Ekspertinis komentaras

2024.02.08

**Draudikai pataria, kaip valdyti kibernetinius incidentus**

*Komentuoja advokatų kontoros „Sorainen“ ekspertė Indrė Pelėdaitė ir teisininkas Dominykas Kulakas*

Naujienų portalų antraštės skelbia pranešimus apie Lietuvoje vykstančius kibernetinius incidentus. Neseniai paskelbta, kad „Telegram“ tinkle buvo paviešinta apie 1,5 tūkst. „Rimi“, „IKI“ ir „Senukų“ prekybos centro klientų duomenų, kurie buvo naudojami bandant prisijungti prie šių prekybos tinklų vartotojų paskyrų. Prekybos centrai patvirtino, kad informacija nutekinta iš jų duomenų bazių, buvo imtasi atitinkamų saugumo priemonių situacijai suvaldyti ir žalai mažinti, pradėtas vidinis tyrimas.

Įdomu tai, kad *IBM Corporation* duomenimis (*Cost of a Data Breach Report 2023, IBM Security*), vieno asmens duomenų pažeidimo kaina pasaulyje vidutiniškai siekia 165 JAV dolerius (apie 152 eurus). Atitinkamai, hipotetiškai skaičiuojant anksčiau minėtų prekybos centrų sukeltą žalą tretiesiems asmenims, vien ji galėtų siekti apie 220 tūkst. eurų. Tikėtina, kad reikalavimas Lietuvoje būtų mažesnis už pasaulinį vidurkį, tačiau tai nėra vieninteliai nuo kibernetinio incidento nukentėjusios įmonės nuostoliai – didžiausią pyrago dalį sudaro negautos pajamos dėl incidento sutrikdytos verslo veiklos, išlaidos ekspertams, duomenų atkūrimui ir kita.

Nesvarbu, ar internetas naudojamas tik pramogoms ir kasdieniams buities poreikiams tenkinti, smulkaus verslo ar didesnės organizacijos veiklai palaikyti ir vykdyti, galimybė nukentėti nuo kibernetinės atakos pastaruoju metu yra ypač išaugusi. Supratimas ir gebėjimas greitai ir efektyviai reaguoti į įvykusį kibernetinį incidentą gali padėti sumažinti žalą ar net apsaugoti informaciją.

Vienas efektyviausių būdų mažinti kibernetinių rizikų grėsmę yra kibernetinių rizikų draudimas. Apsidraudus paprastai kibernetinio incidento pasekmių valdymą perima draudikas, kuris turi tam iš anksto parengtas informacinių technologijų, viešųjų ryšių, teisininkų ir kitų specialistų komandas, užtikrinančias efektyviausią rizikų ir nuostolių mažinimą. Nuolat susidurdami su apdraustuosius ištikusiais kibernetiniais incidentais ir jų pasekmių valdymu, draudikai yra sukaupę nemenką patirtį, kuri leidžia efektyviai kovoti su kibernetinėmis grėsmėmis ir optimizuoti esamų išteklių panaudojimą įvykus incidentui.

Iš kibernetinių incidentų valdymo praktikos dirbant su didžiausiais pasaulio draudikais, išskiriame pagrindines draudikų teikiamas rekomendacijas verslui, susidūrusiam su kibernetiniu incidentu. Verta paminėti, kad dalis žemiau pateikiamų rekomendacijų tam tikrais atvejais tampa reikalavimais būsimiems draudėjams, kurie užtikrina pakankamą bendrovės pasiruošimą ir pajėgumą kovoti su įvykusiu incidentu.

