Riigi Infosüsteemi Amet

Ettevõtte küberturvalisuse lühijuhend

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

2023

Käesolev lühijuhend põhineb Riigi Infosüsteemi Ameti tellimusel loodud juhendil, mille koostas AS BCS Koolitus Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

Sisukord

Eessõna

Tugevamad ettevõtted ehitavad tugevama ühiskonna

Küberturvalisuse seadus seab küberturvalisuse nõuded sellistele ettevõtetele ja asutustele, mille tegevus on ühiskonna toimimise seisukohast oluline – riigiasutustele, sadamatele, energiaettevõtetele, sideoperaatoritele jt. See näitab ühist arusaamist, et teatud organisatsioonide jaoks on küberturvalisus hädavajalik. Mõnelt asutuselt tuleb seda seadusega nõuda.

Samas sõltub Eesti inimeste küberturvalisus otseselt sellest, kui turvaliselt suudavad end ja oma kliente (nende andmeid) kaitsta kõik teised, väiksemad ettevõtted ja asutused, millele me samasuguseid nõudeid seadusega kehtestada ei soovi. Igal aastal kasvab summa, mille ettevõtted kaotavad näiteks meilikontode kompromiteerimise tagajärjel tehtavate finantspettuste kaudu. Samuti näeme, et lunavararünnakud ei kao kuhugi, ja kurjategijad leiavad infosüsteemides pidevalt uusi nõrku kohti, et varastada klientide isikuandmeid.

See kõik tekitab küsimuse, kuidas saab väikese või keskmise suurusega ettevõte end kaitsta erinevate tänapäeval levivate rünnakute vastu. Infoturbejuhtide või -meeskondade palkamine võib neil käia üle jõu, küberturvalisuse standardid võivad paista niivõrd mahukad ja ressursikulukad, et nende rakendamine ei tundu äriliselt mõistlik. Mis siis teha?

Küberturvalisus ei tohiks olla küsimus, kas teeme kõike või mitte midagi. Ka siin on võimalik alustada väikestest sammudest ja liikuda edasi vähehaaval – nii nagu ettevõtted vaatavad pidevalt üle ja täiendavad oma äriprotsesse ning töökorraldust.

Siinne küberturvalisuse lühijuhend on mõeldud selleks, et aidata ettevõtetel astuda esimesi samme küberturvalisemate äriprotsesside suunas. Siit leiab põhimõtted, kuidas kaitsta oma kliente, süsteeme, töötajaid ja kaubamärki. Nende põhimõtete vajadusest peaks aru saama iga ärijuht ja nende meetmete rakendamisega peaks toime tulema iga vähegi infoturbeteadlik IT-teenuse pakkuja.

Alati on võimalik tehniliselt turvalisust täiustada. Alustama peaks aga sellest, et küberturvalisus ei ole üksnes IT-osakonna asi, vaid ka juhtimise ja juhtide küsimus. Mida selgemalt ärijuht mõistab vajadust neid meetmeid rakendada, seda paremini saab ta suunata oma meeskonda ja vahendeid. RIA soovib olla teile sellel teekonnal võimalikult hea partner.

Margus Noormaa
RIA peadirektor

1. Tee selgeks oma ettevõtte kaitsevajadused

Liiga sageli on just (väikesed ja keskmise suurusega) ettevõtted need, kes ei pruugi osata mõista küberturvalisuse olulisust ning puuduliku infoturbega kaasnevaid riske. Samal ajal puudutab teema pea kõiki ettevõtteid, sest kui lähemalt uurima hakata, leiab nõudeid infoturbele nii partnerlepingutest, riiklikest regulatsioonidest, kui ka kliendile näiteks reklaamides antud lubadustest.

Näiteks on tihtipeale asutuse ärimudeli peamine komponent e-pood. Sel juhul tuleb tagada, et e-pood toimiks viperusteta ja oleks hea käideldavusega, st kättesaadav alati, kui klient sellele suundub. Vastasel juhul jääb ettevõttel lihtsalt soovitud tulu saamata. Kliendi ootus on aga turvaline integratsioon pangaliidesega ja see, et tema andmed soovimatult ei lekiks. Ehk siis nõuded terviklusele ja konfidentsiaalsusele. Kui veebipoes pakutakse teiste osapoolte teenuseid, siis on ka nendega sõlmitud lepingud ja neiski omakorda käideldavuse, tervikluse ja konfidentsiaalsuse nõudeid. Vastavate nõuetega käivad sageli kaasas ka sanktsioonid või trahvid, mille ennetamiseks turvameetmeid vaja rakendada on. Samuti tuleb veenduda erinevate turvameetmete rakendamises juhul, kui süsteemide automaatika, millega ka inimesed töötavad, sõltub IT-st. Halvimal juhul võib viga süsteemi toimimises või konfiguratsioonis viia tagajärgedeni, mis ohustavad inimeste elu ja tervist.

Ettevõtte jaoks on äriliselt oluline hoida asutuse head mainet, seda nii olemasolevate klientide ja töötajate säilitamiseks, aga ka uute leidmiseks. Meie digitaliseerinud ühiskonnas on hädavajalik, et ettevõtte loomulikuks osaks oleks ka turve, ehk turvariski käsitletakse nagu iga muud äririski. Kui ettevõte on selgitanud välja oma kaitsevajadused ning on teadlik, mis tuleb tagada, on turvameetmete rakendamisele tekkinud kindel eesmärk. Lisaks annab selline kaardistus juhised olukordadeks, kui mõni leping lõppeb, seadus muutub või alltöövõtja vahetub, et oleks kohene arusaam, mida tuleb ettevõtte turbehalduses muuta, et tagada turvalisus.

2. Tea, millist riist- ja tarkvara kasutad

Selleks, et ettevõtte võrku edukalt kaitsta, peab kõigepealt olema ülevaade, mis seadmed ja tarkvara selles võrgus on. Seetõttu on inventuur turvalise süsteemi loomise esimene ja väga oluline samm. Kui ei ole teada, mis seadmed või tarkvara võrgus olema peaksid, ei saa ka tuvastada, kui sinna on tekkinud tundmata ja lubamata seadmeid või tarkvara. Just selliseid seadmeid või tarkvara võivad ründajad ära kasutada, et saada ligi kontori võrgule. Kui ei teata, et tarkvara on kasutusel, siis ei saa korraldada ka selle uuendamist. Samuti on oht, et installitud on tarkvara, mille kaudu võib sattuda süsteemi kahjurvara (näiteks ebaseaduslik muusika /filmide allalaadimise tarkvara).

