Kibernetinis saugumas – rizika ne IT sistemoms, o visoms verslo operacijoms

Kas yra saugumas? Prie durų įmonės stovintis apsauginis, šarvuotos namų durys, automobilio signalizacija? Prieš keliasdešimt metų to užteko, tačiau šiandien suvokti saugumą reikia kur kas plačiau. Interneto ryšys kiekvieną dieną kuria naujas darbo vietas, tačiau su galimybėmis atsiranda ir grėsmių. Iš esmės kiekvienu prie tinklo prijungtu įrenginiu gali pasinaudoti piktavaliai.

Kibernetinio saugumo tema aktuali daugeliui įmonių, tačiau ji kritiškai svarbi transporto, logistikos bendrovėms. Į kokius aspektus jos turėtų kreipti dėmesį? Kaip identifikuoti grėsmes ir rasti geriausius sprendimus? Apie tai sutiko papasakoti Vilius Benetis, technologinių kibernetinės gynybos konsultacijų, reagavimo į saugos incidentus bei taikomųjų mokslinių tyrimų įmonės „NRD Cyber Security“ vadovas. Plačiau šia tema bus kalbama parodoje „Transbaltica“, kuri vyks Lietuvos parodų ir kongresų centre „Litexpo“ gegužės 16–18 dienomis.

Transportas – didelę įtaką daranti sritis

Kiekvienas internetinį ryšį turintis įrenginys – ar tai būtų asmeninis kompiuteris, ar automobilis, ar mobilusis telefonas, galų gale, netgi savaeigis dulkių siurblys ar išmanusis televizorius – gali būti „nulaužtas“. Sugedus vienam ar kitam įrenginiui, jam nefunkcionuojant tinkamai ar dingus tam tikrai informacijai, nuostoliai yra garantuoti.

Netekti asmeninių duomenų yra skausminga ir nemalonu, tačiau juos praradus įmonėse kyla ne tik moralinių, bet ir finansinių nuostolių.

„Transportas ir paštas Lietuvoje priskiriami ypatingos svarbos valstybės sektoriams. Tai reiškia, kad sutrikusi jų veikla gali padaryti didelės žalos nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams“, – teigia kibernetinio saugumo specialistas V. Benetis.

Transporto industrija visai pasaulio ekonomikai daro didžiulę įtaką, pavyzdžiui, Jungtinių Tautų skaičiavimais, 380 mlrd. JAV dolerių gaunama vien iš krovinių gabenimo laivais mokesčių, o tai sudaro apie 5 proc. pasaulinės prekybos.

Kam tai aktualu?

Kaip transporto įmonės vadovui įvertinti, ar jam reikia investuoti į kibernetinį saugumą? V. Benetis turi paprastą patarimą – įvertinti, ar veikla gali būti vykdoma neturint tam tikrų skaitmeninių duomenų.

„Kiekvienas vadovas turėtų atsakyti į klausimą, kiek organizacijos veikla yra priklausoma

nuo informacinių sistemų ir duomenų. Ar kompanija galės vykdyti veiklą, jei duomenys informacinėse sistemose taps neprieinami arba tam tikros sistemos neveiks?“ – klausia „NRD Cyber Security“ vadovas.

Pavyzdžiui, jūs valdote keliolika darbuotojų turintį servisą. Ar žmonės galės toliau tvarkyti automobilius, jeigu dings duomenų bazė su kiekvienos transporto priemonės remonto istorija, buhalteriniai duomenys apie atlyginimus, atostogas, ilgalaikio turto, įsiskolinimų ar gautinų sumų registras? Pagrindiniam darbui – automobilių remontui – tokie praradimai turi įtakos, tačiau jie įmonės veiklos nesustabdys.

Logistikos situacija – kita. Čia ryšio ir duomenų prieinamumas yra labai svarbus faktorius. Jeigu vieną dieną staiga dings duomenys apie klientus, prekes, pristatymo adresus, įmonės darbas visiškai sustos.

Dėl didžiulės įtakos tiesioginiam darbui kibernetinis saugumas šiam sektoriui – labai svarbus. Vienos didžiausių informacinių technologijų bendrovių pasaulyje IBM kibernetinio saugumo žvalgybos indeksas transportą priskiria dažniausiai atakuojamų sektorių penketukui.

V.Benetis prisiminė kelis vos 2017 m. įvykusius ir daugybę nuostolių pridariusius sutrikimus: „WannaCry“ virusas visiškai sustabdė didžiausios pasaulyje krovinių logistikos laivais įmonės „Maersk“ veiklą, stipriai sutrikdė Vokietijos pašto „Deutsche Post“ ir pervežimų traukiniais bendrovės „Deutsche Bahn“ operacijas.

„Tai reiškia, kad kibernetiniai nusikaltėliai mato piniginę naudą iš logistikos įmonių ir atakuoja jų sistemas, užšifruoja duomenis bei reikalauja išpirkos. Taip nutinka ne tik dėl sistemų saugumo spragų, bet ir darbuotojų neparuošimo kibernetinėms atakoms. Tuomet ganėtinai nesudėtinga organizuoti socialine inžinerija paremtas atakas“, – pasakoja kibernetinio saugumo specialistas.

Turėtų keistis požiūris

V.Benetis įsitikinęs, kad įmonių vadovai turėtų keisti požiūrį: kibernetinis saugumas jau nebėra IT rizika. Tai – operacinė rizika bet kuriai organizacijai, kurios veikla yra priklausoma nuo informacinių sistemų veikimo ir skaitmeninių duomenų prieinamumo.

Įvairios technologijos kaip pažangi analitika (angl. *advanced analytics*), dirbtinis intelektas (angl. *artificial intelligence*), daiktų internetas (angl. *internet of things*), didžiuliai duomenų kiekiai (angl. *big data*) ir kitos vystosi labai sparčiai, verslas jas naudoja vis plačiau –

technologijos didina efektyvumą, leidžia optimizuoti kaštus. Kartu didėja verslo priklausomybė nuo skaitmeninių sistemų.

„Kiekvienas vadovas turi žinoti, kaip jis saugo organizaciją nuo kibernetinio saugumo incidentų, kaip jie gali daryti įtaką verslo operacijoms ir ką reikia daryti, kai toks incidentas įvyksta“, – mano „NRD Cyber Security“ vadovas.

SIEM