-response, sesijos raktas;
- Certificate Signing Request generavimas; (***Laboratorinis***)
- Viešo ir privataus rakto generavimas; (***Laboratorinis***)
- Raktų poros panaudojimas SFTP, SSH; (***Laboratorinis***)

6. Kibernetinių incidentų valdymo reglamentavimas Lietuvoje, incidentų registravimas
- Kibernetinio saugumo būklės gerinimas;
- Pasaulinis CERT modelis;
- Grėsmių nacionaliniam saugumui vertinimas.

Antros dienos tema:
„IT saugumo pagrindai organizacijoje, SME IT infrastruktūros saugumo didinimas, Informacinių technologijų saugos atitikties vertinimas“

Potemės:

1. IT saugumo pagrindai organizacijoje
(Diskusija su dalyviais)
- Perimetro apsauga;
- Ugniasienės kontrolinis sąrašas;
- Darbo vietų saugumas;
- Sistemų spragų „užtaisymas“;
- Anomalijų tikrinimas;
- Slaptažodžių politika;
- Mobiliojo telefono/planšetės apsaugos pagrindai;
- El. pašto apsaugos pagrindai;
- Vidinės ir išorinės saugumo rizikos;

2. Small Medium Enterprises IT infrastruktūros saugumo didinimas
- Realaus organizacijos IT tinklo analizė; (***Laboratorinis***)
- IT tinklo modernizavimas, stebėjimas; (***Laboratorinis***)
- Saugumo zonos;
- Tinklo segmentavimas (VLAN); (***Laboratorinis***)
- saugus DHCP, Proxy konfigūravimas; (***Laboratorinis***)
- VPN rūšys (OpenVPN konfigūravimas); (***Laboratorinis***)
- EMAIL pasirašymas kliento pusėje; (***Laboratorinis***)
- EMAIL pasirašymas serverio pusėje (TLS, DKIM), DMARC;
- Apache vs NGINX vs Internet information services (IIS);
- HSTS naudojimas; (***Laboratorinis***)

3. Ugniasienės ir atakų prevencijos sistemos
- OSI 3 lygio ugniasienė;
- Proxy ugniasienė;
- Unified threat management ugniasienė; (***Laboratorinis***)
- Firewall vs IDS vs IPS;

4. Informacinių technologijų saugos atitikties vertinimas
- Įsilaužimų scenarijai;
- Ethical hacking žingsniai; (***Laboratorinis***)

5. Programinės įrangos saugumas
- Pažeidžiamumai soft’e;
- Pažeidžiamumai hard’e;
- Programavimo principai, kuriuos taikant didinamas bendras sistemos saugumas;
- Gerosios web deployment praktikos.

Kibernetinio saugumo mokymai
Tel.: +370 621 19419
Justas@cyberdefence.lt
https://cyberdefence.lt

mitas.lt