Iga seadme kohta, mis on kontori võrgus, peaks teadma järgnevat infot:

1. seadme nimi;
2. IP-aadress;
3. seadme eesmärk või põhjus, miks see võrgus on (kellegi arvuti, server, võrguseade jne);
4. seadmesse installitud tarkvara nimekiri;
5. millise äriprotsessi toimimist see mõjutab;
6. kuidas varad on omavahel seotud.

2.1 Inventeeri oma riistvara

Kõigepealt peab kindlaks tegema, mis seadmed võrgus asuvad. Isegi kui tegemist on väikese võrguga, kus on ainult paar seadet, tuleb nende info dokumenteerida. Kui seda ei tehta, võivad need seadmed jääda kaitseta. Ründajad otsivadki just kaitsmata seadmeid, et sealtkaudu ettevõtte võrku rünnata. Ülevaade võrgus olevatest seadmetest on vajalik ka siis, kui IT-personal vahetub, sest neil peab olema teave võrgu ja selles olevate seadmete kohta.

Kui ettevõtte võrk on suurem kui paar arvutit, siis on soovitatav kasutada inventeerimiseks tarkvara, mis teeb seda automaatselt. Käsitsi inventeerimisel võivad sisse sattuda vead ja kui on rohkem seadmeid, võtab see töö väga palju aega. Riistvara registrisse tuleks lisada ka kõik seadmed, mis parajasti pole küll võrgus, kuid mis võivad sellesse ühenduda või mille varguse korral võivad andmed kaduma minna.

2.2 Inventeeri oma tarkvara

Kui on olemas ülevaade võrgus olevatest seadmetest, tuleb kindlaks teha, milline tarkvara on nendes kasutusel. See on vajalik selleks, et kontrollida, kas tarkvara on uuendatud ja ega seadmetesse pole installitud tööks tarbetut tarkvara. Ka tarkvara inventeerimisel on mõistlik kasutada mõnda tööriista, mis suudab andmeid automaatselt koguda. Automaatne tarkvara inventuur aitab muu hulgas tuvastada selle, kui seadmesse on tekkinud uut tarkvara. Kogutud tarkvara andmed peaksid olema seotud seadmete registriga nii, et kõiki seadmeid ja nendega seotud tarkvara saaks jälgida ühest kohast.

Küsi IT-spetsialistilt

Riist- ja tarkvara inventeerimiseks on saadaval nii tasuta kui ka tasulist tarkvara. Tasuline tarkvara pakub tavaliselt rohkem funktsionaalsust. Küsi oma IT-personali või -teenusepakkuja käest sobivat tarkvara.

2.3 Kaalu seadmete keskhalduse kasutusele võtmist

Et oma seadmeid ja tarkvara paremini hallata, tasub kaaluda keskhalduslahenduse kasutusele võtmist. Keskhaldus võimaldab seadmeid keskselt hallata ja määrata, missugune tarkvara peaks olema neisse installitud, ning ühtlasi kaotab vajaduse mitme erineva inventeerimistarkvara ja haldussüsteemi järele. Keskhaldus võimaldab teha nii inventuuri kui ka rakendada seadmetele turvanõudeid. Mõne keskhaldustarkvara abil saab interneti teel eemaldada seadmetes olevad andmed, mis on kasulik juhul, kui töötaja peaks seadme kaotama või see varastatakse.

Küsi IT-spetsialistilt

Keskhalduseks on saadaval mitmeid lahendusi vastavalt sellele, millised seadmed (arvutid, nutiseadmed) on kasutuses. Tavaliselt on need tasulised. Küsi oma IT personali või -teenusepakkuja käest ettevõttele sobivaid lahendusi.

2.4 Loo reeglid isiklike seadmete kasutamiseks töökeskkonnas

Tänapäeval on järjest tavalisem, et töötajad soovivad tööks kasutada isiklikke seadmeid. Väga levinud on nutiseadmed (telefonid ja tahvelarvutid), aga üha enam kasutatakse ka isiklikke arvuteid. Lisaks tuuakse tööle enda USB-mälupulki ja väliseid kõvakettaid, mis võimaldavad kiiresti ja lihtsalt andmeid sisevõrgust välisele andmekandjale liigutada. Kui töötajatel on lubatud isiklikke seadmeid kasutada, peaks sätestama selle kohta reeglid, sest nad töötavad isiklikel seadmetel ettevõtte andmetega. Kui võimalik, tuleks reeglid koostada koostöös kasutajate ja IT-personaliga.

Isiklike seadmete kasutamise reeglite koostamisel tuleb:

1. määrata, millised turvanõuded on kehtestatud isiklike seadmete kohta. Näiteks peab kindlasti nõudma, et seadmed oleks kaitstud parooliga ja neisse oleks installitud viirustõrje tarkvara. Kui seadmes hoitakse konfidentsiaalseid andmeid, peaks see seade olema krüpteeritud;
2. koostada nimekiri seadmetest ja operatsioonisüsteemidest, mida pole lubatud ettevõttes kasutada, näiteks turvaaukudega seadmed või seadmed, mille tarkvara tootja enam ei toeta (näiteks Windows XP arvutid peaks olema keelatud). Lisaks peaksid olema keelatud ka isiklikud võrguseadmed (kasutaja isiklikud switchid, ruuterid, WiFi-seadmed jne), mis võivad tekitada ettevõtte võrgu töös tõrkeid;
3. võimalusel pidada nimekirja seadmete kohta, mida töötajad soovivad kasutada. Selles peaks olema töötaja nimi, seadme nimi, tarkvara loetelu jne;
4. vajaduse korral luua reegel, mis keelab talletada isiklikes seadmetes tööalast teavet.

Kasutajad peavad loodud reeglite ja nõuetega tutvuma ja nõustuma ning kinnitama seda oma allkirjaga (muidu ei lubata nende isiklikku seadet tööks kasutada).

3. Kaitse oma vara

Kui on olemas hea ülevaade, mis seadmed ja tarkvara kontori võrgus ja töötajate kasutuses on, tuleb neid hakata kaitsma.

Kuna seadmed ja erinevad teenused (veebileht, majandustarkvara jne) võivad olla teenuseandja juures majutuses või neil võib juba olla mingi tarkvaraline kaitse (tulemüür, viirustõrje), siis võib tunduda, et ettevõttes kasutatavad seadmed ja tarkvara ongi juba kaitstud. Tegelikult sellest aga ohtude vastu kaitsmiseks ei piisa. Tõhusaks seadmete ja andmete kaitseks tuleb rakendada lisameetmeid ning tegeleda kaitsmisega aktiivselt.

3.1 Anna juurdepääsuõigused põhjendatult

Rünnakud ja viirused levivad tavaliselt kasutajate kaudu. Mida rohkem õiguseid kasutajal on, seda kergem on ründajal või viirusel tegutseda.

