



RIIGI INFOSÜSTEEMI AMET



Euroopa Liit
Euroopa
Regionaalarengu Fond



Eesti
tuleviku heaks

Ettevõtte küberturvalisuse lühijuhend

2025

Sisukord

1	Tugevamad ettevõtted loovad tugevama ühiskonna.....	3
1.1	Vastutus on ettevõtte juhil.....	3
2	Tee selgeks ettevõtte kaitsevajadused	4
3	Tea, millist riist- ja tarkvara kasutad	4
3.1	Inventeeri oma riistvara.....	5
3.2	Inventeeri oma tarkvara	5
3.3	Kaalu seadmete keskalduse kasutusele võtmist	5
3.4	Loo reeglid isiklike seadmete kasutamiseks töökeskkonnas	6
3.5	Mõtle läbi pilveteenuste kasutamine	6
3.6	Kasuta uusi tehnoloogiaid turvaliselt.....	8
4	Kaitse oma vara	9
4.1	Anna juurdepääsuõigused põhjendatult.....	9
4.2	Uuenda tarkvara regulaarselt.....	10
4.3	Korralda oma ettevõtte arvutivõrgu ja selle kasutajate kaitse.....	11
4.4	Tõkesta ligipääs andmetele, mis on kaotatud või varastatud seadmetes.....	11
4.5	Hoolitse ka andmete ja seadmete füüsilise kaitse eest	12
5	Kaitse oma töötajaid.....	12
5.1	Loo turvaline paroolipoliitika.....	12
5.2	Kasuta mitmikautentimist	13
5.3	Lihtsusta paroolide kasutamist.....	13
6	Õpi ära tundma rünnakuid.....	14
6.1	Suurenda töötajate teadlikkust.....	14
6.2	Koolita töötajaid	14
6.3	Kontrolli regulaarselt töötajate teadmisi	15
7	Valmistu intsidendiks ja õpi taastuma	15
7.1	Tea, kuidas toimida intsidendi korral.....	15
7.2	Loo taasteplaan	16
7.3	Oma ülevaadet sellest, mis süsteemides toimub.....	16
7.4	Taga varunduse toimimine ja kontroll	17
7.5	Tee proovitaastamisi.....	17
8	Kaitse oma kaubamärki.....	18
8.1	Teadvusta võimalikke ohte	18
8.2	Kaitse end ohtude eest	19
9	Pööra tähelepanu tarneahelale	21

1 Tugevamad ettevõtted loovad tugevama ühiskonna

Küberturvalisuse seadus seab küberturvalisuse nõuded sellistele ettevõtetele ja asutustele, mille tegevus on elutähtis – riigiasutustele, sadamatele, energiaettevõtetele, sideoperaatoritele jt. Samal ajal sõltub Eesti inimeste küberturvalisus ka sellest, kui turvaliselt suudavad end ja oma kliente (nende andmeid) kaitsta kõik teised, väiksemad ettevõtted ja asutused, millele samasuguseid nõudeid seadusega kehtestatud ei ole. Infoturbejuhtide või -meeskondade palkamine võib neil käia üle jõu, küberturvalisuse standardid võivad paista niivõrd mahukad ja ressursikulukad, et nende rakendamine ei tundu äriiselt mõistlik.

Käesolev lühijuhend on mõeldud selleks, et aidata ettevõtetel astuda esimesi samme küberturvalisemate äriprotsesside suunas. Infoturbe tagamine on aga pidev protsess. Kui esimesed sammud on tehtud, tasub tutvuda Eesti infoturbestandardis toodud [soovitustega](#) väikestele asutustele ja ettevõtetele¹ - sealt leiab järgmised tegevused, et infoturvet ettevõttes veelgi paremini korraldada.

1.1 Vastutus on ettevõtte juhil

Alustama peaks sellest, et küberturvalisus ei ole üksnes IT-osakonna asi, vaid ka juhtimise ja juhtide küsimus. Mida selgemalt ärijuht mõistab vajadust meetmeid rakendada, seda paremini saab ta suunata oma meeskonda ja vahendeid. Juhil on võtmeroll organisatsiooni infoturbe tagamisel ning just juhtide tegevus ja otsused mõjutavad otseselt organisatsiooni suutlikkust kaitsta oma andmeid ja süsteeme. 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

Tee nii!

