Gegužės 17 d. minima Pasaulinė informacinės visuomenės diena. Šiais laikais vis aktualesnė kibernetinė sauga. Šioje srityje dirba kelios Lietuvos mokslininkų grupės ir jau gali pasiūlyti verslui inovatyvių paslaugų ir produktų – nuo unikalaus ankstyvojo įsiveržimo nustatymo metodo, dirbtiniu intelektu pagrįsto naujų kenksmingų programinių kodų aptikimo iki virtualių kibernetinio saugumo mokomųjų platformų.

Kol atakai dar rengiamasi

„Kibernetinės atakos didėja ir stipriai paveikia ne tik politinį, visuomeninį, bet ir ekonominį gyvenimą. Nepaisant įvairių tradicinių apsaugos priemonių, nuo gerai parengtų atakų apsiginti gana sudėtinga. Kaip rodo pastarųjų metų atakų pasaulyje analizė, naudojamos tradicinės sistemos iš esmės pradeda reaguoti tik tada, kai ataka jau prasidėjusi ir jos sustabdyti nebeįmanoma", – pabrėžė Kauno technologijos universiteto (KTU) Elektronikos inžinerijos katedros docentas dr. Saulius Japertas.

KTU mokslininkų grupė, vadovaujama dr. S. Japerto, sukūrė ankstyvojo kibernetinio įsiveržimo nustatymo metodą. Jis leidžia panaudojus atitinkamą loginio filtro sistemą dar prieš ataką nustatyti, kad jai rengiamasi, ir imtis apsaugos priemonių.

Unikalus produktas – įranga ir programos – sukurtas bei išbandytas bendradarbiaujant su kibernetinės saugos srityje dirbančia įmone „Media inovacijos". Ankstyvojo kibernetinio įsiveržimo metodas, šių metų kovą pristatytas Kijeve vykusiame Informacinių ir ryšių technologijų inovacijų forume, sulaukė didelio Ukrainos įmonių ir institucijų susidomėjimo.

Daiktų interneto iššūkiai

KTU Informatikos fakulteto Kompiuterių katedros profesorius Egidijus Kazanavičius atkreipė dėmesį į kibernetinio saugumo grėsmes, susijusias su augančia daiktų interneto technologijų plėtra. Jos skverbiasi į visas sritis. Tačiau į tokias mažas daiktų kompiuterines sistemas sunkiau įdiegti rimtą programinę įrangą, apsaugančią nuo virusų.

"Santakos slėnyje atliekami tyrimai, skirti stebėti ir vertinti galimas rizikas bei pažeidimus, informuoti apie juos bei priimti atitinkamus sprendimus", – pasakojo KTU Realaus laiko kompiuterių sistemų centro direktorius prof. E. Kazanavičius.

Realaus laiko kompiuterių sistemų centras glaudžiai bendradarbiauja su verslu diegdamas naujoves. Pavyzdžiui, kartu su kompanija „Teo" sukurta vaizdo turinio šifravimo ir apsaugos nuo vagysčių sistema įdiegta pernai. Su įmone „LL Optic" sėkmingai bendradarbiauta kuriant išmaniuosius šaldytuvus, taip pat vadinamuosius maistomatus, demonstruotus ir

parodoje Milane.

„Horizonto 2020“ projekto pagrindu KTU mokslininkai kartu su partneriais – Švedijos mokslinių tyrimų institutu RISE ir Linšiopingo universitetu bei Vilniaus Gedimino technikos universitetu (VGTU) ir Lietuvos registrų centru – kuria IT kompetencijos centrą, orientuotą į mokslo ir verslo bendradarbiavimą. Vienas artimiausių tikslų – prisijungti prie Europos Sąjungos daiktų interneto klasterio.

Stebėti ir vertinti

Vienas įdomiausių Vytauto Didžiojo universiteto (VDU) Informatikos fakulteto įgyvendintų projektų kartu su partneriais Mykolo Romerio universitetu ir Lietuvos kibernetinių nusikaltimų kompetencijų ir tyrimų centru – parengta ir išbandyta informacinės erdvės stebėjimo koncepcija, leidžianti efektyviai įvertinti situaciją bei sukurti sistemą, skirtą už valstybinės saugumą atsakingoms struktūroms bei verslo ir mokslo partneriams kartu stebėti informacinę erdvę saugumo ir komerciniais tikslais, nepažeidžiant informacijos saugumo reikalavimų.

Pasak Taikomosios informatikos katedros profesoriaus Tomo Krilavičiaus, šiam projektui prielaidas sukūrė kitas VDU projektas, per kurį sukurta viešai prieinama infrastruktūra lietuvių kalbos analizei. Ji gali būti naudojama įvairiems kalbos analizės sprendimams.

Virtualios mokomosios platformos

Vilniaus universiteto (VU) Matematikos ir informatikos fakulteto Informatikos institute doc. dr. Lino Bukausko suburta mokslininkų ir specialistų komanda įkūrė Kibernetinio saugumo laboratoriją. Joje sukūrė programinę įrangą, skirtą mokyti, testuoti ir atlikti įvairius tyrimus kibernetinio saugumo srityje.

