4 programa
Mažos, vidutinės ir didelės apimties elektroninių sistemų ir tinklų saugaus eksploatavimo organizavimas

Mažos, vidutinės ir didelės apimties elektroninių sistemų ir tinklų saugaus eksploatavimo mokymo programa turi apimti įvairių sektorių, dydžių ir konfigūracijos sistemas, praktinę problemų sprendimo būdų analizę ir efektyvų taikymą.
Lietuvoje fiksuoti incidentai, kurių metu valstybės institucijų darbuotojams buvo siunčiami laiškai, imituojantys kompiuterio tinklo administratorių pranešimus, informuojančius apie pašto sistemų atnaujinimus. Pateiktos nuorodos vedė į svetainę, imituojančią institucijos elektroninio pašto paslaugos tinklapį. Taip pat buvo sulaukta daug nusiskundimų iš organizacijų atstovų dėl gaunamų imituojamų vadovų elektroninių laiškų, kuriuose stengiamasi įtikinti už finansines operacijas atsakingą personalą atlikti piniginės perlaidas į atakos iniciatorių sąskaitas. Tai rodo nepakankamo lygmens įvairios apimties elektroninių sistemų ir tinklų saugaus eksploatavimą. Programa orientuota į šių išteklių kibernetinio saugumo praktinį organizavimą, užkirsiantį kelią kibernetinėms atakoms.
Nurodyta problematiką nagrinėjama dalimis:
1. Vietinių ir nuotolinių darbo vietų analizė ir geroji praktika;
Atlikus vietinių ir nuotolinių darbo vietų organizavimo analizę, pateikiami naujausi apsaugos būdai saugiai dirbti nuotoliniu būdu neprarandant funkcionalumo.
2. Socialinės inžinerijos metodai, kontrpriemonės;
Nagrinėjami socialinės inžinerijos metodai, aiškinama, kaip juos atpažinti, taikyti ar naudoti.
3. Saugus duomenų organizavimas įmonės viduje;
Nagrinėjamos duomenų šifravimo galimybės, NFS, SMB ir tinklinės sistemos, jų apsauga ir parametrizavimas.
4. Komercinių ir atviro kodo programinės ir aparatinės įrangų organizavimas saugumo aspektu;
Nagrinėjamos komercinės ir atviro kodo kibernetinės saugos sistemos, pristatomi privalumai ir trūkumai, parengiamos rekomendacijos skirtingiems informacinių sistemų valdytojams.

5 programa
Sistemų kontrolė ir valdymas esant kritinėms, aukšto neapibrėžtumo situacijoms

Sistemų kontrolės ir valdymo, esant kritinėms, aukšto neapibrėžtumo situacijoms, mokymuose turi būti parengtos praktinės situacijas, kuriose būtų kritinių momentų, aukšto sistemų destabilizacijos lygmens ir nestandartinių atakų. Šios dedamosios, turi užtikrinti greitą ir korektišką reakciją (atsaką) į iškilusias kritines kibernetinio saugumo situacijas. Mokymai turi apimti skirtingo lygmens kibernetines situacijas – nuo bandymo įsilaužti į sistemą iki pilno jos perėmimo. Praktinėje plotmėje turi būti išnagrinėti ir pristatyti realūs nacionaliniai ir tarptautiniai įvykiai.
Programos sudedamosios dalys:
1. Įrenginių apsauga, taikomosios programinės įrangos analizė ir saugus naudojimas;
Nagrinėjama įrenginių apsauga programiniu ir aparatiniu požiūriu, analizuojamos sistemų anomalijos, jų dinamika.
2. Meta duomenų agregavimo ir analizės panaudojimo atvejai;
Analizuojama greitaeigė duomenų agregacija ir analizė, atakos pavojingumo nustatymas.
3. Atakų stadijos, jų poveikis kompiuteriniam tinklui ir įterptinėms sistemoms, prevencijos būdai;
Remiantis naujausiais moksliniais šaltiniais, nagrinėjamos atakų stadijos, jų įtaka tinklui ir jį formuojančiai periferijai (įterptinėms sistemoms), atakų atpažinimas ir prevencijos būdai.
4. Atakų stadijos, jų poveikis sistemoms, prevencijos būdai.
Nagrinėjami skirtingų atakų stadijų bruožai, nusakantys atakos pavojingumą turimoms sistemoms, pateikiami atakų prevencijos metodai.