1. Tee infoturbe organisatsiooni strateegiliseks prioriteediks ning eralda rahalised, tehnilised ja inimressursid infoturbe rakendamiseks.
2. Lähtu infoturbealastest seadustest, eeskirjades ja standarditest.
3. Kaardista organisatsiooni kohustused, vastutused, varad ja riskid.
4. Defineeri organisatsiooni riskitaluvuse tase ning määra infoturbe eest vastutajad.
5. Oma ülevaadet infoturbe seisundist ja võimalikest intsidentidest.
6. Läbi regulaarselt turvakoolitusi ning panusta ka töötajate teadlikkuse tõstmisesse.
7. Kujunda infoturvet väärtustav töökeskkond. Ole ka ise eeskujuks, järgides infoturbe parimaid tavasid ja poliitikaid.

¹ <https://eits.ria.ee/et/abimaterjalid/veits>

2 Tee selgeks ettevõtte kaitsevajadused

Infoturve algab selgest arusaamast – mida ja miks me kaitseme. Sageli on just (väikesed ja keskmise suurusega) ettevõtted need, kes ei pruugi osata mõista küberturvalisuse olulisust ning puuduliku infoturbega kaasnevaid riske.

Kaitsetarve on kogum turvanõuetest, mis on vaja täita, et organisatsiooni äriprotsessid saaksid kvaliteetselt toimida. Kaitsetarve hindamiseks tasub läbi mõelda erinevad kahjustsenaariumid, näiteks

1. Millised regulatsioonid ja lepingud seavad organisatsioonile nõudeid/ootusi.
2. Millised on organisatsiooni tegevusega kaasnedavad võivad kahjud kellegi elule ja tervisele?
3. Millised on kahjud, kui organisatsiooni ülesanded jäävad täitmata ja töö kvaliteet pole ootuspärane?
4. Millised tagajärjed võivad kaasa tuua organisatsiooni maine kahjustumine?
5. Milliseid rahalisi tagajärjed võivad kaasa tuua andmete ja süsteemidega seotud rikked?

Stsenaariumite läbimõtlemissel saab organisatsioon enda jaoks teada kõige nõrgemad valdkonnad, mille kaitseks tuleb panustada esmajärjekorras. Samuti selgub riskitaluvus ehk riskikriteeriumid – millisel juhul piisab olukorra jälgimisest ja millisel juhul tuleb kaitsemeetmeid rakendada kohe.

Digitaliseerinud ühiskonnas on hädavajalik, et ettevõtte loomulikuks osaks oleks ka turve, ehk turvariski käsitletakse nagu iga muud äririski. Kui ettevõtte on selgitanud välja oma kaitsevajadused, 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.

3 Tea, millist riist- ja tarkvara kasutada

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 paigaldatud 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 ID või nimi;
2. tootja ja mudel;
3. seadme seerianumber;
4. IP-aadress;
5. seadme eesmärk või põhjus, miks see võrgus on (arvuti, server, võrguseade jne);
6. seadmesse installitud tarkvara nimekiri;
7. millise äriprotsessi toimimist see mõjutab;
8. kuidas varad on omavahel seotud.

3.1 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 kaitsemata seadmeid, et sealtkaudu ettevõtte võrku rünnata. Ülevaade võrgus olevatest seadmetest on vajalik ka siis, kui IT-personal või teenusepakkuja 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.

3.2 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.

3.3 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 paigaldatud, 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 vajalik juhul, kui töötaja peaks seadme kaotama või see varastatakse.

Küsi IT-spetsialistilt

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

3.4 Loo reeglid isiklike seadmete kasutamiseks töökeskkonnas

Tänapäeval on järjest tavalisem, et töötajad soovivad tööks kasutada isiklike seadmeid. Väga levinud on nutiseadmed (telefonid ja tahvelarvutid), aga üha enam kasutatakse ka isiklike arvuteid. Lisaks tuuakse tööle enda USB-mälupulki ja väliseid kõvakettaid, mis võimaldavad kiiresti ja lihtsalt andmeid sisevõrgust välisele andmekandjale liigutada.