Seetõttu tuleb iga ligipääsu andmisega läbi mõelda, kas neid ligipääse/õiguseid (näiteks juurdepääsud jagatud kaustale, või majandustarkvarale, administraatori õigused arvutisse) on ka tegelikult tööks vaja. Kui on jõutud otsusele, et neid on tõesti tarvis, siis tuleb nende andmisel lähtuda vähima õiguse printsiibist ehk töötajale tuleb anda täpselt nii vähe õiguseid, kui tal on tööks vaja, ja mitte rohkem. Tihtipeale minnakse kergema vastupanu teed ja antakse õigused tervele kataloogile, seeläbi võib töötaja juurde pääseda andmetele, millele tal ei tohiks juurdepääsu olla. Isegi kui töötaja ei tee selle juurdepääsuga midagi, võivad ründajad seda ikkagi ära kasutada.

Hea tava!

Jaga juurdepääsuõigused rühmade kaudu. See lihtsustab õiguste jagamist ja annab neist hea ülevaate. Siis on ka töötaja lahkumisel kerge ta lihtsalt vastavatest rühmadest eemaldada, selle asemel et hakata katalooge ükshaaval läbi vaatama ja otsima, millele ta juurde pääses.

Töötajatel pole tavaliselt töökoha antud arvutis administraatori õiguseid vaja.

Administraatori õigustega kaasneb hulk ohte:

- Töötaja võib paigaldada oma arvutisse programme, millega võivad kaasneda turvaaugud ja kahjurvara.
- Kahjurvara tekitatav kahju on suurem, kui töötajal on administraatori õigused.
- Ründajad saavad siis kergemini arvuti üle kontrolli võtta jne.

Kui administraatori õiguseid on siiski vaja, tuleks selle jaoks teha arvutisse eraldi kohalik kasutajakonto, mida kasutataks ainult vajaduse korral, mitte igapäevatoiminguteks. Sedasi väheneb tõenäosus, et kasutaja kogemata installib kahjurvara, ning juhul kui töötaja konto andmed lekivad, ei saa ründaja kohe administraatori õiguseid. Kui see on töötaja isiklik arvuti, tuleb lähtuda punktist 1.4 „Loo reeglid isiklike seadmete kasutamiseks töökeskkonnas“, aga ka sel juhul võiks soovitada tööasjade jaoks eraldi kontot.

Küsi IT-spetsialistilt

Küsi IT-personalilt või -teenusepakkujalt regulaarselt ülevaadet kasutuses olevate administraatori kontode kohta.

Kui IT-personal või -teenusepakkuja juurdepääsuõiguseid annab, peaks ta need pääsude andmised ka dokumenteerima (millal, kuhu, kellele), et omada pidevalt ajakohastatud ülevaadet kellel kuhu pääs on. Antud informatsioon on abiks ka töötaja lahkumisel, sest siis on teada, mis pääsud peab sulgema.

Kui peaks toimuma mõni turvaintsident, siis võib selline dokumentatsioon anda teavet, kuidas see juhtus.

3.2 Uuenda tarkvara regulaarselt

Igasuguse tarkvara kasutamine on tänapäeval tavaline töö osa. Tarkvaradel avastatakse pidevalt turvaauke ja muid puudusi, mida ründajad saavad ära kasutada, et paigaldada kahjurvara, võtta arvuti oma kontrolli alla ja/või varastada andmeid. Seetõttu on tarkvara korrapärane uuendamine väga tähtis ja üks lihtsamaid tegevusi, millega oma ettevõtte vara kaitsta.

Kui tarkvara automaatne uuendamine on võimalik (näiteks arvutite ja nutiseadmete operatsioonisüsteemide puhul), siis tuleks see sisse lülitada. Kui aga tarkvaras sellist funktsiooni pole (näiteks eri programmid või võrguseadmete tarkvara), peab seda tegema käsitsi (ise, IT-personali või -teenusepakkuja abiga) või kasutama lahendust, mis aitab seda teha automaatselt. Näiteks paljud tänapäeva viirustõrjelahendused pakuvad funktsionaalsust, mis aitab mugavalt ja automaatselt programme uuendada.

Kui tootja tarkvara versiooni või riistvara enam ei toeta ega uuenda, siis tuleks üle minna uuemale versioonile. Näiteks Microsoft ei toeta 2020. aastast Windows 7 operatsioonisüsteemiga arvuteid, kuid neid on ikka veel ettevõtetes

kasutusel. Sel juhul oleks tulnud kindlasti minna üle Windowsi operatsioonisüsteemi uusimale versioonile, sest isegi kui veel ei ole vanas tarkvaras turvaauke avastatud, on ainult aja küsimus, kui neid avastatakse ja hakatakse ära kasutama. Tuleb lähtuda põhimõttest, et kui on olemas turvaauk, siis on olemas ka ründaja, kes seda heameelega ära kasutab. Hea varade haldus aitab jälgida näiteks uuenduste rakendamist või nende rakendamise vajadust.

3.3 Korralda oma ettevõtte arvutivõrgu ja selle kasutajate kaitse

Piiri avaliku Interneti ja kontorivõrgu vahel nimetatakse perimeetriks. Mida vähem kahtlast liiklust pääseb kontori võrku, seda väiksem on oht kontori võrku kasutavatele töötajatele ja seadmetele. Perimeetri kaitsmisel on abimeheks tulemüür, mis on vahendaja või lüüs avaliku ja kontori võrgu vahel ning filtreerib ohtliku liikluse. Rohkemate funktsioonidega tulemüürid suudavad tuvastada ja ka takistada kontori võrgu vastu suunatud rünnakuid. Sellised tulemüürid suudavad lisaks piirata, mis lehekülgedele on töötajatel lubatud või keelatud minna. Näiteks saab blokeerida tuntud ohtlikke lehekülgi või muid kahtlase väärtusega lehekülgi, mille kaudu võib tulla viiruseid. Samuti saab kontrollida, millised töötajate poolt kasutuses olevad rakendused Internetti pääsevad (näiteks saab keelata filmide ja muusika allalaadimise veebist).

Kuna palju viiruseid ja rünnakuid tuleb just e-posti kaudu, on rämpspostitõrje olemasolu vajalik. Selline tarkvara eemaldab kahtlased kirjad (spämm, õngitsus- ja viirustega kirjad jms) nii, et need ei jõua töötajateni. Enamik meiliservereid sisaldab mingil määral rämpspostitõrjet, kuid selle funktsionaalsus on tihtipeale piiratud. Rämpspostitõrjet on olemas ka näiteks välise teenusena pilves või majutuses (mis asub kontori võrgust väljaspool) või eraldi serverina kontori võrgus. Paremates rämpspostitõrje tarkvarades on hulk funktsionaalsusi, mis teevad töötajate elu kergemaks – kinni jäänud spämmi kohta raporti tellimine, kirjade vabastamine, saatjate blokeerimine ja palju muud.

