# KTU kibernetinio saugumo specialistas: DI tampa puolimo įrankiu (6 patarimai kaip apsisaugoti)

**Sparčiai augant technologijų naudojimui kasdienybėje, daugėja ir kibernetinių grėsmių. Kauno technologijos universiteto Informatikos fakulteto (KTU IF) kibernetinio saugumo specialistas doc. Šarūnas Grigaliūnas sako, kad  pasaulyje kibernetinių išpuolių skaičius per pastaruosius penkerius metus išaugo 75%, o DI atveria dar nematytas karybos galimybes.**

Pastaraisiais metais kibernetinių atakų mastas ir sudėtingumas sparčiai auga. Pasaulyje kibernetinių išpuolių skaičius per pastaruosius penkerius metus išaugo 75%.

## Kryptis – iš Rytų

Lietuvoje situacija taip pat kelia nerimą – Nacionalinis kibernetinio saugumo centras (NKSC) per pirmuosius devynis 2024 m. mėnesius užfiksavo beveik tris kartus daugiau duomenų išviliojimo (angl. phishing) atvejų nei tuo pačiu laikotarpiu pernai. Tai rodo, kad nusikaltėliai vis aktyviau taikosi į Lietuvos gyventojus ir organizacijas, siekdami išgauti itin jautrią informaciją.

„Kibernetinio saugumo grėsmės ne tik plečiasi, bet ir sudėtingėja. Lietuvoje matome reikšmingą kibernetinių atakų aktyvumą, ypač po Rusijos karo Ukrainoje pradžios. Programišiai neapsiriboja tik viešojo sektoriaus taikiniais – jie renkasi privačias įmones ir net individualius gyventojus“, – pastebi KTU docentas Š. Grigaliūnas.

Pasak jo, Rusijos agresija Ukrainoje atvėrė dar vieną kibernetinių atakų frontą, o Lietuva, remianti Ukrainą, tapo pažangių ir tęstinių kibernetinių grėsmių grupuočių taikiniu. Šios grupės vykdo šnipinėjimo operacijas, paslaugų trikdymo atakas ir renka informaciją apie Ukrainos karo pabėgėlius, naudodamos kenkėjišką programinę įrangą, platinamą prisidengiant Lietuvos institucijų vardu.

Per porą metų buvo taikomasi į daugiau nei 130 viešojo ir privataus sektoriaus interneto svetainių.

„Kibernetinių atakų tikslai yra labai įvairūs: destabilizuoti infrastruktūrą, skleisti dezinformaciją, išgauti jautrią informaciją ar net sukelti ekonominę žalą“, – teigia KTU docentas.

## Dirbtinis intelektas: grėsmė ir galimybė

Jo teigimu, dirbtinis intelektas (DI) tampa ne tik puikiu įrankiu, bet ir iššūkiu kibernetinio saugumo srityje. Gynyboje DI padeda aptikti grėsmes realiuoju laiku, automatizuoti

incidentų valdymą ir analizuoti naudotojų elgseną, didelius duomenų kiekius. Tačiau nusikaltėliai savo ruožtu taip pat išnaudoja turimas DI galimybes.

„DI naudojamas kuriant kintančias kenkėjiškas programas ir vykdant socialines atakas. Pastaraisiais metais net tokios pažangios organizacijos kaip „OpenAI“ (įmonė, sukūrusi „ChatGPT“) susidūrė su kibernetinio saugumo incidentais, parodžiusiais, kad net DI sprendimai gali tapti pažeidžiami – dėl atvirojo kodo klaidos „ChatGPT“ naudotojai galėjo matyti kitų vartotojų vardus, pavardes, banko kortelių duomenis, o daugiau nei 100 tūkst. paskyrų duomenys buvo pažeisti ir parduoti tamsiojoje interneto rinkoje“, – aiškina Š. Grigaliūnas.