Kui töötajatel on lubatud isiklike seadmeid kasutada, tuleb selleks paika panna reeglid, sest isiklikel seadmetel töödeldakse ka ettevõtte andmeid. 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 paigaldatud viirustõrje tarkvara;
2. koostada nimekiri seadmetest ja operatsioonisüsteemidest, mida pole lubatud ettevõttes kasutada, näiteks turvaaukudega seadmed või seadmed, mille tarkvara tootja enam ei toeta. Lisaks peaksid olema keelatud 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. panna paika juhised välise andmekandjate, näiteks mälupulk või kõvaketas, kasutamiseks;
5. 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).

3.5 Mõttele läbi pilveteenuste kasutamine

Pilveteenused pakuvad ettevõtetele suurt paindlikkust, kulude kokkuhoidu ja paremat ligipääsu andmetele. Samas toovad need kaasa uusi riske, mida tuleb teadlikult hallata. Alljärgnevad põhimõtted aitavad teha teadlikke otsuseid pilveteenuse valikul ja kasutamisel, tagades ettevõtte andmete turvalisuse.

3.5.1 Vali sobiv teenusepakkuja

Esmalt on oluline valida teenusepakkuja. Pakkuja valik on strateegiline otsus, mis mõjutab ettevõtte andmete turvalisust - hoolikas planeerimine ja teadlik valik aitavad tagada, et ettevõtte saab pilveteenustest maksimaalset kasu, minimeerides samal ajal võimalikke riske. Peamised kaalutlused pilveteenuse pakkuja valimisel:

1. Veenduda, et teenusepakkuja järgib asjakohaseid turvastandardeid ja regulatsioone.
2. Oluline on teada, kus andmeid hoitakse ja kuidas neid hallatakse. See on tähtis nii andmekaitse kui ka regulatiivsete nõuete täitmise seisukohalt.
3. Milline on teenusepakkuja töökindlus ja teenuse kättesaadavus – abiks võib olla info varasemate intsidentide ja selle kohta, kuidas teenusepakkuja on probleemid lahendanud.

4. Hea klienditugi on kriitilise tähtsusega. Tasub veenduda, et pilveplatvorm pakub õigeaegset ja asjatundlikku tuge.
5. Mis on teenuse maksumus ja lepingutingimused. Oluline on pöörata tähelepanud sellele, et teenusega ei kaasneks varjatud tasusid või lepingulisi kohustusi, seda ka andmete väljastamisel teenuse lõpetamisel.

Enne otsuse tegemist tasub uurida mitmeid teenusepakkujaid, võrrelda nende pakkumisi ja lugeda klientide tagasisidet.

3.5.2 Kasuta pilveteenuseid turvaliselt

Kui sobiv teenusepakkuja on leitud, tuleb pöörata tähelepanud pilveplatvormi turvalisele kasutamisele. Juba teenuse seadistamisel tasub läbi mõelda kõik turvaseaded, näiteks juurdepääsukontroll, võrgu turvaseaded ja logimise seadistamine. Paljud pilveteenuste pakkujad pakuvad sisseehitatud turvafunktsioone, mis aitavad kaitsta küberohtude eest – näiteks rämpsposti või kahjuliku sisu filtreerimine. Kontrolli neid kaitsevõimalusi regulaarselt ning vajadusel lülita haldusliideses sisse lisakaitse ja tee need kohustuslikuks kõigile kasutajatele. Õigesti seadistatud platvorm on pool võitu, ent turvalisus ei ole ühekordne tegevus. Pilvesüsteeme tuleb regulaarselt hooldada ja ajakohastada, et kaitsta süsteemi ja vältida teadaolevate turvanõrkuste ärakasutamist. Selle kõrval on äärmiselt oluline ka tegevuste logimine ja pidev jälgimine – nii saab kiiresti märgata, kui toimub midagi ebatavalist. Selleks tuleb seadistada süsteemilogid ja jälgida regulaarselt pilveteenuses toimuvat, et tuvastada potentsiaalseid intsidente ning neile kiiresti reageerida.