Kuna ründajad on leidlikud, jõuab kahjurvara aeg-ajalt ikkagi kasutajateni. Seetõttu on tähtis, et kõigis seadmetes oleks kasutusel viirustõrje tarkvara, mis selle vastu kaitseks. Viirustõrje tarkvara puhul tuleb ka kindlasti jälgida, et see on viimane versioon ja uuendatud ning kõik funktsionaalsused on sisse lülitatud, sest ainult sel juhul on kaitse tõhus.

3.4 Tõkesta ligipääs andmetele, mis on kaotatud või varastatud seadmetes

Paratamatult mõnikord juhtub, et töötajad kaotavad oma seadmeid (nutitelefonid, tahvel või sülearvutid jms) või need varastatakse. Kuna seadmetes võib olla konfidentsiaalseid ettevõtte andmeid või muud teavet, mis ei tohi sattuda kolmandate isikute kätte, siis tuleks planeerida, mida sellises olukorras teha.

Üks abimees on peatükis 1.3 „Kaalu seadmete keskhalduse kasutusele võtmist“ kirjeldatud keskhaldus, mis võimaldab seadme kaotamise korral see kaugelt lukustada, leida selle asukoht või kõik andmed sealt kustutada. Nutiseadmetele, nagu telefonid ja tahvelarvutid, on olemas ka tasuta rakendusi, mis võimaldavad teha samu tegevusi, ning need tasuks kasutusele võtta.

Andmetele ligipääsu aitab tõkestada ka arvuti krüpteerimine – sellisel juhul on andmed arvutis küll olemas, aga varas ei saa nendega midagi teha. Krüpteerimiseks on erinevaid võimalusi, selleks on saadaval hulk programme ja lisaks saab kasutada krüpteerimistarkvara BitLocker, mis on operatsioonisüsteemiga Windows kaasas.

3.5 Hoolitse ka andmete ja seadmete füüsilise kaitse eest

Lisaks tarkvaralistele kaitsemeetmetele tuleb tähelepanu pöörata ka seadmete füüsilisele kaitsele. Kõik seadmed, kus paiknevad olulised andmed, peavad olema kaitstud võõraste isikute ligipääsu eest. Näiteks tulemüürist ei ole mingit kasu, kui keegi võõras saab vabalt kontorisse jalutada, sealt edasi serveriruumi minna ning seeläbi seadmetele otse ligi pääseda.

Serverid, võrguseadmed ja muud tähtsad seadmed, kus on andmed, peavad paiknema eraldi seadmekapis või selleks mõeldud serveriruumis. Seadmekapi või serveriruumi uks peab olema lukustatud ning võti kindlas kohas hoiul. Ühtlasi tuleks serveriruumi külastuste üle pidada logi (panna kirja, kes, millal ja mis eesmärgil serveriruumi külastas), et pärast saaks tuvastada, kes ja millal seal viibis.

Küsi IT-spetsialistilt

Kui server asub majutuses, siis veendu, et teenusepakkujal on teave selle kohta, kellel on füüsiline ligipääs sellele serverile ja kes on seda kasutanud.

Selleks, et server töötaks tõrgeteta, peab see olema piisavalt hästi jahutatud (serveriruumis konditsioneer) ja ühendatud UPSiga, et kaitsta seda voolukatkestuste eest. Muidu võib server kuumal suvepäeval lõpetada töö või voolukatkestuse korral võivad andmed saada rikutud. Ka konditsioneer võiks olla ühendatud UPSiga, sest muidu võib voolukatkestuse korral server esialgu küll tööle jääda, kuid hiljem ülekuumenemise tõttu töö lõpetada.

Kui kontoris on seinas võrgupesi, mida ei kasutata, siis ei tohiks nendest pesadest võrku pääseda (laske IT-personalil või -teenusepakkujal teha vastav seadistus). Muidu võib tekkida olukord, kus suvaline inimene ühendab sinna oma arvuti ja selle kaudu saab ligi kõikidele kontori seadmetele. Järgmine samm oleks teha seadistus, et arvutid ja serverid asuksid loogiliselt eraldi võrkudes, s.t kui keegi saab ligi arvutivõrgule, siis ei pääse ta kohe serveritesse.

Sama tähtis on töötajaid harida, et arvutist eemale minnes ei jäetaks seda lukustamata ja avalikes kohtades jälgitaks, et seadmed kuhugi maha ei unune, ega antaks neid kõrvalistele isikutele kasutada.

4. Kaitse oma töötajaid

Andmete ja kasutajate kaitsmiseks on tähtis, et igasugune süsteemidele juurdepääsemine nõuaks parooli või muud autentimisviisi. Parool peab olema piisavalt keeruline, et seda oleks raske ära arvata. Kui süsteem ei ole parooliga kaitstud või kasutatav parool on kergesti äraarvatav, siis saavad nii kahjurvara kui ka ründajad märgatavalt hõlpsamini süsteemile ligi. See võib kaasa tuua andmete lekkimise, hävimise või hoopis oluliste andmete muutmise.

4.1 Loo turvaline paroolipoliitika

Autentimine on tegevus, mille käigus süsteem tuvastab, kas isik, kes süsteemi poole pöördub, on see, kes ta väidab end olevat. Tavaliselt kasutatakse tuvastamiseks parooli või sertifikaati.

Et kontori võrk oleks turvaline, tuleb paika panna reeglid parooli keerukuse ja korrapärase vahetamise kohta. Tänapäeval soovitatakse parooli muuta mõistliku aja tagant, nt kuus kuud ja parool peaks olema vähemalt 12 tähemärki pikk. Parooli vahetus tuleb aga koheselt ette võtta, kui on kahtlus parooli lekkimisest või on toimunud

mõni intsident. Liiga pikka ja keerulist parooli pole ka hea nõuda, sest siis võivad kasutajad kirjutada selle kuhugi paberile. Seetõttu on tavaparooli asemel soovitatav kasutada märgulauset. Märgulause koosneb neljast-viiest sõnast, mis moodustavad lause (Näiteks: 1Hobune.On.Vee.Aar3s) – see on pikem, aga kasutajatele lihtsam meeles pidada kui juhuslikest kirjamärkidest koostatud parooli. Paroolis võiks kasutada suur- ja väiketähti, sõnade vahel aga sümbolit (punkt, koma, hüüumärk jne). Parool võiks olla lihtsasti meeldejääv, kuid samas ei tohiks olla liiga lihtsasti ära arvatav.