1. **Krizės valdymo planas**. Planas yra vienas pirmųjų įrankių ir bene svarbiausių veiksnių, padedančių suvaldyti krizinę situaciją. Krizės valdymo planas turėtų įvardinti ne tik už incidento valdymo sprendimus atsakingus asmenis (paprastai tai yra bendrovės vadovas ir teisininkas), bet ir paskirtus projekto vadovus, kurie galėtų reaguoti į incidentą 24/7 režimu. Planas turi apimti aiškų vidaus komandos vaidmenų pasiskirstymą bei išorės specialistų (informacinių technologijų, viešųjų ryšių, komunikacijos, teisininkų) įtraukimą. Šie specialistai padėtų nukentėjusiai bendrovei veikti operatyviai kuriant strateginę komunikaciją, telkiant reikalingus pajėgumus ir atliekant būtinus veiksmus, padėsiančius suvaldyti krizę bei mažinti galimą žalą. Kibernetiniam incidentui iš anksto pasirengusi įmonė gali sėkmingiau sumažinti nuostolius, nes kiekvienas komandos narys tiksliai žinotų, kokios yra jo pareigos ir kokius veiksmus reikia atlikti sužinojus apie įvykusį kibernetinį incidentą.
2. **Vidinė komunikacija**. Ypač svarbi savalaikė komunikacija su darbuotojais ir aktyvus informacijos judėjimas tarp atskirų bendrovės padalinių ar komandų. Geroji praktika rodo, kad planuoti tolesnius veiksmus ir apsikeisti dideliais nuolat atsinaujinančios informacijos srautais padeda periodiniai (dažniausiai net kasdieniai) bendri kibernetinio incidento valdymo komandos skambučiai. Šiuo atveju gali praversti ir papildomas vidinės komunikacijos kanalas, kadangi įvykus kibernetiniam incidentui įprastai naudojamos programos gali neveikti. Siekiant užtikrinti veiklos tęstinumą, viešųjų ryšių specialistai turėtų būti pasitelkiami ir vidinei komunikacijai, kuri užtikrintų pasitikėjimą vadovybe ir savalaikę informacijos sklaidą.
3. **Įrodymų išsaugojimas ir pranešimai institucijoms.** Priklausomai nuo įmonės veiklos, kibernetinio incidento pobūdžio ir pasekmių, kibernetinį incidentą patyrusiai įmonei gali tekti pareiga apie patirtą incidentą pranešti Nacionalinio kibernetinio saugumo centrui arba Valstybinei duomenų apsaugos inspekcijai. Šių institucijų informavimo terminai kartais gali būti vos kelios valandos, todėl svarbi greita reakcija ir iniciatyvumas. Nepaisant įtampos ir chaoso, kuris neretai sukausto kibernetinį incidentą patyrusias įmones, svarbu reaguoti profesionaliai ir apgalvoti tolimesnius veiksmus. Bendrovė turėtų koncentruotis ne tik į incidento pasekmių šalinimą ir galimos žalos mažinimą, bet ir nepamiršti, kad institucijos ar draudikas gali reikalauti pateikti įvykusio kibernetinio incidento įrodymų, užfiksuotų, pavyzdžiui, informacinių technologijų specialistų. Tai gali būti informacija apie incidento pradžią ir požymius, kenkėjiškos programinės įrangos plitimą, apsaugos sistemų reagavimą ir kita.
4. **Išorinė komunikacija**. Išorinė komunikacija turi būti kruopščiai planuojama. Dažnai ją organizuoti pasitelkiami išoriniai viešųjų ryšių profesionalai, kurie sudaro komunikacijos planą kiekvieną viešą pranešimą derinant su teisininkais ir taip valdant galimą kaltės pripažinimo, nepakankamai tikslios informacijos platinimo ar kitas rizikas. Kai kibernetinis incidentas paveikia plataus rato asmenų jautrius duomenis, tikėtina greita ir audringa visuomenės reakcija, tad rekomenduojama nedelsiant parengti komunikacijos planą ir greitai reaguoti į įvykius. Planuojant išorinę komunikaciją, nereikėtų pamiršti ir tikėtino didelio vartotojų užklausų ar skambučio kiekio, į kuriuos privalės reaguoti nuo kibernetinio incidento nukentėjusi bendrovė. Esant didesniam užklausų kiekiui, nukentėjusiai bendrovei rekomenduojama pasitelkti išorinio skambučių centro specialistus, kurie galėtų organizuoti ir palaikyti komunikaciją su nukentėjusiais asmenimis bei atsakyti į gaunamas užklausas. Jei užklausų kiekis masinis, galima pasinaudoti atsakymų automatizavimo galimybe.
5. **Laikas**. Įvykus kibernetiniam incidentui, svarbi kiekviena akimirka, nes su kiekviena minute didėja nukentėjusios bendrovės patiriama žala. Apie kibernetinį incidentą per įstatyme numatytą laiką turi būti informuojamos ir valstybinės institucijos. Todėl kaip įmanoma greičiau apie incidentą turėtų būti informuojama visa bendrovės kibernetinio saugumo komanda ir aktyvuojamas rizikos valdymo planas.

Kiekvienas kibernetinis incidentas yra skirtingas – skiriasi nukentėjusios bendrovės veiklos pobūdis, klientai, partneriai, mastas, teritorija. Visos šios aplinkybės turi esminę įtaką incidento valdymo strategijai ir galimai žalai. Todėl nurodytos rekomendacijos yra bendros, o tinkamiausi sprendimai kiekvienu atveju turėtų būti parenkami individualiai, kruopščiai įvertinus situaciją ir incidento pasekmes pagal bendrovės veiklos pobūdį.

Kibernetinių rizikų draudimu apsidraudusios bendrovės šiuo atveju yra kur kas saugesnėje padėtyje, kadangi krizinės situacijos valdymo planą joms padeda sukurti ir įgyvendinti draudikas ir jo paskirta kibernetinių rizikų valdymo profesionalų komanda. Todėl apsidraudęs verslas dėl kibernetinių incidentų rizikos gali jaustis ramiau jos valdymą perduodamas profesionalams, o pats sutelkdamas visus pajėgumus į sėkmingą verslo vystymą.