KTU eksperto teigimu, kibernetiniai nusikaltėliai „ChatGPT“ naudoja kenkėjiškoms programoms kurti ir kibernetinėms atakoms vykdyti. Grėsmių grupės iš Kinijos ir Irano daugeliui gerai žinomą pokalbių robotą naudojo scenarijų kūrimui ir pažeidžiamumų analizei, kurdami elgesio modelius ir manipuliuodami aukomis.

**Lietuvoje – nauji teisiniai ir praktiniai sprendimai**

Atsižvelgiant į kylančias grėsmes, Lietuvoje 2024 m. spalio mėnesį įsigaliojo atnaujintas Kibernetinio saugumo įstatymas, kuris perkėlė Tinklų ir informacinių sistemų (TIS 2) direktyvos nuostatas į nacionalinę teisę. Šis įstatymas išplėtė kibernetinio saugumo reguliavimo sritį, įtraukiant naujus sektorius ir įmones – dabar taisyklių turi laikytis apie 20 000 organizacijų Lietuvoje.

Jis siekia suvienodinti kibernetinio saugumo lygį visoje Europos Sąjungoje (ES) ir sustiprinti valdysenos modelį Lietuvoje. Atnaujintame įstatyme numatoma, kad subjektai privalo pasitvirtinti saugumo politikos dokumentus, priskirti už tai atsakingus asmenis bei valdyti kilusius incidentus ir apie juos teikti ataskaitas.

Lietuva taip pat aktyviai dalyvauja tarptautiniuose projektuose, įskaitant ES struktūrizuotą bendradarbiavimą kibernetinio saugumo srityje ir bendradarbiavimą su JAV gynybos departamentu.

Šios priemonės padės organizacijoms geriau pasirengti kibernetinėms grėsmėms ir užtikrinti veiklos tęstinumą incidentų atveju. Vis dėlto, siekiant efektyviai kovoti su kibernetinėmis grėsmėmis, būtina nuolatinė viešojo ir privataus sektorių bei visuomenės bendradarbiavimo ir sąmoningumo didinimo iniciatyvos.

**Praktiniai patarimai: kaip apsisaugoti?**

Ekspertas Š. Grigaliūnas rekomenduoja imtis šių veiksmų:

1. Naudokite stiprius ir unikalius slaptažodžius, aktyvuokite dviejų veiksnių autentifikaciją (2FA).
2. Reguliariai atnaujinkite programinę įrangą – tai padės pašalinti žinomus pažeidžiamumus.
3. Būkite atsargūs su el. laiškais, venkite atidaryti įtartinus priedus ar spausti neaiškias nuorodas.
4. Naudokite VPN viešuosiuose tinkluose ir įdiekite antivirusinę programinę įrangą.
5. Ribokite asmeninės informacijos skelbimą socialiniuose tinkluose.
6. Darykite atsargines svarbių dokumentų kopijas, kad išvengtumėte duomenų praradimo.

**Aktyviai prisideda ir KTU**

KTU taip pat aktyviai prisideda prie kibernetinio saugumo vystymo, vykdydamas mokslinius tyrimus, rengdamas specialistus ir dalyvaudamas projektuose.

Čiaveikia Kibernetinio saugumo mokslinė grupė, kuri sprendžia debesų kompiuterijos saugumo problemas, kuria saugumui skirtus sprendimus, kurie užtikrina duomenų apsaugą ir veikia greitai net su ribotais ištekliais.

Be to, KTU dalyvauja projekte „Misijomis grįstų mokslo ir inovacijų programų įgyvendinimas“, vykdydamas misijos temą „Saugi ir įtrauki e. visuomenė“ (DigiDefence). Šio projekto tikslas – spręsti aktualias visuomenės problemas, susijusias su kibernetiniu saugumu ir skaitmenine integracija, skatinant mokslinius tyrimus ir inovacijas šioje srityje.

*Informacija parengta įgyvendinant projektą „Misijomis grįstų mokslo ir inovacijų programų įgyvendinimas“ Nr. 02-002-P-0001, finansuojamą Ekonomikos gaivinimo ir atsparumo didinimo plano „Naujos kartos Lietuva“ lėšomis.*