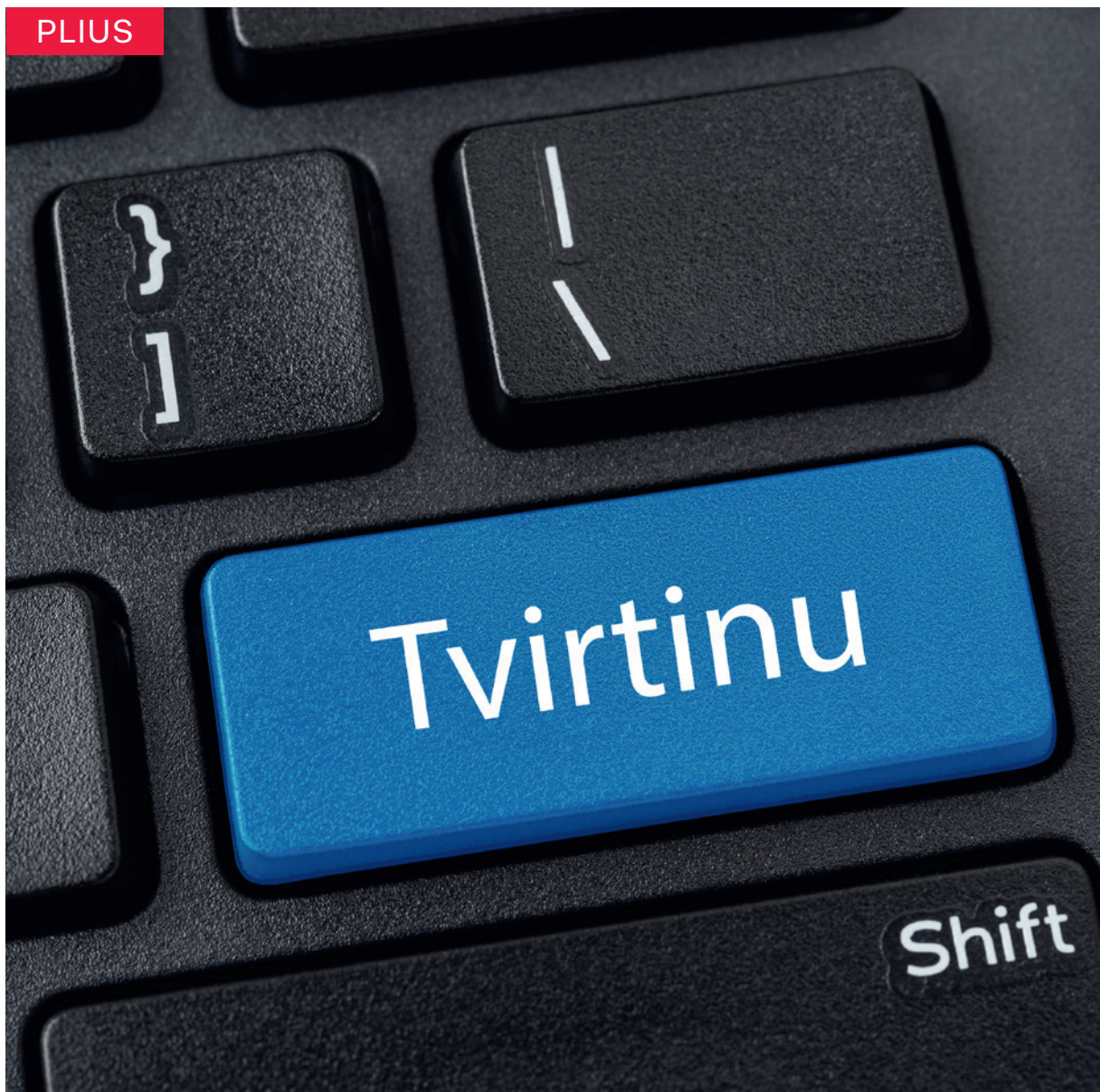


Notariatas

PLIUS



NUOTOLINIO NOTARIATO STARTAS



LOTYNIŠKAJAM
NOTARIATUI
LIETUVOJE

Nr. 3/2022

Turinys

Įžanga	5
eNotaro pirmasis dešimtmetis – nuo idėjos iki realybės Interviu su dr. Paul Bindoku	6
Dar karta apie saugumą jūsų kompiuteryje Dr. Anatolij Nečiporenko	18

Numerį rengė Lietuvos notarų rūmai

Kalbos redaktorė Edita Birulienė

Leidinio maketą rengė UAB „Druka“
Dizainerė Ingrida Ramanauskienė

Leidinyje publikuojamų straipsnių autorių vertinimai,
nuomonės nebūtinai sutampa su Lietuvos notarų rūmų pozicija

Viršelyje panaudota Veni vidi...shoot/iStock iliustracija

ISSN 2669-2996

Lietuvos notarų rūmų adresas:
Olimpiečių g. 4, Vilnius
El. p. rumai@notarai.lt
www.notarurumai.lt

© Lietuvos notarų rūmai, 2022

Ižanga

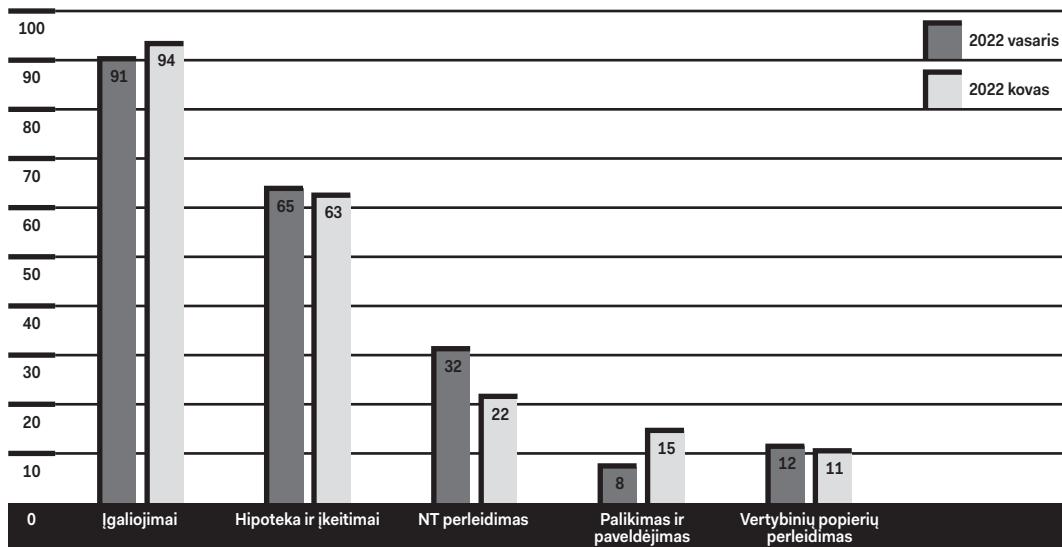
Gerbiamieji skaitytojai,

2021 metų liepos 1 dieną įsigaliojo Notariato įstatymo pataisos, kuriomis įteisinti nuotoliniai notariniai veiksmai. Per devynis mėnesius nuo naujų įstatymo normų įsigaliojimo galima drąsiai sakyti, kad iš egzotikos nuotoliniai notariniai veiksmai tapo notaro kasdienybe, nors jų atliekama dar nedaug palyginti su tradiciniais notariniais veiksmais. Akivaizdu, kad Lietuvoje nuotolinis notariatas žengia Latvijoje ir Estijoje pramintu keliu, būdamas ne tradicinių notarinių veiksmų pakaitalu, ne alternatyva, o papildymu. Ryškėja tendencija, kad aktyviausiai nuotolinius notarinius veiksmus atlieka nedidelių savivaldybių ir miestų notarai, tokiu būdu kompensuodami klientų biuruose deficitą. Nuo pirmųjų dienų dažniausias nuotolinis veiksmas – įgaliojimo patvirtinimas. Pastaraisiais mėnesiais sparčiai daugėja ir per nuotolį sudarytų hipotekos ir įkeitimo sandorių bei su jais susijusių veiksmų, nekilnojamojo turto perleidimo sutarčių, klientai naudojami ir galimybe per nuotolį atlikti palikimo priėmimo procedūrą.

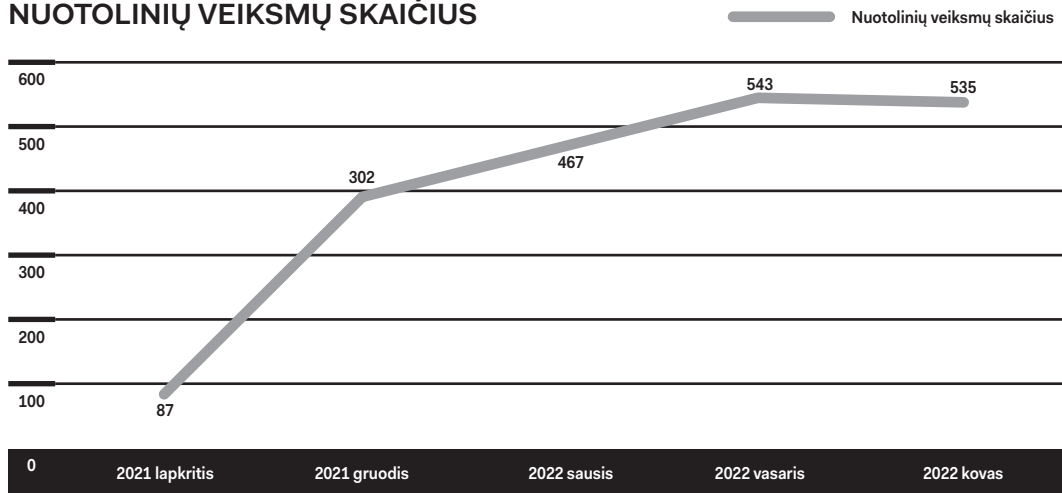
Nuotolinis notariatas pagrįstas Lietuvos notarų rūmų sukurta informacine sistema eNotaras. Šį pavasarį sukanka 10 metų, kai Lietuvos notarų rūmai pradėjo kurti šios sistemos užuomazgas. Apie dešimtmetį trukusį procesą žurnalo puslapiuose pasakoja bendrovės „iTree“ partneris, eNotaras technologinių kūrėjų darbo grupės vadovas dr. Paulas Bindokas. Lietuvos notarų rūmų informacinių technologijų specialistas dr. Anatolijus Nečiporenko savo straipsnyje primena esminius kompiuterinio saugumo reikalavimus, kurių būtina laikytis kiekvieno notaro biuro darbe.

