Изазови информационе безбедности – прошлост, садашњост, будућност

Информациона безбедност (InfoSec) је широка област информатике које се бависпречавањем неовлашћеног приступа, употребе, откривања, модификације, чувања или уништавања информација. Главни циљ информационе безбедности је уравнотежена заштита поверљивости, интегритета и доступности података. Ово излагање упознаће присутне са кратким историјатом и тренутним стањем на пољу информационе безбедности, методологијом напада на информационо- комуникационе ресурсе и на крају са погледом у будућност.

Почетком друге половине прошлог века, комерцијализацијом рачунара и рачунарских мрежа, свет се упознао са новим опасностима – безбедносним ризицима у информационо комуникационим системима. Злоупотребе су се углавном манифестовале у виду експлоатације безбедносних пропуста, неовлашћеног коришћења ресурса и креирања злонамерних програма (малвера) чиме су били угрожени рачунарски ресурси и подаци на њима.

Почетком новог миленијума информационо-комуникационе технологије имплеме-нтирају се свуда – од уређаја који се користе у кући попут беле технике и алармних система, преко оних који се користе у свим гранама привреде – у банкарству, администрацији, здравству, индустрији, све до оних који се користе у полицији, војсци, саобраћају, енергетици и осталим критичним инфраструктурним и безбедносним гранама једне нације. Овим се поље примене информационе безбедности знатно проширило и добило још већи значај у савременом друштву. Сходно трендовима у привреди повећао се и број неопходних високо-школованих стручњака у области информационе безбедности – од стандардних позиција које подразумевају послове на унапређењу система заштите и/или примени тих система, све до нових послова попут етичког хакинга.

Етички хакинг подразумева примену метода и средстава које користе злонамерни нападачи приликом тестирања безбедности система кроз пет специфичних фаза: извиђање, скенирање, добијање приступа, одржавање приступа и прикривање трагова. Блиска будућност нам доноси још већи број паметних уређаја и „ствари“ на интернету, развој вештачке интелигенције и роботике, квантне рачунаре, крипто- валуте, самовозеће аутомобиле, паметне куће, паметне градове и др.

Колико смо спремни да их прихватимо и која улога наставника информатичких и рачунарских предмета у свему томе? Може се закључити да је поље информационе безбедности значајно поље информатике које већ више година уназад штити како рачунаре и рачунарске ресурсе тако и привреду и инфраструктуру. Такође, технички аспект информационе безбедности јесте јако битан, али је једнако битан и људски фактор и едукација ради повећања свести о безбедности.