Kui süsteemiseadistused võimaldavad, tuleks määrata sätted, et sellised piirangud rakenduksid automaatselt, sest kasutaja valib võimalusel ikka lihtsama tee. Kui süsteemselt seadistada pole võimalik, tuleb paroole vahetada regulaarselt käsitsi ja seda peab kasutajatele pidevalt meelde tuletama. Väiksemates ettevõttetes tavaliselt ei ole eraldi paroolipoliitikat, aga tähtis on, et paroolide kasutamisel lähtutakse turvalisuse heast tavast.

Küsi IT-spetsialistilt

Küsi IT-personali või -teenusepakkuja käest, kas kehtiv paroolipoliitika vastab heale tavale. Vajadusel tuleb paroolipoliitika luua ja see rakendada.

4.2 Kasuta mitmikautentimist

Tänu pilvteenuse populaarsuse kasvule on ettevõtetes järjest rohkem teenuseid, mis on avalikult kättesaadavad kogu maailmas. Kui teenus on üldsusele kättesaadav, siis on seda lihtsam rünnata. Kui mõni taoline kommertsteenus (Office 365, Gmail, Dropbox vms) võimaldab, siis tasuks sisse lülitada mitmikautentimist. See tähendab, et peale parooli nõutakse veel mingit autentimismeetodit, näiteks koodi sisestamist, telefonis kinnitamist, ID-kaarti kasutamist, krüptotokenit jne. Kui mitmikautentimine on rakendatud, siis ei saa ründajad süsteemile ligi isegi parooli lekkimisel, sest neil puudub teine autentimiseks vajalik komponent.

4.3 Lihtsusta paroolide kasutamist

Kuna suurem osa süsteeme nõuab paroolide kasutamist, võib töötajal olla palju erinevaid kasutajanimesid ja paroole. Sel juhul hakkavad kasutajad neid ebaturvaliselt paberile kirjutama, kasutama võimaluse korral sama parooli mitmes kohas või valima paroole, mis on liiga lihtsad. Üks lahendus, et kasutajaid aidata, on võtta kasutusele paroolihalduse tarkvara, mis võimaldab neil turvaliselt oma paroole hallata. Selleks on saadaval erinevaid tarkvarasid ja osa neist on ka tasuta.

Kui seadmeid on rohkem, siis tasuks võtta kasutusele mõni keskne kasutajate halduse lahendus. Microsoft Windowsi keskkonnas on selleks puhuks olemas näiteks Active Directory (AD) domeen. AD domeen on teenus, mis võimaldab Windowsi keskkonnas integreeritud autentimist. Selle abil saavad kasutajad sisse logida sama kasutajanime ja parooliga kõikidesse seadmetesse, mis on domeenis. Näiteks kui enne domeeni kasutusele võtmist oli kasutajatel eraldi parool arvuti, e-posti teenuse ja jagatud kausta jaoks, siis tänu domeenile saab kõigile juurde ühe parooliga. AD domeen eeldab Windowsi serveri olemasolu. Leidub ka muid samalaadseid lahendusi, mis ei vaja serverit, näiteks Azure AD, mis eeldab Office 365 tarkvara litsentse. Ka mõnda majandustarkvara on võimalik siduda näiteks AD domeeni või Azure ADga. Keskne kasutajate haldus võimaldab muu hulgas kasutaja lahkumisel ligipääsud kergemini sulgeda, sest siis saab seda teha ühest kesksest kohast.

5. Õpi ära tundma rünnakuid

Süsteem on nii turvaline, kui on selle kõige nõrgem lüli. Tihti on nõrgimaks lüliks just kasutajad. Seetõttu üritavad küberkurjategijad süsteemile ligi saada peamiselt kasutajate kaudu, saates neile kirju, mis võivad sisaldada viiruseid või olla õngitsuskirjad, millega proovitakse kätte saada paroole, pangaandmeid või raha. Samuti leidub internetis veebilehti, mis proovivad kasutajatelt välja petta andmeid ja raha või sisaldavad viiruseid. Seetõttu tuleb õpetada töötajatele, kuidas rünnakuid ära tunda ja nende korral käituda. Töötajate teavitamine ja harimine on ka üks tähtsamaid samme ettevõtte kaitsmisel.

5.1 Suurenda töötajate teadlikkust

Viimaste aastate jooksul on küberkurjategijad märgatavalt arenenud ja järjest raskem on aru saada, kas saadetud kirja või külastatava veebilehe puhul on tegemist pettusega või mitte.

Töötajatele tuleks tutvustada, millised on enim levinud rünnakud, kuidas neid ära tunda ja nende korral käituda. Sellist teavitamist ja juhendamist aitab teha IT-personal või teenusepakkuja.

Enim levinud rünnakud on petukirjad ja veebilehed, mis üritavad kasutajat panna sisestama oma andmeid (phishing ehk andmepüük). Andmete õngitsemine ongi kõige tõenäolisem ja küberkurjategijale ka kergeim viis, mille kaudu ettevõtte seadmetesse sisse saada.

Levinud petukirjade näiteid:

E-kirjad, mis sisaldavad manuses arveid, mis tulevad justkui ettevõtte partneritelt ja kus palutakse kiiresti tasuda maksmata arve mõnele teisele pangakontole kui tavaliselt.

Näiliselt tegevjuhi või juhatuse liikme saadetud e-kiri ettevõtte raamatupidajale, kellel palutakse teha ülekanne mingile pangakontole.

Mõnelt teenusepakkujalt (e-posti teenus, pangateenus, internetiteenuse pakkuja jne) pärinev kiri, kus palutakse sisestada isikuandmeid ja küsitakse kasutaja parooli või PIN koode.

Küsi IT-spetsialistilt

Tähtis on meeles pidada, et pank või e-posti teenuse pakkuja ei küsi ega vaja sinu paroole!

Kui mõni saadud e-kiri tundub kahtlane, siis tasub alati pöörduda oma IT-personali, teenusepakkuja või CERT-EE poole ning paluda neil see kiri üle vaadata. Isegi kui selgub, et see e-kiri on ehtne, on parem karta, kui kahetseda.