Linkime malonaus skaitymo,
Jūsų „Notariatas Plus“

DAŽNIAUSIAI ATLIEKAMI NUOTOLINIAI NOTARINIAI VEIKSMAI 2022 M. VASARIS–KOVAS



NUOTOLINIŲ VEIKSMŲ SKAIČIUS



eNotaro pirmasis dešimtmetis – nuo idėjos iki realybės



Paulas G. BINDOKAS

eNotaras technologinių
kūrėjų darbo grupės vadovas,
UAB „iTree Group“ partneris

Interviu su dr. Paulu G. Bindoku, eNotaras technologinių kūrėjų darbo grupės vadovu, UAB „iTree Group“ partneriu¹

Sunku patikėti, kad sukanka 10 metų nuo pirmosios eNotaras informacinės sistemos strategijos kūrimo pradžios 2012 metais.

Per tą dešimtmetį eNotaras sistema iš idėjos pavirto realybe ir naudojama visuose Lietuvos notarų biuruose. Kelias nebuvo lengvas, tačiau rezultatu, manau, galime visi didžiulis, nes eNotaras nėra vien technologų darbo vaisius, o viso notariato darbo rezultatas.

¹ Interviu su P. Bindoku parengtas 2021 metų pabaigoje. Kai kurie prelegento aptariami sistemos eNotaras pokyčiai 2022 metų pavasarį jau buvo įgyvendinami.

„Notariatas Plus“: Su kokiais iššūkiais teko susidurti, kuriant eNotaras sistemą?

P. Bindokas: Informacinės sistemos eNotaras kūrimą lėmė tie patys „klasikiniai“ iššūkiai, kurie daro įtaką daugumos naujų informacinių sistemų kūrimo eigai. Pirmasis jų buvo tinkamai suprasti notariato veiklos aplinką tam, kad sukurta informacinė sistema taptų veiklos palengvinimu, o ne papildoma administracine našta notarams ir jų klientams. Antra, buvo siekiama užtikrinti, kad sistemos ir duomenų architektūra tinkamai atspindėtų realius duomenų poreikius ir sistemos diegimas nenulemtų nereikalingų duomenų kaupimo. Trečiasis iššūkis buvo įveikti technologinės brandos trūkumą notariate, t. y. suprasti, kad naudotojai yra ne technologijū, o teisės ekspertai, ir kūrimo bei eksploatacijos metu stengtis informaciją perteikti „žmonių kalba“, o ne „technologų čiulbėjimu“. Ketvirta, siekėme užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą teisėtiems naudotojams. Penkta, kėlėme sau užduotį užtikrinti, kad kuriant eNotaras informacinę sistemą nebūtų tiesiog automatizuojami kasdieniai procesai, o jie būtų optimizuojami. Šešta, siekėme užtikrinti, kad sistemos kūrimui ir eksploatacijai atsirastų tinkama programinė ir fizinė infrastruktūra.

Kūrimo procesui kėlė papildomų sunkumų tai, kad notariatas nėra monolitinė organizacija, kaip, pvz., ministerija ar kita valstybinė įstaiga, o tai notarų ir jų biurų asociacija. Be abejoj, visi notariatai ir jų biurai dirba pagal tapačius teisės aktus, tačiau kiekvienas biuras turėjo nusistovėjusias tų teisės aktų reikalavimų įgyvendinimo tradicijas. Kiekviename biure skirtingi technologinės brandos lygiai, vienur jau iki eNotaras sistemos atsiradimo veikla buvo automatizuojama savomis sistemomis, kitur kompiuterinis raštingumas buvo mažesnis nei vidurkis.

Be to, kuriant eNotaras sistemą reikėjo, iš esmės, sukurti ne vieną sistemą, o šimtus atskirų informacinių sistemų, sujungtų bendru technologiniu karkasu. Tai buvo būtina tam, kad vieno biuro duomenys nebūtų matomi kitiems biurams.

„Notariatas Plus“: Dirbant su eNotaras darbo grupe, kas buvo sudėtingiausia, kas maloniausia?

P. Bindokas: Lietuvos notarų rūmų suformuota eNotaras darbo grupė turėjo itin svarbų vaidmenį – suformuluoti ir technologams pateikti reikalavimus, pagal kuriuos sistema buvo kuriama.

Šioje darbo grupėje dalyvavo atstovai iš skirtingų biurų įvairiuose Lietuvos regionuose, tai leido geriau suprasti mažų ir didelių biurų poreikius. Darbo grupėje buvo tiek labai patyrusių, tiek jaunų notariato specialistų, kurie įnešė savus požiūrius į technologijas bei į darbo procesus.

Naudodamasis proga, norėčiau visiems darbo grupės nariams pasakyti „ačiū“ už jų svarbų indėlį. eNotaras sistema, kurią turime šiandien, atsirado darbo grupės pastangomis, notarų suformuotus reikalavimus technologai tiesiog pavertė sistema.

Iš pat pradžių 2012 m., kuriant sistemos strategiją bei 2014 m. pradėdant kūrimo procesą, sudėtingiausias faktorius buvo skirtingų, dažnai susikertančių, darbo grupės narių nuomonių gausa.

Įprastai dirbant su būsimais sistemos naudotojais, darbo grupės ateina į posėdžius turėdami iš anksto suderintą ir vieningą nuomonę. Kadangi eNotaras buvo pirmoji stambi informacinė sistema notariate, darbo grupė buvo valdoma, sakykim, labai demokratiškai. Ši demokratija lėmė ilgas diskusijas, iš šono žiūrint, net dėl paprastų klausimų, todėl tikriausia ne itin efektyviai naudotos sistemos kūrimui skirtas darbo valandas. Jei šiandien pradėčiau projektą iš naujo, prašyčiau, kad iš karto būtų skiriamas griežtas darbo grupės pirmininkas, kuris tą nuomonių gausą suderintų.

Iššūkis, su kuriuo iš tiesų sunkiai susidorojome, buvo poreikis ne tik automatizuoti veiklą biuruose, bet ją ir optimizuoti. Suprantu, kad teisės aktų reikalavimus būtina užtikrinti, bet dažnai buvo prašoma „ekraninę“ dokumento formą padaryti kuo panašesnę į „popierinę“ formą, prie kurios visi pratę. Tai nėra geriausia praktika. Todėl per pirmuosius metus teko nesyk grįžti prie daugelio formų aptarimo, siūlyti alternatyvas, kurios būtų patogesnės naudotojams, nepaisant fakto, kad ekranas atrodo kitaip nei įprastas dokumentas.

Buvo reikalavimų sukurti ir kitus sistemos elementus, kurie šiandien yra itin retai naudojami, pvz., Dokumentų šablonų funkcionalumą, kurį reguliariai naudoja mažiau nei 10 proc. naudotojų, nes daugeliui labiau įprasta tiesiog teksto redaktoriuose (pvz., Microsoft Word) kurti notarinio veiksmo dokumentus. Jei tektų įgyvendinti projektą iš naujo, tokių elementų siūlyčiau atsisakyti.

Pirmieji metai buvo nelengvi, manau, visiems, tačiau bėgant laikui situacija keitėsi ir nuo antrojo kūrimo etapo darbo grupėje sustiprėjo darbo grupės pirmininko vaidmuo. Lietuvos notarų rūmų teisininkai padėjo tarpusavyje suderinti skirtingas darbo grupės narių nuomones.

Per pastaruosius devynerius metus pasiektas ne tik abipusis supratimas, bet ir labai sklandus bendradarbiavimas su darbo grupės nariais. Lietuvos notarų rūmai tvirtai laiko sistemos raidos vairą ir džiaugiuosi, kad per pastaruosius metus LNR komandą papildė tikrai profesionalūs IT specialistai, kurie perėmė pirminę pagalbą naudotojams bei kūrimo proceso kontrolę. Maloniausia buvo tai, kad visi iki vieno darbo grupės nariai – tikri savo sričių profesionalai.

Pastaruosius 25 metus teko kurti sistemas ne vienai valstybinei institucijai, tiek Lietuvoje, tiek kitose šalyse. Dažnai viešojo sektoriaus projektuose iš užsakovo pusės būna surinktos gan silpnos darbo grupės, kurios nariai posėdžiuose dažnai arba tiesiog „stumia laiką“ arba sąmoningai įneša destrukciją, siekdami sau politinės naudos.

eNotaras darbo grupėje to nebuvo ir nėra ir, manau, tuo reikia notariatui didžiulis. Viso buvo ir visko bus, bet tam tikru požiūriu darbas su notariatu yra atgaiva, ypač lyginant su valstybinėmis institucijomis.

