Pasaulį sukrėtusi viruso „WannaCry“ ataka akivaizdžiai parodė – net itin lengvai užtaisoma, tačiau laiku nepašalinta saugumo spraga, kiekvienam asmeniui, įmonei ar organizacijai gali pridaryti didžiulių nuostolių. Kiek mes, mūsų darbovietės ir svarbiausios institucijos yra atsparios kibernetinio saugumo pavojams? Ir ar deramai įvertiname mums iškilusį pavojų?

Daugiau nei 300 tūkst. Tiek kompiuterių 150 valstybių kiek daugiau nei per 2 paras sugebėjo užkrėsti virusas „WannaCry“, kuris užšifruodavo visus kompiuterio duomenis ir už šifro raktą reikalaudavo išpirkos. Ir visa tai dėl vienos operacinės sistemos „Windows“ saugumo spragos, kurią bendrovė užtaisė ir vartotojams tebuvo likę įsidiegti atsiųstą atnaujinimą.

„Ši ataka atskleidė privačių asmenų bei institucijų abejingumą kibernetinei higienai. Dėl tokio aplaidumo, norint gauti prieigą prie daugelio namų ar įmonių kompiuterinių tinklų, net nereikia techniškai sudėtingos atakos ar komplikuoto kenkėjiško kodo“, – tvirtina „CUJO“ kibernetinio saugumo ekspertas Kęstutis Malakauskas.

Anot jo, internete kasdien pasirodo tūkstančiai naujų virusų atmainų, o didžioji jų dalis išnaudoja jau žinomus, tačiau vartotojų taip ir nepašalintus pažeidžiamumus.

Daugiau įrenginių – daugiau grėsmių

„Ateities rizikos gana aiškios – daiktų internetas plečiasi, prie tinklo jungiami milijonai naujų, lengvai pažeidžiamų prietaisų. Jie bus „nulaužiami“ ir jungiami prie kompiuterių „zombių“ tinklų, naudojamų DDoS atakose prieš globalius informacinių technologijų (IT) paslaugų teikėjus, finansų ir energetikos įmones. Jų darbo sutrikdymas gali sukelti chaosą globalioje visuomenėje.

Tiek gamintojams, tiek vartotojams reikia labiau rūpintis saugiu ir patikimu internetu. Jei nebus rimtų sprendimų, jei institucijos neskirs deramo dėmesio kibernetiniam švietimui, ateityje galime turėti didelių problemų“, – teigia K. Malakauskas, dalyvausiantis modernių technologijų ir verslumo renginio #SWITCH diskusijoje apie pasiruošimą atremti kibernetines grėsmes.

Virtuali valiuta pakeitė žaidimo taisykles

„Swedbank“ Saugumo incidentų tyrimo tarnybos vadovas Tomas Beinaravičius sako, kad pastaraisiais metais kibernetiniai išpuoliai pasikeitė iš esmės. Anksčiau bankų specialistams klientus tekdavo saugoti nuo nusikaltėlių, kurie pinigų vagystėms naudojo išpirkos reikalaujančius internetinius virusus (ransomware). Dabar tokių vagysčių smarkiai

sumažėjo. Deja, tai nereiškia, kad mažėja bendras nusikaltimų mastas.

„Išpopuliarėjusi virtuali valiuta bitkoinai paskatino išpirkos reikalaujančių virusų išplitimą. Šis nusikaltimo būdas nėra naujas, tačiau anksčiau nusikaltėliai turėjo labai ribotas galimybes anonimiškai gauti išpirką. Bitkoinai ir kitos kriptovaliutos suteikė galimybes išvengti teisėsaugos dėmesio.

Nesupraskite klaidingai – savaime bitkoinai nėra blogis, yra daugybė teisėtų jų naudojimo būdų. Tai tarsi degtukai, kuriais galima ir padegti namą, ir uždegti žvakę romantiškam vakarui“, – teigia T. Beinaravičius.

Nusikaltėliai stengiasi likti nepastebėti

Tomas Beinaravičius sako, kad bankai prieš „WannaCry“ ataką atsilaikė neblogai. Be to, jie dažniausiai susiduria ne su išpirkos reikalaujančiais virusais, o su labai užmaskuotais įsilaužimais – jų metu nusikaltėliai stengiasi likti nepastebėti ir kuo ilgiau savintis konfidencialią informaciją, verslo paslaptis ar pinigus.

Anot eksperto, atakos prieš valstybines įstaigas bei verslo ir finansų organizacijas vis dažnėja. O jų iniciatorės yra ne tik užsienio vyriausybės, bet ir kriminalinis pasaulis, kurio pagrindinis tikslas yra pinigai.

Tiesa, pašnekovas pažymi, kad kibernetiniai nusikaltimai daromi ne tik dėl pinigų. Nemažiau svarbios ir dažnos yra informacijos vagystės ar nedraugiškų jėgų bandymas kelti sumaištį. Tai reiškia, kad su kibernetiniu nusikalstamumu turi kovoti ne viena kuri organizacija ar sektorius – tai bendras visų reikalas.

Laikas pagalvoti apie katastrofinius scenarijus

Europos rizikos valdymo asociacijų federacijos (ERVAF) vadovas Jo Willaert sako, kad skaitmeninės technologijos jau tiek įsišaknijo mūsų kasdienybėje, kad atsparumas kibernetinėms atakoms tapo neatsiejama įmonės reputacijos dalimi.

„Įmonėms reikėtų galvoti ne tik apie savo, bet ir apie verslo partnerių kibernetinį saugumą, nes vieno subrangovo pažeidžiamumas kelia riziką visai tiekimo grandinei. Todėl kibernetinio saugumo rizikų valdymas nebegali būti tik IT padalinio rūpestis. Reikia suvokti galimos rizikos mastą bei jos valdymą pakylėti iki vadovybės lygmens“, – sako J. Willaert. ERVAF vadovas, taip pat dalyvausiantis šį rudenį Kaune vyksiančiame #SWITCH! renginyje.

J. Willaert teigia, kad iki 2020 m. daugeliui įmonių reikėtų sukurti su kibernetiniu saugumu

susijusius katastrofinių praradimų scenarijus ir juos naudoti kaip streso testą. Jis leistų sukurti efektyvias atakos nuostolių švelninimo strategijas, veiksmų scenarijus bei didinti savo, o kartu ir visos ekonomikos atsparumą.

Daugiau tarptautinio lygio profesionalų pasisakymų bei diskusijų kibernetinio saugumo klausimais bus galima išgirsti rugsėjo mėnesį vyksiančiame nemokamame modernių technologijų ir verslumo renginyje #SWITCH!, profesionalų diskusijoje „Kokia yra silpniausia mūsų kibernetinio saugumo grandis ir kaip ją pagerinti?“

Apie didžiausią Baltijos šalyse moderniųjų technologijų ir verslumo renginį #SWITCH!

Rugsėjo 19 d. įvyks trečiasis ir Baltijos šalyse didžiausias nemokamas moderniųjų technologijų bei verslumo renginys #SWITCH! Šiemet jis iš Vilniaus persikelia į Kauną – „Žalgirio“ arenoje susitiks visi neabejingi pažangai, talentingas jaunimas, vizionieriai bei visuomenės lyderiai. Renginys nemokamas, tačiau reikalinga registracija www.switchit.lt