Töötajaid tuleks õpetada ära tundma petu- ja õngitsuskirju ning ohtlikke veebilehti:

1. Tuleks vaadata e-kirja saatja aadressi – kuigi mõnikord tundub see ehtne, on saatja aadress enamasti väikeste muutustega. Näiteks „@eesti.ee" asemel võib olla „@eetsi.ee". Mõnikord, kui aadress tundub ehtne, võib kirjale vastates olla näha, et adressaadireal on hoopis keegi teine kui e-kirja saatja.
2. Veebilehtede puhul tuleks vaadata nende aadressi. Sarnaselt e-kirja aadressidega võib ka veebilehe aadress olla muutustega, näiteks aadressi lõpus on „.ee" asemel „.ea" või on lisatud aadressile tähtede asendamiseks numbreid, näiteks „eesti.ee" asemel on „eest1.ee".
3. Igasugused e-kirjad ja veebilehed, mis lubavad raha, reisi, tasuta väärtuslikke asju vms, on suure tõenäosusega pettused.
4. Kuna küberkurjategijad pärinevad tavaliselt teistest riikidest, siis on tihti e-kiri või veebileht eesti või inglise keelde tõlgitud Google Translate'i või muu sarnase lahenduse abil ja seetõttu võib sisaldada märgatavalt palju grammatika- või stiilivigu. Kuna küberkurjategijad pidevalt arenevad ja tõlkeprogrammid lähevad järjest paremaks, siis pimesi ei tohi usaldada ka heas eesti või inglise keeles kirjutatud e-kirja või veebilehte.
5. Kui e-kiri tuleks justkui ettevõtte juhatuselt või raamatupidajalt, tuleks vaadata, kas kirja stiil on selline nagu tavaliselt, eriti kui nõutakse raha ülekandmist. Tavaliselt on petukirjad kahtlaselt lühikesed ja toonilt ähvardavad (näiteks stiilis „Maksa kohe, see peab 24 tunni jooksul makstud olema!" jne).

5.2 Koolita töötajaid

Lisaks töötajate üldise küberturvalisuse teadlikkuse suurendamisele tuleks korraldada lõppkasutajate koolitusi. Selline koolitus peab hõlmama turvateemasid laiemalt: käitumist sotsiaalmeedias, avalike pilveteenuste kasutamist, WiFi turvalist kasutamist jms.

Koolituskava võiks hõlmata:

1. ettevõttes kehtestatud IT-turvareeglite tundmaõppimist, turvanõuete ja riskide selgitamist;
2. erinevate seadmete ja teenuste (kaasaskantavad seadmed, sotsiaalmeedia, avalikud pilveteenused jne) ohtude analüüsi;
3. turvaintsidentide korral käitumist (keda teavitada, mida teha jne);
4. võimalike ohtude ja enim levinud ründeviiside äratundmist, selliste rünnete tagajärgede hindamist;
5. hiljutiste avalikuks tulnud turvaintsidentide analüüsi koos põhjuste ja võimalike ennetusviiside kirjeldusega;

5.3 Kontrolli regulaarselt töötajate teadmisi

Selleks et kontrollida, kas töötajate üldine juhendamine ja koolitamine on tulemust andnud, tuleb nende teadmisi regulaarselt kontrollida. See aitab õpitut meelde tuletada ja värskelt meeles hoida. Teadmisi saab kontrollida näiteks küsitluste abil, mida võivad pakkuda erinevad küberturvalisuse teenuseid või koolitusi pakkuvad ettevõtted – nemad oskavad kõige paremini ka neid teste ajakohastada. Nii saab ettevõte ka teavet, kas mõne teema puhul oleks vaja töötajatele korduskoolitust.

Töötajate käitumise kontrollimiseks on hea korraldada ka väikeseid õppusi – näiteks saata töötajatele võlts õngitsuskiri. Selliste testide tulemuste alusel saab teada, mida peaks kasutajatele veel rääkima või kas on vaja lisakoolitust. Teavita inimesi intsidentide analüüsi tulemustest ja kaasa neid reeglite väljatöötamisse. Nii on nad motiveeritud ise neid reegleid täitma.

6. Õpi taastuma

Paratamatult esineb mõnikord olukordi, kus andmed (failid, e-kirjad, andmebaasid jms) kustuvad või riknevad. Põhjuseks võib olla, et töötaja kustutab kogemata mõne faili ära või salvestab faili valede andmetega üle. Lisaks esineb küberrünnakuid (näiteks krüptoviirused), seadmete vargust või õnnetusi (tulekahju, üleujutus), mis hävitavad või rikuvad andmed. Seetõttu on oluline, et kõik ettevõttele tähtsad andmed on varundatud ja varukoopiad talletatakse turvalises asukohas.

Hea teada!

Krüptoviirus ehk lunavara on viirus, mis krüpteerib kõik andmed või osa nendest arvutis või serveris, mille taga-järjel ei saa neid enam kasutada. Selleks, et failid uuesti kasutuskõlblikuks muuta, on vaja maksta ründajatele lunaraha.

6.1 Loo taasteplaan

Väga oluline on luua taasteplaan. Kuigi võib tunduda, et on teada, kuidas mingi tõrke puhul süsteem taastatakse, siis Murphy seadustele tuginevalt võib oletada, et infosüsteemi taastamise vajadus tekib ettevõtte kõige kiiremal tööajal, kui konkreetses süsteemis kõige paremini orienteeruv spetsialist pole kättesaadav. Sel juhul on abiks taasteplaan, mis aitab kõige kriitilisemas olukorras kiiresti ja korrektselt süsteemi taastada. Taasteplaanis on üksikasjalikult ja samm-sammult kirjas, mis tegevusi spetsialist peab süsteemi taastamiseks tegema.

Taasteplaanis peab olema detailselt kirjas kogu vajalik teave ettevõttele tähtsate süsteemide taastamiseks:

1. riist- ja tarkvara kirjeldus – kõik seadmed, tööriistad, andmed ja tarkvara versioonid, mis on taastamiseks vajalikud, ning nende täpne asukoht;
2. sammsammuline tegevusjuhend – mis tegevusi millises järjekorras tuleb teha;
3. taastatava süsteemi seadistused;
4. taastamiseks vajalikud kasutajad (teenuskontod, administraatori parool jne).

6.2 Taga varunduse toimimine ja kontroll

Varunduse kavandamisel tuleb kõigepealt määrata, millised on ettevõttele tähtsad andmed, mis peavad olema varundatud. Varundada tuleb kõike vajalikku – e-kirjad, majandustarkvara andmebaasid, jagatud kataloogid ja failid – ning arvestama peaks ka kasutajate arvutites olevaid andmeid.

Teiseks tuleb läbi mõelda, kui vanu andmeid peab olema võimalik varukoopiast taastada. Olulisi andmeid, nagu igapäevaselt kasutatav jagatud kaust või majandustarkvara, võib olla vajalik varundada iga päev ja näiteks alles hoida ühe kuu seisud (see tähendab, et on võimalik taastada kuu aega vanu andmeid). Andmeid, mis tihti ei muutu (näiteks pildipank või arhiiv), võib varundada ka kord kuus ja nendest hoida alles vaid üks seis.

Küsi IT-spetsialistilt

Lepi IT-personali või -teenusepakkujaga kokku varunduse (mis andmed, sagedus, varukoopiate arv) korraldamine.