„Notariatas Plus“: Kokios technologijos panaudotos kuriant eNotaras informacinę sistemą?

P. Bindokas: Saugumo sumetimais detaliai neįvardysiu visų sistemoje naudojamų technologijų, o verčiau pakalbėsiu apie technologinius principus.

Pradžioje norėčiau apibrėžti dvi sąvokas: sisteminė programinė įranga bei eNotaras sistemos taikomoji programinė įranga.

Sisteminės programinės įrangos sąvoka apima tokius dalykus kaip operacines sistemas, duomenų bazių valdymo sistemas ir kitas platformines, arba, galima sakyti, „karkasines“, sistemos dalis, ant kurių „pastatyta“ eNotaras sistema.

Taikomoji programinė įranga yra tai, ką naudotojas mato prisijungęs prie sistemos, ir tai, kas naudotojo įvedamas instrukcijas bei duomenis paverčia veiksmais sistemoje.

Tam, kad būtų paprasčiau suprasti, įsivaizduokite savo darbo kompiuterį – jame yra *MacOS* arba *Windows* operacinė sistema (sisteminė programinė įranga) ir įvairios programos, kaip *Excel* arba interneto naršyklė (taikomoji programinė įranga).

Taikomosios programinės įrangos savininkas yra Lietuvos notarų rūmai. Tai, kas buvo sukurta, tapo Lietuvos notarų rūmų nuosavybe ir gali būti eksploatuojama be jokių papildomų licencinių mokesčių kūrėjams.

O sisteminės programinės įrangos savininkais išlieka tos programinės įrangos kūrėjai. Vieni kūrėjai leidžia sisteminę įrangą naudotis nemokamai, kiti reikalauja licencinių mokesčių ir / arba kasmetinių prenumeratų tam, kad būtų galima legaliai naudotis ta įranga.

2012–2013 metais Lietuvos notarų rūmai apibrėžė eNotaras sistemos strategiją, kurioje buvo numatyta, kad eNotaras sistema turi būti pagrįsta technologijomis, kurios patikimos, palaikomos jų gamintojų, saugios ir plečiamos.

Originalioje koncepcijoje technologinis karkasas buvo pagrįstas „atviro kodo“ (angl. *open source*) platformine programine įranga, kuri patikima, palaikoma, bet nereikalauja didelių kasmetinių licencijų palaikymo mokesčių.

eNotaras sistema taip ir buvo sukurta, tačiau dėl tuo metu buvusių aplinkybių, Lietuvos notarų rūmams priėmus sprendimą sistemą sudiegti valstybės įmonės Registrų centro (toliau – RC) serveriuose, RC reikalavo, kad sistemos branduolys būtų perkeltas į *Oracle* duomenų bazės valdymo sistemas, kadangi RC turėjo šios platforminės įrangos licencijų.

Teko perrašyti dalį sistemos kodo tam, kad jis veiktų su *Oracle* duomenų bazės serveriu. Ir, deja, Lietuvos notarų rūmams perkėlus eNotaras iš RC serverių į dabartinio prieiglos (angl. *hosting*) teikėjo serverius, teko pirkti šios duomenų bazės valdymo sistemos licencijas bei mokėti kasmetinius sistemos palaikymo mokesčius.

Oracle yra pasaulyje stipriausias duomenų bazių valdymo sistemų teikėjas. Tai, kad naudojame jų įrangą, nėra blogai, tiesiog tai sukuria papildomų kaštų, kurių originaliai buvo siekta išvengti.

Taikomoji sistemos dalis realizuota *Java* karkasais. *Java* yra brandi programavimo kalba, kuri plačiai naudojama per visą pasaulį ir grindžia milijonus skirtingų taikomųjų sistemų.

Konkrečiai, eNotaras sistemoje naudojama *OpenJDK* tam, kad nereikėtų pirkti kasmetinių prenumeratų. Sistemoje saugomi duomenys „gyvena“ Oracle duomenų bazėje, o dokumentai „gyvena“ *Alfresco* turinio valdymo sistemoje.

Atvaizdavimo sluoksnis, t. y. ta sistemos dalis, kuri nupiešia naudotojams matomus ekranus, yra pagrįstas *Primefaces* karkasu. 2021 m. spalio mėnesį teko visiškai atnaujinti šį komponentą tam, kad būtų užtikrintas sistemos saugumas, nes, nustačius senosios versijos pažeidžiamumą, gamintojas išleido naują versiją.

Dar, be šių sisteminės programinės įrangos komponentų, yra nemažai kitų, kurie užtikrina, kad

- sistemos dalys tarpusavyje tinkamai komunikuočiau;
- sistema tinkamai komunikuočiau su naudotojais (pvz., programų serveriai, turinio valdymo sistemos);
- būtų sumažinta rizika, kad pašaliniai asmenys bandytų sistemai arba jos duomenims pakenkti (fizinės ir programinės ugniasienės bei kitos priemonės);
- būtų registruojami ir įrašomi į žurnalus visi naudotojų veiksmai;
- būtų užtikrinta integracija su kitomis sistemomis (pvz., valstybės registrais) ir kt.

„Notariatas Plus“: Kaip vertinate dabartinę eNotaras architektūrą šiuolaikiniame pasaulyje?

P. Bindokas: eNotaras loginė architektūra, t. y. pats duomenų modelis ir taikomosios dalies architektūra yra gana šiuolaikiška ir, vertinant technologijų vystymąsi, matyt, liks tinkama naudoti dar maždaug penkmetį. Tada reikės įvertinti naujas technologijas, atrinkti ir peržiūrėti architektūros elementus, kurie moraliai pasenę, ir juos pakeisti.

Tam tikri **sisteminės programinės įrangos** komponentai jau yra technologškai pasenę, nes jie atrinkti prieš aštuonerius metus, o technologijos tikrai pasikeitė per tą laiką.

Lygiai taip, kaip naudotojai periodiškai atsinaujina savo darbo vietos kompiuterius, pvz., per *Windows Update* arba *Apple update*, reikia periodiškai atnaujinti ir tokių sistemų, kaip eNotaras, komponentus. Tai ir yra palaiptis daroma tam, kad būtų užtikrintas sistemos stabilumas ir, svarbiausia, saugumas.

Kaip jau minėjau, neseniai pakeistas visas atvaizdavimo sluoksnis. Turėsime netrukus naujinti ir programų serverius, integracinės terpės karkasą ir kelis kitus elementus tam, kad užtikrintume saugumą, nes tų komponentų gamintojai išleido naujas versijas ir nebepalaikys mūsų iki šiol naudojamų versijų.

Gera žinia – kadangi eNotaras sistema lanksčiai sukurta, nereikės perrašyti sistemos, o tik sudiegti atnaujintus komponentus ir juos ištestuoti, kas nėra labai didelis uždavinys.

Šiandien opiausia vieta yra ne programinė įranga, o fizinė. Dabartiniai serveriai, kuriuose įdiegta eNotaras sistema, darosi per silpni. Didėjant duomenų kiekiams, atsirandant naujoms funkcijoms ir įvertinant tai, kad nuo 2021 metų pradžios prisidėjo keli šimtai naujų naudotojų, tai yra natūralus dalykas.

Dabartinė fizinė infrastruktūra jau „braška“, t. y. dėl fizinės infrastruktūros ribojimų jau jaučiame tam tikrą sulėtėjimą, maždaug kas 8 savaites patiriame trumpus sistemos veik-

los sutrikimus, nes serverių procesoriai ir / arba atmintis nesugeba susidoroti su sistemos apkrovimu piko metu.

Šiuo metu Lietuvos notarų rūmai svarsto įvairius variantus, kaip stiprinti fizinę infrastruktūrą, įskaitant galimą sistemos iškėlimą į „debesų kompiuteriją“.

Atrodo tai kaip didelis pokytis, nes „debesų kompiuterijos“ sąvoka skamba gan mistiškai, tačiau debesų kompiuterija panašu į tai, ką turime šiandien – išsinuomojama vieta serveriuose prieglobos teikėjo duomenų centre.

Šiandien turime savus serverius, kurie yra patalpinti prieglobos teikėjo duomenų centre. Debesų kompiuterijos atžvilgiu, serverių savininkas jau nebebūtų notariatas, o būtų paslaugos teikėjas. Nepriklausomai nuo to, ar serveriai nuomojami debesų kompiuterijos principu, jie būtų visiškai valdomi notariato, prie juose esančių duomenų negalėtų prieiti tretieji asmenys.

Esminis skirtumas tas, kad galima lengviau pridėti serveriui atminties, arba disko talpos, arba procesorių – perkama paslauga, o ne fizinis serveris. Fiziniai serveriai, jų priežiūra ir plėtra tampa debesų kompiuterijos teikėjo rūpesčiu, o notariatas tiesiog pasako, kad „mums reikia tiek to, tiek ano“. Tai yra tvariau ir pigiau nei turėti savus serverius ir visiškai palaikau šią LNR iniciatyvą.

„Notariatas Plus“: Kalbant apie dabartinę sistemą, ar ji jau užbaigta, ar dar liko nesukurtų dalių?