Viimaks ei tohi unustada andmete varundamist. Pilv ei välista vajadust regulaarselt andmeid varundada – pigem vastupidi. Andmetest tuleb regulaarselt teha varukoopiaid ja veenduda, et need on turvaliselt salvestatud. Mõne teenuse puhul pakub varundamist ka pilvteenus ise, kuid üks varukoopia tuleb alati hoida keskkonnast eraldi ning salvestatuna organisatsiooni kontrolli all olevale andmekandjale või teise pilvteenusesse. See tagab andmete taastamise võimaluse ootamatute probleemide korral. Turvalise varundamise kohta saab rohkem lugeda peatükist 7.3 Taga varunduse toimimine ja kontroll.

3.5.3 Tea, kes pääseb pilveteenustele ligi

Ettevõtte sees tuleb hoolega läbi mõelda, kellel millele ligipääs on. Iga töötaja peaks saama just sellise juurdepääsu, mis on tema töö tegemiseks vajalik – mitte rohkem.

Ka pilveteenustes luuakse igale kasutajale isiklik konto, mida haldab organisatsioon. Iga kontot tuleb aga kaitsta tugeva ja kordumatu parooliga ning mitmeastmelise autentimisega. Pilvteenuste kasutamisel ei tohi unustada sulgeda töölt lahkuvate töötajate kontod hiljemalt töötaja viimasel tööpäeval, et endisele töötajale ei jääks ligipääsu organisatsiooni andmetele. Nii saab vältida olukordi, kus volitamata isikud pääsevad ligi tundlikele andmetele. Rohkem teavet juurdepääsuõiguste ning kontode kaitsmise kohta saab juhendi peatükist 4.1 Anna juurdepääsuõigused põhjendatult ja peatükist 5 Kaitse oma töötajaid.

Administraatori kontol on rohkem õigusi kui tavakasutajal. Seetõttu tuleb neil, kes haldavad pilveteenuseid, kasutada eraldi administraatori kontot, mida ei kasutata igapäevaseks tööks. Pilvkeskkondade kasutamisel on väga oluline, et organisatsioonil oleks alati olemas administraatoriõigustega ligipääs oma kasutajakeskkonnale (ehk pilves eraldatud ja isoleeritud

keskkonnale, mis on mõeldud just sellele organisatsioonile). Selleks tuleb kasutajakeskkonna loomisel uurida, kuidas saab antud pilveteenuse pakkuja juures administraatori ligipääsu vajadusel taastada, ning teha vajalikud seadistused. Näiteks võib vaja minna sisestada administraatori kontaktandmed (nt lisameiliaadress) ja salvestada taastamiskoodid turvalises kohas väljaspool pilvkeskkonda, näiteks seifis. Ka administraatorikontod peavad olema kaitstud tugeva parooli ja mitmeastmelise autentimisega. Mõne pilveteenuse puhul saab piirata ligipääsu organisatsiooni kasutajakeskkonnale või haldusliidesele kindlate IP-aadresside või seadmete alusel. Lisaks tasub kaaluda tingimuslike ligipääsureeglite (*Conditional Access Policies*) kasutamist – need võimaldavad määrata, kes ja kuidas võib teenustele ligi pääseda, näiteks sõltuvalt asukohast, seadme turvasemest, kellaajast või kasutatavast rakendusest. Nii saab luua paindlikumaid ja tugevamaid kaitsemeetmeid kui ainult tavaliste staatiliste reeglitega

Oluline on anda töötajatele selged juhised pilveteenuste kasutamiseks ning viia ka nemad kurssi platvormiga seotud riskidega. Informeeritud ja ettevalmistatud personal suudab vältida paljusid levinud turvariske, mis tulenevad just hooletusest või teadmatusesest.

3.6 Kasuta uusi tehnoloogiaid turvaliselt

Tehisintellekt (TI) ja masinõpe võivad aidata ettevõttel kasvada, protsesse kiiremaks muuta ja kulusid vähendada. Samas on oluline mõista, et uute tehnoloogiatega kaasnevad ka riskid.

