Asmeninių prietaisų naudojimas darbui Lietuvoje ir kitose šalyse tapo norma. Karantinas ir darbas namuose šią tendenciją dar labiau sustiprino. Argumentai „už“ yra intuityviai suvokiami ir nereikalauja didesnių diskusijų: tai patogumas, reagavimo greitis, galimybė pasiekti savo kolegas bet kuriame pasaulio krašte, darbdavio lankstumas. Tačiau argumentai „prieš“ pasimeta kitų temų kontekste ir todėl retas darbdavys įvertina asmeninių prietaisų naudojimo darbui pavojų. Šia tema parengėme du straipsnius: pirmame aptarsime technologinius darbo iš asmeninių prietaisų pavojus, antrame – teisinius iššūkius.

Kai įmonė visiems savo darbuotojams sukuria stacionarią darbo vietą biure, išduoda darbinius kompiuterius bei telefonus, tokios įmonės vadovas gali daugiau mažiau sukontroliuoti, kad šiuose įrenginiuose būtų laiku atnaujintos operacinės sistemos, įdiegtos antivirusinės programos, kad įrenginiai būtų techniškai prižiūrėti ir fiziškai saugūs.

Kas atsitinka, kai darbuotojui yra leidžiama naudoti asmeninius prietaisus darbui? Pirmiausia, labai reikšmingai išauga įrenginių, kurie jungiasi prie įmonės IT infrastruktūros, skaičius. Kaip žinoma, kuo daugiau įrenginių jungiasi prie vidinių sistemų, tuo sunkiau užtikrinti informacijos jose saugumą. Antra, tokiems asmeniniams įrenginiams (jų saugumui) darbdavys turi labai ribotą įtaką arba visai jos neturi. Taigi atsiranda toks nevaldomas spiečius įrenginių, besijungiančių į įmonės IT sistemas, kuris sukuria puikias sąlygas piktavaliams pasinaudoti techninėmis spragomis.

Pagrindinės informacijos saugumo grėsmės, kai darbui naudojami asmeniniai prietaisai yra šios:

Įrenginių praradimas

Dėl tol, kad asmeniniai komunikacijos įrenginiai yra mobilūs, jų praradimas vis dar yra viena dažniausių problemų, kylančių darbdaviui leidus specialistams naudoti asmeninius telefonus, kompiuterius ir kitas priemones. Skirtingi tyrimai rodo, kad maždaug trečdalis duomenų saugumo pažeidimų yra susiję būtent su įrangos praradimu.

Techninių galimybių šiam „žmogiškajam faktoriui“ efektyviai užkirsti kelią beveik nėra. Iš esmės vienintelis būdas, galintis padėti surasti pamestus ar pavogtus daiktus yra „surask mano prietaisą“ tipo programinė įranga. Tačiau ir ji neužtikrina, kad piktavaliai nesuspės pasinaudoti suteikta proga.

Yra keletas teisinių priemonių, kurios sumažintų potencialią žalą įmonei, tačiau jų efektyvus didžiąją dalimi priklauso nuo darbuotojų sąžiningumo ir suvokimo, kokią žalą gali padaryti vienas pamestas neapsaugotas įrenginys. Tarp tokių priemonių paminėtinas įpareigojimas registruoti visus asmeninius prietaisus naudojamus darbui, privalomas nuotolinio informacijos sunaikinimo funkcijos instaliavimas, reikalavimas pranešti apie pamestą asmeninį prietaisą, specialių programėlių padedančių atskirti privačią ir darbinę aplinką instaliavimas, įpareigojimas apsaugoti įrenginį stipriu slaptažodžiu ir panašios priemonės.

Informacijos (ne)valdymas

Iššūkių kelia ir naudotojų patogumui sukurta informacijos bendrinimo (dalijimosi per debesiją) galimybė. Dažnu atveju, net žmogui pačiam to neįtariant, darbinė informacija, esanti asmeniniame įrenginyje, gali būti persiunčiama į asmeninę debesies talpyklą. Taip vyksta todėl, kad dalis įrenginių ir naudojamų programėlių automatiškai bendrina informaciją, nes tokie yra jų numatytieji (angl. default) nustatymai.

Tokiam informacijos bendrinimui užkirsti kelią siūlomi techniniai sprendimai yra, pavyzdžiui, konteinerizacija ir programinė įranga, leidžianti asmeniniame įrenginyje atskirti darbinę erdvę nuo privačios, tokiu būdu užtikrinant, kad bet kokia nauja įdiegta programėlė neturės prieigos prie darbinės aplinkos.

Visgi praktikoje labai reta įmonė paminėtas priemones naudoja. Tai reiškia, kad kiekvieną dieną įmonės informacija gali būti automatiškai bendrinama su asmeninėmis darbuotojų talpyklomis.

Virusai ir kiti kenkėjai

Paradoksalu, tačiau antivirusinių programų naudojimas ir kitoks kibernetinių atakų užkardymas yra savaime suprantamas kalbant apie kompiuterius, tačiau beveik visiškai ignoruojamas kalbant apie telefonus, planšetinius kompiuterius, išmaniuosius laikrodžius ir kitus įrenginius. Nuo virusų neapsaugoti asmeniniai darbuotojų prietaisai – tai saugumo spragos jūsų įmonės IT infrastruktūroje.