P. Bindokas: Informacinės sistemos niekada nebūna „užbaigtos“ iki tos dienos, kai jos atjungiamos. Lygiai kaip keičiasi teisės aktai arba darbo metodai, turi keistis informacinės sistemos.

eNotaras atžvilgiu tai gali būti, pvz., naujų ataskaitų, naujų integracijų atsiradimas arba naujos / pakeistos notarinės paslaugos įvedimas. Pavyzdžiui, pandemija paspartino nuotolinių paslaugų atsiradimą ir neseniai įgyvendintas su tuo susijęs funkcionalumas. Pokyčiai yra natūrali gyvenimo dalis.

Tačiau, žiūrint tiek iš Lietuvos notarų rūmų pusės, tiek iš biurų pusės, manyčiau, kad dabartinė eNotaras sistema funkcinė prasme tenkina visus pagrindinius poreikius. Be abejo, norėčiau kelias jos vietas patobulinti.

„Notariatas Plus“: kurios dalys yra labiausiai tobulintinos?

P. Bindokas: Tikrai yra vietų, kurias reikėtų patobulinti, ir turiu savo nuomonę, ką reikėtų sistemoje pakeisti. Be abejo, visa tai yra tiktai mano nuomonė ir pokyčiai galėtų būti realizuojami tiktai su Lietuvos notarų rūmų pritarimu.

Manyčiau, pagrindinės tobulintinos dalys notariato portale yra:

- detali mokėjimų išsklotinė (tvirtinant notarinius veiksmus),
 - archyvų dalis bei
 - visa naudotojo sąsaja.
-

Detali mokėjimų išsklotinė buvo suprojektuota 2014–2015 m. pagal darbo grupės apibrėžtą „tipinio notarinio veiksmo“ scenarijų. Tačiau matome, kad jei yra daugiau nei penkios notarinio veiksmo šalys, ši sistemos dalis darosi nepatogi, per lėta ir reikalauja per daug pelės spustelėjimų.

Jei bandoma tvirtinti veiksma su daugiau kaip 50 šalių, pvz., uzufuktą su visais daugiabučio savininkais, detali mokėjimo išsklotinė dažnai stringa, net jei tik viena iš tų šalių yra mokėtoja. Ši sistemos dalis realizuota su *Alfresco* komponentu, norėčiau, aišku, jei tai LNR būtų priimtina, ją perkelti tiesiai į jau turimą *Oracle* duomenų bazę, kad viskas „suktųsi“ daug greičiau ir lengviau.

Be to, manau, visiems būtų gerai anksčiau matyti preliminarinius notarinio registro numerius, kas ypač aktualu rengiant elektroninius notarinio veiksmo dokumentus. Detalios mokėjimo išsklotinės dalies pertvarkymas leistų ankstesniuose tvirtinimo proceso žingsniuose matyti preliminarų notarinio registro numerį, tai palengvintų elektroninių veiksmo dokumentų rengimą (įrašyti registro numerį į dokumentus, tvirtinamuosius įrašus).

Kita dalis, kurią, mano nuomone, būtina pertvarkyti, yra archyvai. Archyvų dalies poreikis šiandien yra daug didesnis, nei buvo sistemos bandomosios eksploatacijos metu. Vien tai, kad atsirado elektroniniai notarinio veiksmo dokumentai, kurie nesaugomi biurų popieriniuose archyvuose, yra rimtas postūmis eNotaras archyvų funkcijai tobulinti.

eNotaras informacinės sistemos archyvų dalis buvo suprojektuota pagal tuo metu (2015 m.) galiojusią archyvų tvarkymo tvarką, kuri keitėsi kelis kartus nuo sukūrimo laikų.

Manyčiau, kad būtina tą dalį atnaujinti, labiau pritaikyti prie elektroninių notarinio veiksmo dokumentų, užtikrinti savalaikį elektroninių parašų pakeitimą archyviniais parašais.

Be to, manau, būtina į archyvų dalį perkelti senuosius duomenis iš pagrindinės eNotaras sistemos. T. y. „darbinėje“ eNotaras dalyje palikti tik griežtai apibrėžto einamojo laikotarpio duomenis, kas padėtų užtikrinti greitaveiką (gerokai sparčiau veiktų su mažesne duomenų aibe) ir sumažintų reikalavimus serverių pajėgumams, taip taupant lėšas.

Visus senus duomenis reikėtų laikyti atskiroje saugykloje, užtikrinant, esant poreikiui, jų pasiekiamumą per paiešką „darbinėje“ sistemos dalyje.

Duomenys archyvų dalyje turėtų būti saugomi pagal teisės aktuose numatytus saugojimo terminus, apsaugoti nuo pakeitimų nuo archyvo suformavimo dienos, tinkamai indeksuojami, kad būtų galima juos lengvai surasti.

Tinkamai sutvarkius šios dalies pajėgumus, be abejo, kartu su būtinu teisėkūros procesu, ilgainiui būtų galima spręsti ir „kilometrinių“ popierinių archyvų klausimą. Tai biurams tikrai būtų į naudą. Būtų galima visus dokumentus skenuoti, saugoti vien elektronine forma (su galimybe lengvai atlikti paiešką, pakelti reikiamus dokumentus), taip taupant notarų lėšas ir atlaisvinant patalpas nuo apdulėjusių segtuvų.

Trečia vieta, kurią norėčiau tobulinti, yra naudotojo sąsaja.

Naudotojo sąsaja buvo suprojektuota ir suderinta su darbo grupe prieš 7 metus, 2014 metais. Mano akimis žiūrint, ta naudotojo sąsaja jau yra „pavargusi“ ir reikėtų ją atšviežinti ne tik vizualiai, bet ir labiau pritaikyti įvairiems ekranams. Vis daugiau biurų pradeda dirbti su mobiliais įrenginiais, norėčiau, kad naudotojo sąsaja būtų labiau pritaikyta darbui su planšete arba mobiliuoju telefonu.

Be to, norėčiau atsisakyti 2014 m. stiliaus su tamsiai mėlynais atspalviais bei sunkia, daug ekrano užimančia, kvadratine meniu juosta, padaryti vizualiai lengvesnį vaizdą, sumažinti nenaudotinus balto fono plotus, restruktūrizuoti ekranines formas, kad jos būtų lengvesnės, modernesnės, greitesnės ir malonesnės naudotojams, bei užtikrinti jų pritaikymą jutiminiams ekranams, kai dirbama be pelės.

Žinoma, naudotojo sąsajos atšviežinimas nėra prioritetas, kadangi jis nėra tiesiogiai susijęs su funkcionalumu. Tačiau, mano nuomone, naudotojo potyriai naudojantis sistema tiek pat svarbūs, kiek jo atliekamos funkcijos.

Kalbant apie išorinį, klientams skirtą portalą, jo naują dizaino koncepciją neseniai aptarėme su darbo grupe ir Prezidiumo nariais ir jau judėsime lengvesnio dizaino bei supaprastinto paslaugų užsakymo link. Po išorinio portalo atnaujinimo, manyčiau, logiška dirbti ir notariatui skirtu portalo dizaino klausimais.

Atėjus laikui, klientų portale norėčiau patobulinti sąskaitų dalį, kad klientams būtų patogiau tiesiai iš portalo apmokėti išankstines sąskaitas (nuotoliniams notariniams veiksams) bei elektroniniu būdu gauti bei apmokėti sąskaitas už paslaugas, suteiktas biuruose. Logiška, kad jei klientas užsako nuotolinę paslaugą, kad jis per tą patį portalą galėtų keliais pelės spustelėjimais ir sumokėti už ją, o ne tik gauti pranešimą su prisegta išankstine sąskaita. Tad, jei LNR tam pritarėtų, manau, tikslinga būtų tokį funkcionalumą įgyvendinti.

Tokia apmokėjimo sistema galėtų būti integruojama ne tik su notarams skirtu eNotaras portalu, bet ir su biurų naudojamomis buhalterinės apskaitos sistemomis, leidžiant lengvai susieti gaunamus mokėjimus su išrašytais sąskaitomis. Be to, jei pavyktų dėl portalo atsisakyti popierinių sąskaitų ir kvitų, bent jau daliai klientų, tai taupyti biurų lėšas, skirtas šių dokumentų spausdinimui ir tvarkymui.

„Notariatas Plus“: Pakalbėkime apie kibernetinį saugumą. Kokios saugumo priemonės taikomos eNotaras sistemai? Ar reikėtų ką nors stiprinti?

P. Bindokas: Notariatas yra profesionaliausia ir patikimiausia Lietuvos Respublikos institucija. Todėl ir notariato naudojamos sistemos privalo būti patikimos ir tinkamai apsaugotos.

Kibernetinės saugos klausimas tampa vis svarbesnis, nes piktavalių asmenų rengiami išpuoliai prieš visas informacines sistemas tampa ne tik dažnesni, bet ir „profesionalesni“, jei taip galima juos pavadinti. Atsižvelgiant į tvarkomus duomenis ir vykdomas darbu sekas, eNotaras sistema „blogiukams“ yra tikrai įdomi sistema.

Remiantis 2021 m. I pusmečio LR Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos ataskaita, įsilaužimo tipo incidentų Lietuvoje užfiksuota net 129 proc. daugiau nei per analogišką periodą 2020 m.²

Kalbant apie kibernetinį saugumą, trumpai tariant, Lietuvos notarų rūmų tikslas yra užtikrinti visų notariato tvarkomų duomenų konfidencialumą, vientisumą ir prienamumą.

² Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos 2021 metų I pusmečio NKSC CERT-LT ataskaita, 2021-07-26.

Konfidencialumo reikalavimą lengva suprasti – duomenis turi matyti tik tie asmenys, kurie turi teisę juos matyti.