Hea teada!

RIA ja Cybernetica AS uurisid TI tehnoloogiaga kaasnevate riskide ja nende leevendamise võimalusi väikestes ning keskmistes ettevõtetes. Täpsemalt saab lugeda siit: <https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf>.

Selleks, et ettevõtte saaks kasutada tehisintellekti targalt, vastutustundlikult ja turvaliselt, tuleb läbi mõelda sammud, kuidas kaasnevaid riske juhtida:

1. Mõttele läbi, miks ja milleks TI-d kasutad

Enne TI kasutuselevõttu mõttele selgelt läbi, mida sa sellega saavutada tahad, näiteks millist probleemi see lahendab, milliseid andmeid kasutab ja kuidas see tehniliselt üles ehitatud on. Selge süsteemikirjeldus on vundament riskide mõistmiseks.

2. Vii end kurssi kogu elutsükliga

TI-süsteem ei ole lihtsalt „tehnoloogia käima panek“. Süsteemil on algus, arendus, kasutus ja hilisem hooldus. Seetõttu tuleb kaardistada süsteemi elutsükkel – alates planeerimisest ja andmete kogumisest kuni juurutamise ja pideva seireni. Riskid võivad tekkida igas etapis, mistõttu on vajalik järjepidev teadlikkus ja kontroll. Mõttele ka läbi, kes vastutab iga etapi eest ja mis võib valesti minna.

3. Veendu, et kõik oleks seaduslik

Kui TI kasutab isikuandmeid (nt klientide infot), pead järgima andmekaitse reegleid, nagu GDPR, kuid lisaks võivad valdkonnaspetsiifilised regulatsioonid nõuda täiendavat vastavust.

Kontrolli, kas sinu tegevus on seadustega kooskõlas ja kas sul on kõik vajalikud load ja nõusolekud.

4. Mõttele, keda see mõjutab

Meeles tasuks hoida, et lisaks tehnilistele ja õiguslikele aspektidele tuleb hinnata ka laiemat mõju. TI võib mõjutada kliente, töötajaid, kogukonda või keskkonda. Seetõttu mõttele läbi, kas süsteem võib olla ebaõiglane, eelistada ühte gruppi teisele või hoopis tekitada segadust ja muret. Sellised riskid ei pruugi olla kohe nähtavad, ent võivad pikas perspektiivis tekitada tõsisemaid tagajärgi.

5. Hinda riske ja leia lahendused

Pärast riskide kaardistamist on oluline valida sobivad meetmed riskide leevendamiseks. Tee nimekiri võimalikest probleemidest ja mõttele kui tõsised need on. Seejärel vali sobivad lahendused – võib-olla vajad paremat infoturvet, selgemaid reegleid või töötajate koolitamist. Läbimõeldud riskikäsitus aitab ennetada probleeme ja suurendab kasutajate usaldust.

4 Kaitse oma vara

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

Kuna seadmed ja 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.

4.1 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, majandustarkvarale, või administraatori õigused arvutisse) on 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 üksikshaaval läbi vaatama ja otsima, millele ta juurde pääses.

Igapäevane töö peaks toimuma tavakasutaja õigustes kontoga, mitte administraatori õigustes kontoga. Administraatori õigustega kaasneb hulk ohte:

1. Töötaja võib paigaldada oma arvutisse programme, millega võivad kaasnedada turvaaugud ja kahjurvara.
2. Kahjurvara tekitab kahju on suurem, kui töötajal on administraatori õigused.
3. Ründajad saavad siis kergemini arvuti üle kontrolli võtta jne.

Kui administraatori õiguseid on siiski vaja, tuleks sellele kasutajale teha eraldi õigustega administraatori konto, mida kasutatakse ainult vajaduse korral, mitte igapäevatoiminguteks. Sedasi väheneb tõenäosus, et kasutaja kogemata paigaldab kahjurvara, ning juhul kui töötaja konto andmed lekivad, ei saa ründaja kohe administraatori õiguseid. Kui see on töötaja isiklik arvuti, tuleb lähtuda punktist 3.4 „Loo reeglid isiklike seadmete kasutamiseks töökeskkonnas“, aga ka sel juhul võiks soovitada tööasjade jaoks eraldi kontot.