Et kaitsta varukoopiat õnnetuse (tulekahju, üleujutus) või varguse puhul, tuleks teha ka väline varukoopia. Selline varukoopia võib asuda pilves, teises kontoris või näiteks teenusepakkuja juures majutuses. Sel juhul on seadmete ja andmete hävimisel väline varukoopia kindlas kohas olemas. Pilvteenuse või välise teenusepakkuja puhul tuleks arvestada, et andmed asuvad kellegi teise juures, ning siis tuleb kaaluda, kas oma konfidentsiaalseid andmeid ja ärisaladusi sinna varundada või mitte.

Tähtis on tagada ka varunduse edukas toimimine, sest mittetoimunud või vigasest varundusest ei ole võimalik andmeid taastada. Selleks tuleb seadistada teavitus e postile varukoopiate toimimise kohta ning regulaarselt kontrollida varukoopiate tegemise logisid, et teha kindlaks, kas varukoopiate tegemine on läinud edukalt. Perioodiliselt on mõistlik kontrollida, kas kõik vajalikud andmed on ikka varundatud (näiteks võib olla mingi kaust tõstetud teise kohta ja varunduses on see seadistamata), ning vajaduse korral muuta varukoopia seadistusi. Lisaks on tähtis pidada varundamise kohta dokumentatsiooni: mis andmeid ja kuhu varundatakse, mitu seisu hoitakse, mis programm varundab jms teavet.

6.3 Tee proovitaastamisi

Väga tähtis on regulaarselt teha proovitaastamisi. Nende käigus taastatakse mõni oluline süsteemi osa praegusest süsteemist eraldatud asukohta (et see ei mõjutaks töökeskkonda) ja vaadatakse üle, kas peale taastamist kõik töötab. Proovitaastamised on tähtsad, sest isegi kui tundub, et varukoopiad on edukalt tehtud, võib süsteemi taastamisel esineda vigu, mida ei osata ette näha. Näiteks võib varukoopia olla vigane, andmeid võib olla puudu või selgub, et süsteemi taastamiseks on vaja teha lisaseadistusi. Kõik avastatud kõrvalekalded ja eriseaded tuleb dokumenteerida taasteplaanis. Proovitaastamisi tuleb teha kõigi tähtsate süsteemide kohta ja varukoopia proovitaastamiseks tuleks valida pisteliselt.

Küsi IT-spetsialistilt

Küsi IT-personali või -teenusepakkuja käest, kas ettevõtte süsteemide taastamiseks on taasteplaan olemas ning kas proovitaastamised on tehtud. Kui vaja, tuleb luua taasteplaan ja korraldada proovitaastamine.

7. Kaitse oma kaubamärki

Ettevõtte kaubamärgiga on seotud avalikud veebilehed, sotsiaalvõrgustiku kontod ja e posti aadressid. Kuna need on avalikult nähtaval, siis on oht, et ründajad tahavad neid ära kasutada firma maine kahjustamiseks, raha saamiseks või muul põhjusel. Seetõttu on tähtis, et need oleksid kaitstud.

7.1 Teadvusta võimalikke ohte

Avalikke teenuseid (veebilehed, e-post) varitsevad ohud, mille kaudu võib olla häiritud ettevõtte töö ja mis võivad ettevõtte mainet kahjustada.

Avalike veebilehtede puhul võivad esineda näiteks järgmised ohud:

1. Ründajad võivad teha ettevõtte veebilehe kättesaamatuks. See halvab näiteks e-kaubandusega tegeleva ettevõtte töö ja segab ka paljude teiste ettevõtete tööd, sest kliendid ei pruugi veebilehelt saada vajalikku teavet.
2. Ründajad võivad pääseda veebilehe haldusele ligi ja varastada sealt näiteks ettevõtte klientide andmeid, mis võib kaasa tuua mainekahju ja GDPRi trahvid.

3. Ründajad võivad muuta veebilehe sisu sobimatuks (näiteks solvavaks), mis jällegi võib segada ettevõtte tööd ja kahjustada selle mainet.
4. Ründajad võivad paigaldada veebilehele tarkvara, mis nakatab veebilehte külastavad kliendid kahjurvaraga. See toob kaasa olukorra, kus ettevõtte kliendid hakkavad seda veebilehte vältima, isegi kui see on korda tehtud.

Hea teada!

GDPR (General Data Protection Regulation) on Euroopa isikuandmete kaitse üldmäärus, millega kehtestatakse suunised isikuandmete töötlemiseks Euroopa Liidus. GDPRi rikkumine võib kaasa tuua suured trahvid: 20 000 000 eurot või 4% eelneva majandusaasta käibest, olenevalt sellest, kumb on suurem. Trahvid võivad intsidendi korral rakenduda juhul kui näiteks asutus on ignoreerinud tehniliste ja protseduuriliste turvameetmete rakendamist. Täpsemalt saab lugeda siit:

Kui ründajad võtavad üle sotsiaalvõrgustiku kontod, võib see ettevõttele kaasa tuua nii maine- (tehakse ebasobivaid postitusi, solvatakse kliente jne) kui ka rahakahju, kui need kontod on seotud maksetega (näiteks Facebooki reklaami ostmiseks on lisatud krediitkaardi teave, millele ründajad saavad ligi). Tuleks arvestada, et lisaks ettevõtte enda sotsiaalvõrgustike kontodele tuleb kaitsta ka ettevõtte juhtkonna ja võtmetöötajate kontosid.

Kui ettevõtte e-posti teenus ei ole kaitstud, võivad ründajad kasutada ettevõtte e-posti aadresse, et petta selle töötajatelt või partneritelt raha välja või saata rämpsposti. See võib tuua kaasa nii maine- kui ka rahakahju.

7.2 Kaitse end ohtude vastu

Ohtude vastu kaitsmise esimene samm on teadvustamine, et need on olemas. Ohtude vastu kaitsmiseks on hulk tegevusi, mida ettevõtted saavad ise teha, et neid ohte ära hoida.

7.2.1 Vali tööriistad turvanõrkuste tuvastamiseks

Avalike teenuste rünnakuks kasutatakse tavaliselt ära teenuste (näiteks veebileht või e posti server) tarkvaras olevaid turvaauke, nõrku turvasätteid, muutmata paroole jne. Turvanõrkuste tuvastamiseks on olemas erinevaid tööriistu, mis teevad seda automaatselt. Sellised tööriistad skaneerivad avalikke teenuseid ja loovad avastatud turvanõrkuste kohta ülevaatlikud aruanded. Peale nende avastamist tuleks IT-personalil või teenusepakkujal need kõrvaldada. Seejärel tuleb teha uus skaneerimine ja vaadata, kas varem avastatud turvanõrkused on kõrvaldatud. Neid on vaja skaneerida regulaarselt (näiteks kord kuus), et järjepidevalt uusi turvanõrkuseid avastada ja need kõrvaldada.