Vientisumas šiek tiek sudėtingesnis terminas ir apima reikalavimą, kad duomenys privalo būti apsaugoti ne tik nuo neteisėto atskleidimo, bet ir užtikrinta, kad niekas negalės tų duomenų pakeisti, įvesti, ištrinti arba kitaip paveikti, jei tam neturi teisėto poreikio.

Prieinamumą paprasta suprasti – naudotojai turi galėti prieiti prie duomenų tada, kada jų reikia. T. y. duomenys sistemoje turi būti pasiekiami tada, kada juos būtina pasiekti tam, kad notaras arba notaro darbuotojas galėtų atlikti savo funkcijas. Duomenys turi būti apsaugoti nuo ištrynimo, turi būti užtikrintas jų saugojimas teisės aktuose numatytiems laikotarpiais ir informacinės sistemos, naudojamos tiems duomenims tvarkyti, turi veikti tada, kada reikia.

eNotaras informacinė sistema susideda iš dvejų dalių: klientams skirto portalo ir notariatui skirto portalo. Kibernetinio saugumo prasme reikėtų apie šias dvi dalis pakalbėti atskirai. Vėlgi, saugumo sumetimais neišvardinsiu visų saugumo priemonių, dėl suprantamų priežasčių – nesinori „blogiukams“, kurie potencialiai skaitytų šią informaciją, duoti viso priemonių sąrašo...

Klientams skirtas portalas yra laikomas serveriuose, visiškai atskirtuose nuo notariatui skirto portalo. Tai viena iš saugumo priemonių, nes, jei pavyktų piktavaliui asmeniui įsilaužti į Klientų portalą, tas asmuo negalėtų tiesiu taikiniu perimti ir notariatui skirtame portale esančių duomenų.

Kliento portalo naudotojai jungiasi tiktai per elektroninius valdžios vartus (el. parašas, bankai arba Smart-ID), tad šio portalo naudotojų autorizacija ir autentifikacija patikėta valdžios vartų sistemos valdytojui.

Tiek klientams, tiek notariatui skirti portalai yra apsaugoti fizinėmis bei programinėmis ugniasienėmis. Tos ugniasienės stebi ir filtruoja visą naudotojų sąveiką su portalais, fiksuoja ir nepraleidžia neleistinių veiksmų.

Ugniasienės dirba baudos balų principu – už kiekvieną neleistiną veiksmą naudotojui ir jo IP adresui priskiriami tam tikri balai, o pasiekus balų limitą, užblokuojami prisijungimai iš anksto nustatytam laikui. Balų kiekiai tiesiogiai priklauso nuo naudotojo veiksmo rūšies – neteisingai suvestas slaptažodis gauna vienokį balą, bandymas į duomenų įvesties lauką rašyti kenkėjišką kodą gauna visiškai kitokius balus.

Abu portalai į specialius elektroninius žurnalus fiksuoja visus prisijungimus, naudotojų veiksmus sistemose. Abiejuose portaluose yra įdiegtos specialios priemonės, draudžiančios naudotojams atlikti neteisėtus veiksmus, pvz., duomenų įvesties laukuose bandyti įvesti programinio kodo atkarpas.

Duomenys sistemose yra šifruojami tiek duomenų bazės lygiu, tiek siuntimo metu, taip pritaikant principą, kad duomenys turėtų būti apsaugoti tiek saugojimo, tiek siuntimo metu.

Kalbant apie vidinį portalą, jame įdiegtos papildomos priemonės, kurios atskiria notarų biurų erdves. T. y. jei įvyktų neteisėtas naudotojo prisijungimo duomenų perėmimas į biuro A erdvę, tas piktavališkas asmuo negalėtų pasiekti ir biuro B duomenų.

Vidinio portalo naudotojai yra išskaidyti į vaidmenis (notaras, darbuotojas, notarų rūmų darbuotojas), visiems šiems vaidmenims taikomi skirtingi leidimai ir apribojimai.

Prieš pradėdant eksploataciją, visi eNotaras komponentai buvo atskirai ir kaip vientisa sistema ištestuoti nepriklausomos trečios šalies, kibernetinio saugumo ekspertų. Testavimo metu atrastos silpnos vietos buvo sutvarkytos iki eksploatacijos pradžios.

„Notariatas Plus“: Kibernetinio saugumo prasme, kas Jums kelia didžiausią nerimą?

P. Bindokas: Sakyčiau silpniausia bet kurios informacinės sistemos vieta yra naudotojai. Technologinės apsaugos priemonės labiausiai skirtos sistemai apsaugoti nuo pašalinų asmenų įsibrovimo.

Teisėti naudotojai, tyčia ar netyčia, gali lemti konfidencialių duomenų atskleidimą, pakeitimą, sunaikinimą. Vaidmenų sistema šiek tiek mažina pakeitimo ir sunaikinimo riziką. Be to, kertiniai duomenys yra versijuojami, t. y. saugomi ne tik aktualūs duomenys, bet ir jų ankstesnės versijos, kartu su įrašu apie naudotoją, kuris atliko pakeitimus.

Tačiau, bendraudamas su notarų biurais, esu matęs nemažai dalykų, kurie iš tiesų mažina sistemos saugumą, tarp jų:

- naudotojai naršyklėse išsaugoja prisijungimo duomenis ir palieka darbo vietos kompiuterius neužrakintus;
- tam tikri naudotojai pasidalina prisijungimo duomenimis su kitais naudotojais biure, arba su jais pasidalina savo el. parašo laikmena ir kodais;
- naudotojai dirba su įrenginiais, kuriuose nėra įdiegti operacinės sistemos atnaujinimai, arba naujausios apsaugos nuo kenkėjiškų programėlių bibliotekos, arba iš viso naudoja nelegalizuotas / neaktyvuotas operacines sistemas;
- naudotojai savo darbinius įrenginius parsineša namo, leidžia su jais dirbti savo vaikams ir kitiems šeimos nariams ir kt.

Mano nuomone, būtų tikslinga panaikinti galimybę prisijungti prie notariatui skirto portalo su naudotojo vardu ir slaptažodžiu ir leisti naudotojams jungtis tik su kvalifikuotais elektroniniais parašais. Tai labai padidintų sistemos saugumą, nes naudotojo vardo ir slaptažodžio naudojimas yra vienas iš lengviausiai pažeidžiamų prisijungimo būdų.

Be abejo, suprantu, kad toks žingsnis galėtų sukelti nepatogumų, nes ypač notarų USB laikmenos su parašais dažnai naudojamos kituose kompiuteriuose sąveikai su VĮ Registrų centro portalais bei ne visi notarų darbuotojai turi el. parašus. Tačiau skatinu šiuo atžvilgiu pasverti nepatogumus lyginant su galimo kibernetinio saugumo incidento pasekmėmis.

Jeigu el. parašo naudojimas, kaip vienintelis leistinas prisijungimo būdas, atrodytų per griežtas žingsnis, tada bent jau reikėtų įgyvendinti dviejų veiksnių autentifikaciją.

T. y. jei naudotojas prisijungia prie sistemos, kaip įprasta, su naudotojo vardu ir slaptažodžiu, jam papildomai atsiunčiamas kodas į registruotą mobilų įrenginį, kurį privalo suvesti prisijungimo metu.

Esu tikras, kad visi matėme tokių sistemų, kur gaunami kodai – tai nėra nepatogu, o saugumo lygį gerokai didina. Svarstyтина tokius kodus naudoti ir notarams tvirtinant notarius veiksmus, panašiai kaip suvedame kodus tvirtindami pavedimus el. bankininkystės portale.

Svarbu užtikrinti, kad visi sistemos elementai, pradedant nuo naudotojo ir įrenginio, su kuriuo dirba darbuotojas arba notaras, iki pačių sistemos serverių, būtų tinkamai apsaugoti, įdiegti visi gamintojo rekomenduojami atnaujinimai, be abejojimo, ir fiziškai apsugoti.

Serverių atnaujinimus valdo Lietuvos notarų rūmai, tačiau darbo įrenginių saugumu privalo pasirūpinti patys naudotojai.

Atnaujinimai yra svarbesni, nei atrodo iš pažiūros. Atsiminkime, kad 2021 metų pirmojo pusmečio reikšmingiausias kibernetinės saugos incidentas Lietuvoje buvo susijęs su vadinamu „nulinės dienos“ (angl. *Zero day*) pažeidžiamumu *Microsoft Exchange* el. pašto sistemose, kuris paveikė daugiau kaip 1 300 serverių IP adresų³ mūsų šalyje.

Be abejojimo, įdiegti atnaujinimus kainuoja – laiką, mokesčius gamintojams arba rangovams, kaštus, susijusius su sistemos pertestavimu. Bet, tie kaštai yra lašas jūroje, lyginant su kaštais, kurie atsirastų įvykus rimtam kibernetinės saugos incidentui.

Papildomai rekomenduočiau visam notariatui (notarams, darbuotojams, notarų rūmų darbuotojams) išklausti kasmetinius kibernetinio saugumo kursus, galimai tokius mokymus įtraukiant į privalomo kvalifikacijos kėlimo programos sąrašus.

„Notariatas Plus“: Pamaštykime apie ateitį. Ar manote, kad eNotaras sistema galėtų padėti įvesti kokias nors novatoriškas paslaugas?

P. Bindokas: Be abejojimo, tokios informacinės sistemos, kaip eNotaras, leidžia jų naudotojams įvesti naujoves. Notariato atžvilgiu tai yra sudėtingiau nei, pvz., verslo įmonėje, kadangi visa notariato veikla reglamentuojama teisės aktais. Tad bet kuri novatoriška paslauga nėra vien technologinis, bet ir teisėdaros uždavinys.