Dar daugiau, į dalį išmaniųjų įrenginių netgi technologiškai neįmanoma instaliuoti antivirusinių programų. Sakysite, na ir kas čia tokio. O gi problema tame, kad dažniausiai visi šie asmeniniai daiktai, paprastai būna sujungti į bendrą darbuotojo namų bevielio interneto tinklą. Toks sujungimas tarpusavyje leidžia programišiams, radus spragą viename įrenginyje, pateikti į visą namų wi-fi tinklą. Jeigu tuo metu darbuotojo kompiuteris taip pat būtų prijungtas prie tinklo, be abejo, programišiai patektų ir į jį.

Nesaugus internetas

Jau minėta, kad belaidis namų interneto ryšys nėra saugus. Tą patį galima pasakyti ir apie viešuosius wi-fi tinklus. Nepaisant to, kad šį faktą žino kiekvienas vidutinis interneto vartotojas, dėl to įsilaužimų į įmonių sistemas būtent tokiu keliu – per viešai prieinamą Wi-Fi, nemažėja.

Jungimosi prie viešo belaidžio interneto įpročiai buvo itin detaliai analizuoti 2016 metų Londono universiteto koledžo tyrime. Šio tyrimo metu nustatyta, kad žmonės dėl savo patogumo ir todėl, kad mano, jog nesaugus scenarijus neįsigyvendins, naudojasi viešu interneto ryšiu, net ir žinodami, kad jis nesaugus. Dar kiti sociologiniai tyrimai duomenų saugumo srityje rodo, kad kai žmonės susiduria su konkuruojančiais poreikiais, reikalaujančiais jų laiko ir įsigilinimo, jie sumažina savo pastangas skiriamas saugumui. Kaip tai pasireiškia naudojant viešą Wi-Fi? Tarkime žmogui reikia skubiai atlikti darbinę užduotį, o jis tuo metu miesto kavinėje geria kavą. Labai tikėtina, kad jis paaukos saugumą vardan greito rezultato net nesusimąstydamas, kad gali kuruti saugumo spragą savo darbdavio infrastruktūroje.

Kaip galima mažinti technologines rizikas?

Apibendrinant technologinius iššūkius, galima daryti išvadą, kad problema, kurią turi spręsti darbdavys, yra tokia – kaip užtikrinti, kad darbuotojų asmeniniuose prietaisuose ir namų tinkle bus imamasi visų būtinų saugumo priemonių arba kaip apsaugoti įmonės konfidencialią informaciją, nuo nesaugių prisijungimų iš išorės.

Dažnas teisininkas paminėtų darbuotojų švietimą, draudimą naudoti asmeninius prietaisus darbui, vidines tvarkas, įpareigojančias keisti slaptažodžius, atnaujinti operacines sistemas savo įrenginiuose, kaip galimus sprendimų variantus. O kibernetinio saugumo specialistai rekomenduotų šifruoti savo duomenis, riboti prieigos teises, naudoti dvigubą autentifikaciją, konteinerizaciją, o internetiniam prisijungimui prie įmonės infrastruktūros naudoti virtualius privačius tinklus (VPN), kurie sukuria savotiškus saugius skaitmeninius tunelius, vedančius tiekiai nuo jūsų įrenginio iki darbinės infrastruktūros.

Ar šių priemonių pakaktų visiškai apsisaugoti nuo išorinių technologinių grėsmių? Greičiausiai, ne. Todėl tikėtina, kad greitu metu asmeninių prietaisų naudojimo problemai spręsti nebus sugalvotas koks nors genialus sprendimas ir ji išliks galvos skausmu bet kuriam darbdaviui, nusprendusiam neriboti asmeninių prietaisų naudojimo darbui atlikti.

Pabaigai, norisi pažymėti, jog šio straipsnio tikslas nėra agituoti uždrausti naudoti

asmeninius prietaisus darbui. Kaip rodo socialiniai tyrimai, kuo jaunesnės kartos darbuotojai ateina dirbti, tuo labiau nesuprantamas jiems yra draudimas naudoti, pavyzdžiui, asmeninį telefoną darbinei pašto dėžutei tikrinti. Tikslas yra atkreipti dėmesį į šią, rodos, nereikšmingą problemą, kuri, galbūt, ką nors išgelbės nuo kibernetinio incidento.

Antroje šio straipsnio dalyje bus aptarti teisiniai argumentai, kuriuos būtina apsvarstyti prieš darbuotojams pasiūlant galimybę dirbti iš jiems patogiausios vietos ir su jiems labiausiai priimtinais įrankiais, o taip pat – žingsniai, kurių reikėtų imtis siekiant apriboti tokio darbo pobūdžio rizikas.

Apie COBALT:

COBALT yra viena didžiausių advokatų kontorų Baltijos šalyse. Daugiau kaip 200 teisininkų teikia kompleksines paslaugas vietos, regiono ir tarptautinėms korporacijoms, fondams, kredito įstaigoms bei įmonėms, taip pat privatiems asmenims visose verslo teisės srityse. Septynis kartus kontora laimėjo „Geriausios advokatų kontoros Baltijos šalyse“ titulą. Prestižiškiausi advokatų kontorų žinynai „Chambers Global“, „Chambers Europe“, „Legal 500“, „IFLR 1000“ ir kiti kasmet COBALT įtraukia į geriausių regiono advokatų kontorų sąrašą.

Advokatų kontoros COBALT vyresnioji teisininkė Renata Vasiliauskienė

Daugiau: **darbo kėdės**