Küsi IT-spetsialistilt

Turvanõrkuste avastamiseks on saada erinevaid lahendusi. Küsi oma IT-personalilt või teenusepakkujalt sobivat tarkvara.

7.2.2 Kaitse oma avalikke teenuseid

Avalike teenuste kaitsmiseks tuleb kõrvaldada avastatud turvanõrkuseid. Tähtis on ka see, et veebilehtede või e-posti serveri tarkvara oleks uuendatud (vt peatükk 2.2 „Taga tarkvara regulaarne uuendamine“). Uuendama peab nii teenuse serveri kui ka teenuse enda tarkvara.

Küsi IT-spetsialistilt

Kui server on teenusepakkuja juures majutuses ja tema hallata, siis tuleb teenusepakkujalt uurida, kas serveri tarkvara uuendatakse korrapäraselt ning kas see on tehtud.

E-posti teenuse kaitsmiseks peab IT-personal või -teenusepakkuja tegema järgnevad seadistused:

1. Selleks et ründajad ei saaks vabalt kasutada ettevõtte e-posti aadresse, tuleks DNSi luua SPF-kirje (Sender Policy Framework), mis ütleb, millised e-posti serverid võivad kirju saata ettevõtte e-posti domeeni alt.
2. Selleks et tõestada ettevõtte e-posti serveri õigsust, on võimalik seadistada ka DKIM (DomainKeys Identified Mail). DKIM allkirjastab serverist väljuvad e-kirjad ning teised e-posti serverid kontrollivad, kas antud allkiri on õige. DKIMi kasutusele võtmiseks peab e-posti server seda toetama või on vaja selleks osta või paigaldada lisatarkvara.
3. DMARC (Domain-based Message Authentication, Reporting and Conformance) levitab DNSi kaudu e-posti serveritele poliitika, mis ütleb, mida peaks sellelt domeenilt tulnud e-kirja puhul kontrollima ja kuidas e-posti server peaks selle kirjaga edasi käituma. DMARC kasutab SPFi ja DKIMi, et oma poliitikale vastavust kontrollida. DMARCi saab kasutada ka ainult SPFi abil, kuid on turvalisem, kui ka DKIM on kasutuses. DMARC abil on võimalik saada raport selle kohta, kas keegi on üritanud saata kirju mujalt kui lubatud kohtadest.

7.2.3 Kaitse oma sotsiaalvõrgustiku kontosid

Tihti rünnatakse ettevõtete sotsiaalvõrgustiku kontosid, nagu Twitter, Facebook, Instagram jne. Ohtu satuvad ka ettevõtte juhtkonna ja võtmetöötajate kontod ning neid tuleb samamoodi kaitsta.

Ettevõtte sotsiaalmeedia kontode kaitseks tuleb teha järgnevaid tegevusi, mis ei ole üldse keerulised, kuid suurendavad turvalisust märgatavalt:

1. Loo ettevõtte sotsiaalmeedia kasutamise eeskiri (mis töötaja mis kontole ligi pääseb, milleks kontosid kasutatakse, mis töötaja neid haldab, kuidas töötaja sotsiaalvõrgustikes käitub jne).
2. Kasuta tugevaid paroole!
3. Vaheta paroole regulaarselt. Kindlasti peab paroolid vahetama, kui ettevõttest lahkub töötaja, kes pääses sellele kontole ligi.
4. Lülita kindlasti sisse mitmeastmeline autentimine.
5. Kontrolli aeg-ajalt üle olemasolevad sotsiaalmeedia kontod. Kontrolli, kes kontodele ligi pääsevad, ja eemalda ligipääsud ettevõttest lahkunud isikutelt ja nendelt, kellel pole neid ligipääse vaja.
6. Kontrolli üle ka kontode sätted, sest sotsiaalmeedia uuenemise käigus võib tekkida uusi privaatsussätteid või olemasolev seadistus võib muutuda (näiteks seni privaatne teave võib olla kõigile näha).
7. Kui kontod ei ole aktiivselt kasutuses, tuleks neid ikkagi jälgida, et tuvastada võimalik konto ülevõtmine.

Küsi IT-spetsialistilt

Kui ettevõte on sotsiaalmeedia võrgustikes aktiivne, siis tasub kaaluda sotsiaalmeedia kontode kaitseks mõeldud tarkvaralahenduse kasutamist. See võimaldab näiteks automaatselt eemaldada kahtlast sisu, takistada lubamata sisu avaldamist, avastada ettevõtte kaubamärgiga loodud teisi kontosid jne. Küsi oma IT-personalilt või -teenusepakkujalt selliste lahenduste kohta.

8. Eesti infoturbestandard (E-ITS)

Käesolev lühijuhend aitab ettevõtetel astuda esimesi samme küberturvalisemate äriprotsesside suunas. Edasijõudnutele on Riigi Infosüsteemi Ameti eestvedamisel valminud Eesti infoturbestandard – etalonturbel põhinev, riskihaldusele suunav, eestikeelne ning Eesti õigusruumile vastav infoturbe halduse süsteem, mis on ühtlasi vastavuses rahvusvaheliselt tunnustatud standardiga ISO/IEC 27001.

E-ITS pakub tüüpseid lahendusi kasutavatele organisatsioonidele ettevalmistatud komplekte turvameetmetest (nt tüüptarkvara, väljasttellimine, tulemüürid jne). Etalonturve võimaldab organisatsioonil taaskasutada infoturbe parimaid praktikaid ning seeläbi kokku hoida infoturbe rakendamisele kuluvaid vahendeid. Etalonturbest välja jäävale osale pakub E-ITS riskipõhist infoturbe haldust nii, et tulemuseks oleks siiski organisatsiooni põhine ja kaitsetarbest lähtuv terviklik lahendus.

E-ITS on küll esmajoones loodud avaliku sektori asutustele, kuid sobilik ka kõigile teistele asutustele sõltumata suurusest ja kasutatavast tehnoloogiast. E-ITSiga seonduvad materjalid on koondatud portaali eits.ria.ee.

Mida teha, kui toimub küberintsident?

Püüa võimalikult kiiresti aru saada intsidendi põhjustest ja allikast, et intsident peatada ning kahjusid vähendada.

Teavita RIA intsidentide käsitlemise osakonda CERT-EE (cert@cert.ee).

Teavita oma töötajaid intsidendi toimumisest.

Kaalu, kas sul on vaja intsidendi kohta koostada raport politseile ja/või andmekaitseinspektsioonile.

Teata intsidendist oma klientidele või koostööpartneritele, keda see mõjutab.

Teavita jooksvalt oma töötajaid, kliente (ja vajaduse korral avalikkust) sellest, kuidas intsidendist taastumine läheb.