Technologinio vystymo prasme galimi du požiūriai: jei tai „nauja ir blizga“, reikia būtinai naudoti, arba, pažiūrėkim iš veiklos pusės, ar naujosios technologijos gali duoti mums konkrečios naudos.

Pats niekada nesirgau „šarkos sindromu“, t. y. man nesvarbu, ar kas nors madinga, man svarbu, ar tai naudinga, ar investicijos į naujas technologijas atsipirks realiomis naudomis.

Žiūrint į Europos notariatus, pvz., Prancūzijos notarų⁴, matome, kad tam tikri notariatai žengia į blokų grandinių technologijas (angl. *blockchain*) tam, kad padėtų užtikrinti notarinių veiksmų dokumentų panaudojimo atsekamumą ir patikimumą tų dokumentų naudotojų akyse.

Blokų grandinių naudojimas šiuo metu yra „ant bangos“ ir pati technologija iš tiesų yra gan įdomi. Tačiau, manau, Lietuvos notariatui dar trūptų per anksti apie tai galvoti.

Mano nuomone, leiskim technologijai subręsti, palaukime, kol Lietuvos notariate bus atsakyta popierinių archyvų, įvedant vien skaitmeninius archyvus, ir tada įvertinkim realius kaštus ir naudas prieš žengdami į blokų grandinės technologijų pasaulį.

³ Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos 2021 metų I pusmečio NKSC CERT-LT ataskaita, 2021-07-26.

⁴ Journal Spécial des Sociétés, Nr. 77, „Forum TECHNOT'2021 des Notaires du Grand Paris – Crise sanitaire: comment la profession a-t-elle bénéficié de son avancée technologique?“, Maria-Angélica Bailly.

Kalbant apie novatoriškas paslaugas, atsiminkime, kad nuo 2021 metų liepos 1-osios tokia jau atsirado – nuotolinės notarinės paslaugos ir elektroniniai notarinio veiksmo dokumentai.

Tai buvo itin svarbus žingsnis ir esame vienas iš nedaugelio notariatų pasaulyje, kuris gali pasiūlyti tokias paslaugas klientams. Šis funkcionalumas jau įgyvendintas, naudojamas, bet jį dar reikia tobulinti, padaryti draugiškesnį tiek notarams, tiek klientams.

Visgi yra viena nauja novatoriška paslauga, apie kurią siūlyčiau notariatui jau dabar pagalvoti. Tai yra skaitmeninio turto valdymo ir skaitmeninio turto paveldėjimo klausimų sprendimo automatizacija.

Vis daugiau turto persikelia į virtualią erdvę ir tas turtas retai visiškai inventorizuojamas, įvertinamas, jau nekalbant apie tinkamą to turto paveldėjimo proceso reglamentavimą.

Kaip pavyzdį apsvarstykime vadinamų „nuomonės formuotojų“ (angl. *influencer*) internetines paskyras socialiniuose tinkluose. Šios paskyros, jų turinys ir sekėjai generuoja šimtus tūkstančių eurų pajamų per metus.

Egzistuoja ir domenų vardai (pvz., kad ir „notarai.lt“ arba „google.com“) kurie perkami ir parduodami už šimtus tūkstančių eurų ir kurių savininkai gali būti ir fiziniai asmenys.

Neseniai atsirado nauja meno rūšis – vadinama nesuklastojamais žetonais (angl. *NFT – non-fungible token*). Kolekcionieriai (daugiausia fiziniai asmenys) už mažą paveiksluką arba originalią žinutę socialiniuose tinkluose (pvz., kokią nors *Twitter*⁵ žinutę) moka milžiniškas sumas, nors tas žetonas tiesiog kelios eilutės programinio kodo ar duomenų.

O kas su tomis paskyromis, turiniu ir sekėjais bei kitu skaitmeniniu turtu atsitiks po savininko mirties? Kas tą skaitmeninį turtą apsaugos tol, kol jis bus perduotas teisėtiems paveldėtojams?

Yra ir virtualios valiutos, kurios turi realią piniginę vertę ir kurios saugomos fizinių asmenų valdomose skaitmeninėse piniginėse. Dažnas atvejis, kai tos virtualios valiutos savininkui sutrinka sveikata, jis tampa neveiksnus arba miršta ir, kadangi prisijungimo duomenys ir raktiniai žodžiai gyvena tik jo smegenyse, palikuoniai negali prieiti prie milžiniškų sumų⁶.

Lygiai taip, kaip notariatas dabar priima asmeninius testamentus saugojimui, galbūt galėtų priimti saugoti ir tą skaitmeninį turtą, užtikrinti jo apsaugą ir perdavimą palikuoniams arba valstybei po savininko mirties. Esant poreikiui, notariatas testatoriams galėtų saugoti ir prisijungimo duomenis, raktažodžius arba skaitmeninius įrašus.

Kiek domėjaisi, tokios paslaugos dar neteikia nė vienas Europos notariatas, niekur Europoje iki galo nėra suformuotas tokios paslaugos teisinis pagrindas.

⁵ CNBC portalas, 2021-03-24 „Twitter CEO Jack Dorsey's first tweet NFT sells for \$2.9 million“, Todd Haselton. Prieiga per internetą <https://www.cnbc.com/2021/03/22/twitter-ceo-jack-dorseys-first-tweet-nft-sells-for-2point9-million.html>.

⁶ MarketWatch portalas, 2021-0-03, „Bitcoin pros speculate over possible loss of \$2 billion crypto fortune after death of one large owner“, Mark DeCambre. Prieiga per internetą <https://www.marketwatch.com/story/bitcoin-pros-speculate-over-possible-loss-of-2-billion-crypto-fortune-after-death-of-one-large-owner-11625255745>.

Tačiau, tinkamai suformavus teisinį pagrindą, Lietuvos notariatas šioje srityje galėtų tapti pirmuoju, kuris tinkamai rūpinasi skaitmeniniu turtu, ir rodyti pasauliui pavyzdį.

Technologine prasme, su smulkiais pakeitimais, šią paslaugą būtų galima visai netrukus pradėti teikti per eNotaras sistemą. Belieka teisinis klausimas.

Tokia paslauga ne tik būtų naudinga šiandienos visuomenei, kuri vis labiau neria į skaitmeninį pasaulį, bet galėtų tapti ir Lietuvos notariato viešųjų ryšių pergale, tampant pirmuoju notariatu pasaulyje, tinkamai sprendžiančiu skaitmeninio turto saugojimo ir paveldėjimo klausimus.

Dar kartą apie saugumą jūsų kompiuteryje



**Dr. Anatolijus
NEČIPORENKO**

Lietuvos notarų rūmų
IT specialistas

**Straipsnis parengtas dalyvaujant
dr. Paului BINDOKUI**

Informacinė sauga nėra vien technologų rūpestis, o yra kiekvieno notaro, notaro darbuotojo ir Lietuvos notarų rūmų darbuotojo atsakomybė. Būtina suprasti, kad jūsų kasdien įvairiais įrankiais tvarkomi duomenys yra turtas, kurį mielai pasigvelbtų piktavaliai asmenys, ir nesvarbu, ar tie duomenys laikomi tikrai jūsų darbo stalo kompiuteryje, eNotaras sistemoje, VĮ Registrų centro valdomose sistemose, jūsų mobiliajame telefone ar surašyti ant popieriaus lapo.

Technologinės priemonės gali mažinti tik tam tikras, būtent su technologiniais įrankiais susijusias neteisėto informacijos atskleidimo ar sunaikinimo rizikas. Šiame straipsnyje, be abejo, aptarsime ir technologinius klausimus – tai neišvengiama. Tačiau, norėtume pabrėžti ir tam tikrus kitus rizikos veiksnius ir kaip tą riziką būtų galima sumažinti.

eNotaras informacinės sistemos prisijungimo duomenys

Prie notariatui skirto eNotaras portalo jungiasi notarai, notarų darbuotojai ir Lietuvos notarų rūmų darbuotojai naudodami arba naudotojo vardo ir slaptažodžio kombinaciją, arba galiojantį kvalifikuotą elektroninį parašą. Be abejo, daug saugiau yra jungtis su

elektroniniu parašu, tačiau, jei renkatės naudotis naudotojo vardu ir slaptažodžiu, būtina užtikrinti, kad tie slaptažodžiai būtų sunkiai atspėjami.

eNotaras sistema reikalauja, kad slaptažodžiai būtų bent jau nustatyto ilgio, susidarytų iš didžųjų ir mažųjų abėcėlės raidžių, skaitmenų ir simbolių. Tačiau, netgi laikantis šių reikalavimų, būtina jums patiems rinktis slaptažodžius, kuriuos pašaliniai asmenys negalėtų atspėti. T. y. nenaudokite kaip slaptažodžio elemento savo vaikų, vaikaičių, augintinių vardų, užtikrinkite, kad skaičių sekos nebūtų vaiko gimtadienis ar kitas lengvai atrandamas duomuo iš jūsų gyvenimo aplinkos.

Savais slaptažodžiais nesidalinkite su kitais, net kolegomis biure. Suprantama, kad kartais atrodo daug paprasčiau, pvz., kolegos paprašyti: „Jonai, prisijunk mano vardu ir padaryk“, nei pačiam važiuoti į biurą. Tačiau slaptažodžiais dalintis griežtai draudžiama. Taip pat griežtai draudžiama slaptažodžius užrašyti ant lapelio, priklijuoto prie monitoriaus ar darbo stalo, kaip teko ne kartą matyti lankantis biuruose.

