Küberkaitsjad korraga kahes ülikoolis

9. oktoober 2011 - 23:56 Autor: AM

(Arvutimaailm 6/11)

Arvutiturvalisus, krüptograafia, ID kaart, e-valimised, NATO küberkaitsekeskus ja palju muud sama teemaga seonduvat on Eesti IT valdkonna üks suuremaid edulugusid. Väikese ja paratamatult väheolulise riigina oleme edukalt kasutanud just seda valdkonda enesereklaamiks ning oma võimekuse ja tähtsuse tõestamiseks.

Pronkssõduri saaga paljudest kasulik/kahjulik aspektidest jäi tolmu settides pinnale üks, võibolla ainus Eesti jaoks selgelt kasulik sündmustejada: küberrünnakud, nende tõrjumise mütologiseeritud eepos ja poliitikute blufi piiripealse kampaania edukas väljamäng. Tekitasime maailmas palju suuremat – seejuures positiivset – meediakajastust ja huvi, kui nö harilikud rahutused seda kunagi oleks suutnud.

Vähe küberspetsialiste

Kuigi Eesti IT-maastikul on küberkaitse tõepoolest üks edukamaid valdkondi, on ka siin sama mure, mis teistes keerukates valdkondades: väga vähe tõeliselt kompetentseid spetsialiste.
Veel mõned aastad tagasi oli meie ülikoolides seis selline, et küberkaitse eriala-aineid õpetati eeskätt valikainetena ja suhteliselt süsteemitult niiöelda harilike infotehnoloogia erialade tudengitele. Spetsialiste kasvas peale eeskätt sedajagu, kui neid tippude poolt ükshaaval juhendati ja valdkonda harjutamiseks tööle võeti.
Olukorra parandamiseks käivitas Tallinna Tehnikaülikool kolm-neli aastat tagasi küberkaitse “poolmagistriõppekava”, st magistrikava spetsialiseerumist, kus umbes pool ainetest olid spetsiaalsed küberkaitse-ained. Eriala muutus väga populaarseks ning kaks aastat tagasi võeti küberkaitse õpetamine ette suuremalt: Tallinna Tehnikaülikool ja Tartu Ülikool käivitasid kahe peale ühise rahvusvahelise küberkaitse- magistriõppekava, kus peale üldainete on pea kogu kaheaastane õppetöö suunatud valdkonna eriainetele.
Tegu on siis kaheaastase rahvusvahelise kavaga, mis tähendab täielikult inglisekeelset õpet ja ca kolmandiku ulatuses välistudengeid.

Kaks ülikooli korraga

Kava lõpetajad saavad kaks diplomit: nad on nii Tartu Ülikooli kui Tallinna Tehnikaülikooli lõpetajad. Praktiline õppetöö toimub samuti mõlemas ülikoolis: esimene ja kolmas semester Tallinnas, teine semester põhiliselt Tartus. Neljandal semestril saavad tudengid ise valida, kus nad resideeruda soovivad.
Küberkaitse ei erine “tava”-ITst mitte ainult oma nime poolest. Päris sisuliselt on tegu väga interdistsiplinaarse erialaga, kus humanitaaria on sama oluline, kui tehnoloogia. Selgelt üle poole ainetest on nii või teisiti seotud inimeste, sotsioloogia ning haldusjuhtimisega.

Pooleldi humanitaarne

Tegelik küberkaitsjate töö nimelt ongi suurel määral seotud just ründajate huvidest ja motivatsioonidest arusaamisega ning vastavalt sellele inim-vastumeetmete ettevõtmisega. Heaks näiteks on Tehnikaülikoolis äsja doktoritööd kaitsnud Rain Ottis, kelle uurimistöö NATO küberkaitsekeskuses on niiöelda eeskätt praktilise sotsioloogia, mitte niivõrd tehnoloogia vallast.
Sestap ka magistriprogrammi jaotus Tallinna ja Tartu vahel: Tallinnas loevad aineid peamiselt just pankade, telekomi, riigisfääri ja NATO küberkaitsekeskuse praktikutest tippspetsialistid, Tartus õpetatakse rohkem sotsiaal- ja humanitaarala aineid ning matemaatilise iseloomuga krüptograafiat. Lisaks saavad tudengid osa aineid valida IT kolledžist.
Nagu eelneva põhjal võiks arvata, võetaksegi küberkaitse erialale õppima mitte ainult tehnolooge, vaid samamoodi ka majaduse, juriidika ja halduskorralduse tudengeid, kellel olemas huvi tehnoloogia vastu ning valmisolek end ses osas täiendavalt harida. IT-tausta puudumisel saab tudeng esimesel kahel semestril valida aineid, mis ei nõua spetsiaalseid eelteadmisi ja viivad tudengi tehnoloogiavaldkonda jõukohaselt sisse.

Laia profiiliga

Lõpetajate esmane rakendus administratiivsel poolel on eeskätt infoturbespetsialisti ja infoturbejuhi amet, tehnoloogia poolel aga süsteemiadministraator, serveri- ja võrguadministraator. Saadav haridus on väga hea baas ka ametikohtadel, mille põhifookus ei ole turvaküsimustel, vaid asutuse/ettevõtte IT-korraldusel.
Küberturbealased nõutavad teamised sellise profiiliga ametikohtadel on väga laiaulatuslikud: peab suutma erinevaid komponente (tarkvara, seadmed, teenused, protsessid) suuremaks turvavajadustele vastavaks süsteemiks kokku panna, valdama turvalise tarkvara-arenduse põhimõtteid, tundma võrguprotokolle, operatsioonisüsteeme ja rakendustarkvara, oskama neid administreerida, tundma nõrkusi ja ründamise võimalusi, suutma hinnata infoturbe alaseid riske ja oskama neid hallata, olema kursis rünnete motivatsiooni ja tehnikaga, suutma anda ülevaateid strateegilistele juhtidele, olema kursis infoturvet ning arvutikuritegevust reguleeriva seadusandlusega, suutma juhtida infoturbeintsidentide operatiivset lahendamist jne jne.

Taustal käib pidev rünnak

Reaalses elus on enamvähem kõik arvutisüsteemid pideva leebe "taustarünnaku" all ning suuremaid ja põnevamaid süsteeme uuritakse ja rünnatakse mitmete gruppide poolt puht-majanduslikest eesmärkidest motiveerituna ja täiesti professionaalselt. Iga kaitse toob kaasa uued viisid rünnakute suunamisel. Iga paari aasta järel tekivad uued riskisfäärid, millega tõsisemalt tegeleda: viimase aasta jooksul on märgatav huvi suundunud tööstussüsteemide - energeetika, vabrikud jms - häkkimisvõimaluste uurimisele ja vastupidi, nende haavatuse uurimisele ning kaitsemeetodite väljatöötamisele.
"Küberkaitse" sõna kõlab küll pehmelt - justkui mitte-päris-reaalne "küber" ja passiivsusele viitav "kaitse", kuid tegelikult on asjad üpris

vastupidi. IT-valdkonnas on inimeste käed väga vähe seotud ja nad võtavad kaunis kergekäeliselt ette tõsiseid rünnakuid pankade ja tervete riikide vastu (mis oleks mõeldamatu automaatide ja tankidega!), samuti kehtib tihtipeale vana tõde, et parim kaitse on rünnak.

TANEL TAMMET
TTÜ võrgutarkvara professor

- Tegijad
- Turvalisus