Kaip pasakojo Informatikos instituto lektorius Eduardas Kutka, Kibernetinio saugumo laboratorijoje yra dvi atskiros mokomosios platformos. Viena – procedūriniam mokymui, grindžiamam teisės aktų išmanymu, kaip reikėtų tinkamai reaguoti grėsmės atvejais. Parengta procedūrinė aplinka, kurią galima pritaikyti konkrečiai įmonei, institucijai ar organizacijai. Mokymų dalyviai gali pasitikrinti savo įgūdžius ir patobulinti juos pagal reikalavimus, nustatytus įstatymų ir naujų poįstatyminių aktų.

Kita platforma – kibernetinis poligonas – imituoja įmonės ar valstybinės įstaigos kompiuterinį tinklą. Per kibernetines pratybas galima pasimokyti dirbti su įvairiomis sistemomis, pasitobulinti turimus kibernetinių incidentų turimo įgūdžius ir įgyti naujų žinių

bei kompetencijų. Taip IT specialistai būtų labiau pasirengę reaguoti į incidentus ir apsaugoti savo įmonę ar įstaigą nuo įvairių problemų.

Bendradarbiavimas su įmonėmis dažniausiai konfidencialus. Tarp didžiausių viešai skelbiamų pavyzdžių – mokslininkų pagalba rengiant nacionalines kibernetines pratybas „Kibernetinis skydas“ 2016 ir 2017 metais, bei kibernetines pratybas kariškiams.

Kibernetinio saugumo laboratorija šiemet taip pat pristatyta Kijeve per Mokslo, inovacijų ir technologijų agentūros (MITA) kuruojamo atviro mokslinių tyrimų ir eksperimentinės plėtros tinklo “OPEN R&D Lietuva” surengtą vizitą. Vizito metu užmegzti kontaktai ir su mokslininkais, ir su verslo atstovais.

Mažoms ir vidutinėms įmonėms

“IT sauga neišvengiamai darysis vis aktualesnė. Yra nemažai standartų, kurie aktyviai diegiami ir Lietuvoje. Pavyzdžiui, nuo šių metų gegužės 25 dienos bus pradėtas taikyti Bendrasis duomenų apsaugos reglamentas, ir kiekviena įmonė bus tiesiogiai atsakinga už laikomų duomenų apsaugą. Neapsaugojus gresia didžiulės baudos”, – įspėjo Vilniaus Gedimino technikos universiteto (VGTU) mokslo ir inovacijų prorektorius prof. Antanas Čenys.

Didelėms kompanijoms susitvarkyti su tokio tipo iššūkiais nebus taip sunku, nes jos turi savo ekspertų, bet mažos įmonės dažniausiai jų neturi, o pasamdyti, pavyzdžiui, reguliariai atlikti rizikos analizę, brangiai kainuoja. VGTU mokslininkai, vadovaujami dr. Nikolajaus Goranino, jau kuria ekspertinę sistemą, skirtą atlikti rizikos analizę mažose ir vidutinėse įmonėse, kad jos galėtų sutaupyti, bet kartu atitiktų saugos reikalavimus.

Padės dirbtinis intelektas

VGTU mokslininkų grupė – didžiausia Lietuvoje, dirbanti kibernetinės saugos srityje, ir vykdomų tyrimų spektras, kaip pabrėžė VGTU Fundamentinių mokslų fakulteto prodekanas, Informacinių sistemų katedros docentas N. Goraninas, gana platus. Viena tyrimų krypčių – anomalijų ir atakų atpažinimas naudojant dirbtinio intelekto metodus. Įsiskverbimo detektavimo sistemai pateikiamas didelis duomenų kiekis, kad galėtų mokytis ir sugebėtų aptikti pagal veikimo bruožus naujus kenksmingus programinius kodus.

Dar viena sritis, plėtojama VGTU, – anomalijų analizė tinklo lygmeniu. Bandoma aptikti kenksmingų arba įtartinų protokolų, kurie gali slėptis bendrame tinklo sraute.

Tarp bendradarbiavimo su verslu pavyzdžių – neseniai vykdytas projektas su Kanados įmone

„Arcadia“, susijęs su anomalijų analize kompiuterių lygmeniu ir dirbtinio intelekto taikymu.

Per MITA projektą bendradarbiaujant su įmone „nSoft“ sukurtas produktas, pavadintas „Gedimino akimi“ – biometrinė judančio žmogaus autentifikavimo sistema pagal akies rainelę. Su biometriniais tyrimais taip pat susijęs projektas, vykdytas kartu su VU Fizikos fakultetu ir bendrove „nSoft“, skirtas daugialypei praėjimo kontrolės sistemai sukurti.

Kad pažangios idėjos lengviau pasiektų Lietuvos ir užsienio įmones, MITA įkūrė mokslinių tyrimų ir eksperimentinės plėtros tinklo “OPEN R&D Lietuva” Kontaktų centrą. Didžiausias Baltijos šalyse inovacijų infrastruktūros, paslaugų ir kompetencijos tinklas “OPEN R&D Lietuva” yra subūręs 14 valstybinių universitetų, 13 valstybinių mokslinių tyrimų institutų, septynis mokslo ir technologijų parkus bei 25 atviros prieigos centrus. “OPEN R&D Lietuva” Kontaktų centras padeda verslui greičiau surasti tinkamus žmones mokslo institucijose, sužinoti, kur galima užsisakyti reikalingas paslaugas, sudaro galimybes individualiems susitikimams. Užtenka elektroniniu paštu open@mita.lt atsiųsti užklausą, ir pateikiamas atsakymas, su kuo toliau reikėtų bendrauti. Padedama ne tik užmegzti kontaktus, bet ir tapti partneriais.