Jei turite klausimų apie sistemos veikimą, arba sistemos sutrikimo metu Jums skambina asmuo, prisistatęs Lietuvos notarų rūmų darbuotoju arba sistemos priežiūros rangovu, žinokite, kad šie asmenys niekada neprašys atskleisti savo slaptažodžio. Tad, jei tokį prašymą gaunate, labiausiai tikėtina, kad bendraujate su apsimitėliu, o ne tikruoju specialistu.

Naudotojų vardų ir slaptažodžių negalima saugoti naršyklės atmintyje, negalima saugoti ir paprastuose failuose kompiuteryje. Tai yra itin nesaugu, nes, jei įrenginyje nesaugiai laikote slaptažodžius, bet koks asmuo, perėmęs jūsų įrenginio kontrolę, iš karto turės prieigą ir prie eNotaras sistemos. Esame matę, kaip naudotojai savo slaptažodį užsirašo į el. pašto laišką sau, „kad nepamirštų“. Tai irgi itin nesaugu, nes jei kas perims pašto paskyros kontrolę, tas piktavališkas asmuo iš karto sužinos ir Jūsų eNotaras slaptažodį.

Geriausia praktika yra laikyti naudotojų vardus ir slaptažodžius tik vienoje, tik jums prieinamoje vietoje – savo atmintyje. Tačiau, jei tai tampa nepatogu, galite naudoti specialias slaptažodžių valdymo programėles savo įrenginiuose, kurios visiškai užšifruoja visą saugomą informaciją. Tokios programėlės yra mokamos (pavyzdžiai *Keeper password manager and Digital vault*, *Zoho vault*, *LastPass Premium* ir kt.)

Elektroninio pašto apsauga

Elektroninis paštas yra viena iš dažniausiai pažeidžiamų priemonių. Tiek Lietuvos, tiek pasaulinė statistika byloja, kad daugiau nei trys ketvirtadaliai visų sėkmingų kibernetinių atakų prasideda iš pažiūros nekaltai atrodančiais el. pašto pranešimais. Gaunamos el. pašto žinutės gali į jūsų įrenginį atnešti kenkėjiškų programėlių, kurios gali pakenkti jūsų duomenims, užrakinti jūsų įrenginį arba tyliai vogti iš jo jūsų duomenis.

Kadangi neseniai Lietuvos notarų rūmai centralizuotai atnaujino notarų el. pašto dėžutes aptarnaujančius serverius, ši rizika notarams yra mažesnė. Tačiau notarų darbuotojų el. pašto paskyros yra biuro atsakomybė ir būtina užtikrinti tinkamas jūsų naudojamų kitų el. pašto sistemų saugumą.

Nepriklausant nuo to, ar esate notaras ir naudojate LNR suteiktą pašto paskyrą, ar darbuotojas, atkreipkite dėmesį į šiuos patarimus:

Visada

- įsitikinkite laiško siuntėjo tapatybę, patikrinkite, ar adresas, iš kurio gavote pranešimą, sutampa su adresu, iš kurio tas asmuo įprastai jums siunčia pranešimus;
- nespauskite nuorodų, esančių gautame laiške, prieš tai jų nepatikrinę. Tai galite lengvai padaryti, jei skaitote paštą per interneto naršyklę – tiesiog pelę palaikykite virš nuorodos ir turėtumėte matyti jos santrauką ir kitą informaciją apie tą nuorodą. Neatidarykite nuorodų, kurios yra „sutrumpintos“ nuorodų trumpinimo programėlėmis, kaip bit.ly, nes dažnai slepiamos galimai pavojingos nuorodos;
- skeptiškai vertinkite laiškus, kurie prašo prisijungti prie eNotaras arba VĮ Registrų centro sistemų tam, kad „atnaujintumėte savo prieigas“ prie tų sistemų. Paspaudę laiške esančią nuorodą galite matyt įprastai atrodantį portalo langą, bet adresas bus visai kitoks. O suvedus informaciją į tokio lango laukus, ją atiduosite tiesiai į piktavaliu asmens rankas;
- praneškite apie potencialiai kenkėjiškus laiškus Lietuvos notarų rūmų sistemų administratoriams (jei esate notaras) arba savo tiesioginiam vadovui, jei esate darbuotojas.

Niekada

- neatidarykite prie el. paštu gaunamų laiškų prisegtų dokumentų, jei juos jums atsiuntė nepažįstamas siuntėjas;
- neatidarykite nuorodų, kurias atsiuntė nepažįstami siuntėjai;
- nesiųskite savo prisijungimo duomenų el. paštu kitam asmeniui (ar netgi sau).

Saugiam dokumentų apsikeitimui ir saugiam susirašinėjimui su klientais rekomenduojame naudoti eNotaras sistemą ir eNotaras klientų portalą.

Programinės įrangos atnaujinimai

Ilgapirščiai nuolat bando naujus būdus, kaip pavogti ar sugadinti svetimą informaciją reikalaujant išpirkos ar kitais tikslais. Didžiausią pavojų kelia neatnaujinta jūsų kompiuterio operacinė sistema ir kitos kasdien naudojamos programos.

Pagrindinės programos, kurias būtina nuolat atnaujinti to neatidėliojant (nebūtina diegti visų išvardytų programų, jos nurodytos pasitikslinimui):

Interneto naršyklės: *Google Chrome, Mozilla Firefox, Safari, Opera*, kt.

Microsoft Office arba *LibreOffice* paketas.

Archyvavimo programos: *7-Zip, WinRAR, WinZip* ir kt.

Labai svarbu atnaujinti programos, kuriomis atidarote iš trečiųjų šalių (pvz., klientų) gautus dokumentus. Gali užtekti parsisiųsti ir atidaryti vieną „apkrėstą“ dokumentą, jei *Microsoft Office* paketas ar kita programa, kuria atidaromas šis dokumentas, bus pažeidžiama / neatnaujinta.

Reikia labai susirūpinti, jei kompiuteriuose vis dar naudojate *Windows 7, Vista* ar *XP* versijas. Šios *Microsoft Windows* versijos jau nebepalaikomos ir jas būtina nedelsiant atnaujinti į **Windows 10 arba 11**.

Jei naudojate *Microsoft Office* paketą, pasitikrinkite, ar jo versija yra *Microsoft Office 2013* ar naujesnė. Jums reikės tiesiog reguliariai diegti atnaujinimus.

Jei naudojate *Microsoft Office 2010* ar senesnę versiją – šios programos nebegauna gamintojo atnaujinimų. Laikas įsigyti ir atsinaujinti programų paketą iki *Microsoft Office 2016, 2019* ar *365* (naujausia), *Microsoft Office 2013* nesiūloma, nes 2023 m. balandžio 11 d. pasibaigs šios versijos palaikymas (angl. *end of life*).

Šioje lentelėje pateikti būsimi palaikymo pabaigos terminai, kurie turi įtakos *Microsoft* produktams.

Microsoft produktas	Data
Windows 8.1	2023 m. sausio 10 d.
Office 2013	2023 m. balandžio 11 d.
Office 2019 for Mac	2023 m. spalio 10 d.

Šaltinis: <https://docs.microsoft.com/en-us/deployoffice/endofsupport/resources>

Jei naudojate *Apple* įrenginius, užtikrinkite, kad jūsų naudojama operacinė sistema yra ne senesnė nei *MacOS Sierra, iOS 14, iPadOS 14* versijų. Jei įrenginiai senesni ir nebepalaikomi naujomis operacinės sistemos versijomis, rekomenduojame tų įrenginių nebenaudoti. Taikomasias *Apple* programėles galite atsinaujinti per *App Store* programėlę.

Dėl *Apple* ir kitų programinės įrangos gamintojų kreipkitės į savo IT prižiūrinčius specialistus ir pasiteiraukite, ar operacinė sistema ir naudojamos programos turi gamintojo atnaujinimus. Jei atnaujinimų naudojamai programinei įrangai nėra (angl. *end of life, end of support*), raginame atsinaujinti programinę įrangą arba gauti paskutinę palaikomos programinės įrangos versiją.

Jei naudojate *Android* operacinė sistema valdomus mobilius įrenginius darbui, juos taip pat būtina atnaujinti, nes tai yra populiarūs taikiniai piktavaliams asmenims. Nenaudokite *Android* įrenginių, kurių operacinės sistemos versija senesnė nei 10 versija. Jei galite, atnaujinkite operacinę sistemą. Jei ne, rekomenduojame to mobilaus įrenginio nebenaudoti.

Apsaugos nuo kenkėjiškų programėlių

Nepriklausomai nuo to, ar naudojate *Microsoft Windows*, ar *MacOS* operacinę sistemą, būtina užtikrinti, kad jūsų įrenginiuose būtų tinkamai atnaujinta apsauga nuo kenkėjiškų programėlių (virusų, išpirkos reikalaujančių programėlių ir kt.). Naujausios *Microsoft Windows* versijos turi elementarią apsaugą nuo kenkėjiškų programėlių, jei nepirksite kitos apsaugos priemonės, užtikrinkite, kad ši *Windows* funkcija įjungta ir tinkamai atnaujinta.

Apple MacOS operacinės sistemos yra saugesnės ir mažiau pažeidžiamos nei *Microsoft Windows* operacinės sistemos. Tačiau, ir šioms operacinėms sistemos rimtai svarstyta įdiegti papildomą saugumo priemonių paketą. Pasitarkite su savo kompiuterius prižiūrinčiais specialistais ir nuspręskite, ar verta tokių apsaugos priemonių įsigyti.

