**Kibernetinio saugumo tyrimas: tik 3 iš 10 įmonių pakankamai „apsiginklavusios“, kad atremtų išpuolius**

**Dirbtinio intelekto plėtra, geopolitinė įtampa, ekonominis netikrumas ir auganti kibernetinių išpuolių rizika drebina verslo pagrindus, tačiau daugelis įmonių vis dar neskiria pakankamai dėmesio kibernetiniam saugumui. Vos 30 proc. įmonių – arba 3 iš 10 – galima laikyti gerosios praktikos pavyzdžiais, kurios sėkmingai valdo skaitmeninėje erdvėje kylančias grėsmes ir gali jaustis ramiau.**

Vienos iš pirmaujančių IT įmonių pasaulyje ir Baltijos šalyse „Accenture“ užsakymu atliktas tyrimas parodė, kad per pastaruosius beveik dvejus metus 97 proc. įmonių fiksuoja išaugusias kibernetinių grėsmių apimtis, taip pat beveik visi patvirtino, kad jaučia Rusijos agresijos Ukrainoje įtaką.

Nors beveik visi apklaustieji pažymi, kad atliko tam tikrus patobulinimus savo skaitmeninėse apsaugos sistemose, tačiau daugiau nei pusė – arba 54 proc. – mano, kad labiausiai pažeidžiami yra trečiųjų šalių ir išoriniai tinklai.

Kas antra įmonė – arba 51 proc. – pastaruoju metu sustiprino savo gebėjimus užtikrinti veiklos tęstinumą ir valdyti kibernetinio saugumo rizikas, panašus skaičius apklaustųjų pagerino incidentų stebėjimo ir reagavimo galimybes. Tuo tarpu tik 39 proc. organizacijų prioritetą teikia glaudžiam bendradarbiavimui su valstybės institucijomis kibernetinio saugumo politikos srityje.

Augantis dirbtinio intelekto pritaikomumas tampa tiek iššūkiu, tiek galimybe saugumui, tačiau Dmitrijaus Sorokino, „Accenture“ Kibernetinio saugumo departamento Baltijos šalyse vadovo, teigimu, sumaniai pritaikyti dirbtinio intelekto sprendimai gali padėti aptikti, analizuoti ir reaguoti į grėsmes.

„Dirbtinis intelektas spartina automatizavimą versle. Dauguma vadovų, kurių įmonėse ir organizacijose naudojami automatizavimo sprendimai kibernetinio saugumo srityje, nurodė, kad automatizavimas padeda sumažinti kibernetinio saugumo talentų trūkumą, o tai yra vienas pagrindinių iššūkių kiekvienai įmonei, norinčiai pagerinti savo IT sistemų atsparumą“, – sako D. Sorokins.

Apklausa rodo, kad daugiau nei pusė įmonių ir organizacijų pradeda suprasti kibernetinio saugumo svarbą ir vaidmenį skaitmenizuojant savo veiklą. Tiesa, kai kuriose įmonėse vis dar yra skirtumų tarp to, kaip saugumo klausimus vertina IT specialistai ir vadovai, kurie rečiau susiduria su kibernetinėmis grėsmėmis. Tad didžiausias iššūkis už kibernetinį saugumą atsakingiems asmenims – gebėti kalbėti verslo kalba ir įtikinti įmonės vadovybę imtis šiais laikais jau būtinų saugumo priemonių.

Tyrimas atskleidė, kad įmonės, kurios suderina kibernetinio saugumo strategiją su verslo tikslais ir nuosekliai jį stiprina, turi 18 proc. daugiau galimybių pasiekti prognozuojamą pajamų augimą bei 26 proc. sumažinti žalą, kurią patirtų įvykus kibernetinio saugumo incidentui.

„Accenture“ tyrime „Kibernetinio atsparumo statusas 2023“ („State of Cybersecurity Resilience 2023“) buvo apklausta 3 000 IT saugumo ir verslo lyderių iš didelių organizacijų bei įmonių Europoje, Šiaurės Amerikoje, Pietų Amerikoje ir Azijos Ramiojo vandenyno regione.

„Accenture“ yra viena pirmaujančių IT įmonių Baltijos šalyse ir pasaulyje. Įmonė teikia tarptautines valdymo konsultacijas, technologijų ir užsakomąsias paslaugas. Nuo 2021 m. įmonė turi biurą Lietuvoje, o Latvijoje įmonės padalinys veikia jau daugiau nei 20 metų. „Accenture“ dirba 733 000 darbuotojų, kurie yra įsikūrę 120 pasaulio šalių.

Daugiau informacijos: Sanita Kalve, „Accenture“ Baltijos šalių komunikacijos vadovė, sanita.kalve@accenture.com