Tačiau jei naudojate senesnius *Apple* kompiuterius, kuriuose jau nebegalima atnaujinti operacinių sistemų, tuose įrenginiuose būtina įdiegti trečių šalių papildomos apsaugos priemones.

Kalbant apie mobiliuosius įrenginius, *Android* įrenginiams rekomenduojame įdiegti papildomas apsaugas nuo kenkėjiškų programėlių. *iOS* ir *iPadOS* įrenginiams tai mažiau aktualu.

Interneto prieiga ir biuro vidinis tinklas

Gali pasirodyti, kad biuro vidinis kompiuterių tinklas yra besąlygiškai saugus, nes visi kompiuteriai sujungti laidais ir nėra kaip prie jo prisijungti iš išorės. Tačiau neretai interneto tiekėjai paslaugas teikia kartu su savo įranga, kurią labai dažnai sudaro tik vienas įrenginys – maršrutizatorius (angl. *router*, *wireless router*). Labai dažnai toks maršrutizatorius yra sukonfigūruotas paprasčiausiai – sujungiant laidinį ir belaidį tinklus į vieną bendrą. Tokie nustatymai būna padaromi dėl to, kad taip dažniausiai patogiau vartotojui. Juk jeigu jūsų kompiuteris prijungtas laidu prie tinklo, jūs galite prisijungti prie biuro įrenginio (spausdintuvo, skenerio).

Taip pat biuro darbuotojo (-os) nešiojamasis kompiuteris, kuris prijungtas prie belaidžio tinklo (angl. *wireless*, *wifi*), irgi gali spausdinti ir skenuoti (per vidinį tinklą), pasiekti visus vidinio tinklo resursus. Tokia „plokščio“ (angl. *flat*) tinklo topologija yra „tiesiog patogi“, nes nauji įrenginiai (kompiuteriai, nešiojamieji kompiuteriai ir išmanieji telefonai) pridedami be jokių apribojimų, nereikalauja sudėtingos konfigūracijos, bet saugumo prasme tai yra prastas pasirinkimas.

Resursai vidiniame tinkle

Naudojant „plokščią“ tinklą, kompiuteriai, biuro įrenginiai, išmanieji mobilieji įrenginiai (telefonai, planšetiniai kompiuteriai), išmanieji televizoriai / projektoriai, tinklo duomenų saugyklos, serveriai ir kita įranga, kuri prijungta prie biuro vidinio tinklo, yra tarpusavyje

sujungti resursai. Prie šių resursų gali prisijungti ir juos valdyti visi tinkle esantys įrenginiai, kuriems suteiktos teisės. Labai dažnai dėl paprastumo arba dėl nežinojimo yra sukuriami neapsaugoti resursai tinkle, pvz., kompiuteryje ar tinklo saugykloje esantys aplankai su failais bendrinami (angl. *shared folders*) vidiniame tinkle su kolegomis, nustačius teisių (paprastčiausiai be slaptažodžio). Spausdintuvai dažnai nustatyti priimti spausdinimo užduotis iš visų įrenginių be jokių teisių, prie televizorių leidžiama prisijungti tiesiog paspaudus kelis klavišus – besąlygiškai patogiu, bet ar tai saugu?

Visi resursai vidiniame tinkle turi būti apsaugoti. Tai galima padaryti naudojant slaptažodžius. Jei įmanoma, kiekvienas resurso naudotojas (angl. *user*) privalo turėti savo unikalų prisijungimo vardą ir slaptažodį. Tokiu būdu galėsite lengviau valdyti prieigos teises, skirtingiems vartotojams suteikti skirtingus resursus ir valdymo teises – tik skaityti, redaguoti, trinti. Keičiantis darbuotojams nereikės keisti vieno slaptažodžio visur, nes bus galima tiesiog užblokuoti vieną naudotoją, o naujam darbuotojui sukurti naują.

Mobilieji išmanieji įrenginiai vidiniame tinkle

Mobilusis išmanusis telefonas arba planšetė yra kasdienis darbo įrankis. Tikriausiai jūs ir darbuotojų mobilūs įrenginiai yra prijungti prie belaidžio tinklo biure. Dažnai tokie įrenginiai naudojami skambinant, susirašinėjant, siunčiant el. laiškus ir naršant internetą. Kai mobilusis įrenginys prijungtas prie bendro biuro belaidžio ryšio, jis gali jungtis prie kitų įrenginių vidiniame tinkle. Išmaniuoju telefonu (arba planšetiniu kompiuteriu) kaip ir kitais įrenginiais galima atspausdinti dokumentą prisijungus prie biuro įrenginio arba prisijungti prie kitų bendrų resursų.

Android ir *iOS (iPadOS)* įrenginiai turi daugybę programų, kuriomis galima pasinaudoti ne tik dokumentams atspausdinti, bet ir duomenims iš bendrų aplankų ar tinklo saugyklų valdyti. Tai labai svarbu, nes valdyti reikia – nuskaityti, pakeisti, ištrinti, sukurti naujus dokumentus.

Rizikos, klaidos ir patarimai

Neatskleiskite niekam savo biuro belaidžio (angl. *wireless, wifi*) tinklo slaptažodžio, išskyrus biuro darbuotojams.

Prisijungę prie belaidžio tinklo pašaliniai asmenys per vidinį tinklą galės pavogti jūsų asmeninius ir klientų bylų duomenis, jei resursai bus neapsaugoti papildomomis priemonėmis (teisių valdymas, slaptažodžiai).

Jei esate suteikę savo biuro vidinio belaidžio tinklo slaptažodį tretiesiems asmenims (pvz., klientams), **nedelsdami pakeiskite slaptažodį** (jei nežinote kaip, kreipkitės į interneto ryšio teikėją instrukcijos arba paprašykite, kad jis pakeistų slaptažodį).

Biuro belaidžio tinklo slaptažodį taip pat reikia pakeisti, jei keičiasi darbuotojai, nes belaidžio tinklo slaptažodžiai yra išsaugomi mobiliuosiuose įrenginiuose ir kompiuteriuose.

Saugokite biuro belaidžio tinklo slaptažodį – jis yra vartai į jūsų biuro vidinį tinklą. Visi, kas jį žinos, turės prieigą prie visų vidiniame tinkle esančių resursų.

Reguliariai, kas 30–90 dienų, keiskite biuro belaidžio tinklo slaptažodį.

Esant bent mažiausiai tikimybei ar kilus įtarimui, kad slaptažodis buvo atskleistas, nedvejodami keiskite biuro belaidžio tinklo slaptažodį.

Jei yra galimybė, būtinai atskirkite vidinį ir svečių (klientų) belaidžius tinklus. Reguliariai keiskite svečių belaidžio tinklo slaptažodį. Geriausia iškart po to, kai klientas pasinaudojo ir išėjo.

Klientų poreikis pasinaudoti belaidžiu tinklu susijęs su papildomomis rizikomis. Gali atsitikti taip, kad kliento kompiuteris buvo užkrėstas kenkėjiška programa (virusu) ir kol jis naudojosi jūsų biuro internetu per svečių belaidį tinklą, buvo padaryta nusikalstama veika.

Švaraus stalo režimas

Vienas iš svarbiausių informacinės saugos priemonių yra tai, kaip paliekate savo darbo vietą išeidami namo ar tiesiog trumpam išvykdami pietauti. Pakylant iš darbo vietos būtina užtikrinti, kad atsijungtumėte iš visų informacinių sistemų ir uždarytumėte tų sistemų naršyklės korteles (eNotaras, VĮ Registrų centro valdomų sistemų, kt.), užrakintumėte savo darbo vietos įrenginį, užtikrintumėte, kad ant stalo nepaliekate konfidencialios informacijos popierine forma, o ją saugiai sudedate į rakinamus stalčius ar spintas.

Visi kompiuteriai ir mobilūs įrenginiai, kuriuos naudojate tvarkydami notariato duomenis, turėtų turėti ekrano užsklandas, kurioms atrakinti naudotojas privalo suvesti to įrenginio slaptažodį arba bent PIN kodą. *Microsoft Windows* kompiuterius galite greitai užrakinti paspaudę Windows ir L mygtukus tuo pačiu metu. *Apple MacOS* įrenginius lengvai užrakinsite paspaudę Control-Command-Q mygtukus vienu metu. Mobiliuosius įrenginius užrakinsite tiesiog paspaudę jų įjungimo / išjungimo mygtuką. Jei nežinote kaip užrakinti savo įrenginio, kreipkitės patarimo į kolegas arba aptarnaujantį personalą.

Be abejo, tiek stacionarūs, tiek mobilūs įrenginiai turėtų būti apsaugoti nuo vagysčių. Paprasčiausias būdas tai padaryti yra tiesiog rakinti be priežiūros paliktų patalpų duris. Galima nebrangiai įsigyti ir naudoti ir specialias spynas bei kabelius įrenginiams prirakinti prie stambių baldų arba tam skirtų konstrukcijų.

Priminimas

Draudžiama kitiems asmenims atskleisti prisijungimo vardą, slaptažodį prie eNotaras informacinės sistemos ar notarų *Microsoft Exchange* el. pašto sistemos, *Microsoft Teams* ar kitaip sudaryti sąlygas visomis šiomis priemonėmis pasinaudoti (pvz., užrašyti slaptažodį ant lapelio ir palikti darbe arba namuose).