Küsi IT-spetsialistilt

Küsi IT-personalilt või -teenusepakkuvalt 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. Oluline on meeles pidada, et töölt lahkunud inimeste ligipääsud tuleb sulgeda ja õigused eemaldada.

4.2 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 tuleb üle minna tarkvara uuendada toetatud versioonile või riistvara välja vahetada. Näiteks ei toeta Microsoft 2025. aastast Windows 10 operatsioonisüsteemiga arvuteid. Sel juhul tuleks minna üle Windowsi operatsioonisüsteemi uusimale versioonile või kaaluda kasutusele võtta mõni alternatiivne operatsioonisüsteem. Aegunud tarkvara kasutamine võib mõjutada seadme turvalisust, ühilduvust ja tugiteenuseid, tuues endaga kaasa mitmed riskid. Näiteks jäävad uued turvaaugud ja haavatavused parandamata. See muudab süsteemi küberkurjategijate jaoks kergemini rünnatavaks. Isegi kui vanas tarkvaras ei ole veel turvaauke avastatud, on ainult aja küsimus, kui neid leitakse 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.

4.3 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 kontorivõrku kasutavatele töötajatele ja seadmetele. Perimeetri kaitsmisel on abimeheks tulemüür, mis on vahendaja või lüüs avaliku ja kontorivõrgu vahel ning filtreerib ohtliku liikluse. Rohkemate funktsioonidega tulemüürid suudavad tuvastada ja ka takistada kontorivõrgu vastu suunatud rünnakuid. Sellised tulemüürid suudavad lisaks piirata, mis lehekülgedele on töötajatel lubatud või keelatud minna. Näiteks saab blokeerida tuntud ohtlike 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 e-posti serveris vajalik viirusetõrje ja rämpspostitõrje tarkvara. Selline tarkvara eemaldab kahtlased kirjad (spämm, õngitsus- ja viirustega kirjad jms) nii, et need ei jõua töötajateni. Enamik meiliservereid sisaldab mingil määral rämpspostitõrjet. Rämpspostitõrjet on olemas ka näiteks välise teenusena pilves või majutuses (mis asub kontori võrgust väljaspool) või eraldi serverina kontorivõrgus. 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 tarkvara on viimane versioon ja uuendatud ning kõik funktsionaalsused on sisse lülitatud, sest ainult sel juhul on kaitse tõhus.

4.4 Tõkesta ligipääs andmetele, mis on kaotatud või varastatud seadmetes

Paratamatult juhtub mõnikord, 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 3.3 „Kaalude 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 krüpteerimine. Kui arvuti või väline kõvaketas varastatakse või läheb kaotsi, ei saa keegi seal olevaid andmeid lugeda, kui neil pole õiget parooli või võtit. Krüpteerimine teeb andmed loetamatuks, see on eriti oluline, kui seal on tundlik info (nt finantsandmed, isikuandmed või ärisaladused). Tänapäeva arvutites on juba olemas tööriistad, millega saab andmeid krüpteerida (näiteks BitLocker või FileVault). Samuti on olemas teised krüpteerimistarkvarad, mis võivad pakkuda lisaturvalisust. Oluline on meeles

pidada, et krüpteerimine töötab hästi ainult siis, kui kasutad tugevat parooli ja hoiad selle turvalises kohas.

4.5 Hoolitse ka andmete ja seadmete füüsilise kaitse eest

Lisaks tarkvaralistele kaitsemeetmetele tuleb tähelepanu pöörata 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 küllastuste üle pidada logi (panna kirja, kes, millal ja mis eesmärgil serveriruumi küllastas), 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 volukatkestuste eest. Muidu võib server kuumal suvepäeval lõpetada töö või volukatkestuse korral võivad andmed saada rikutud.

Kui kontoris on seinas võrgupeski, 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. Töötajatele ja külalistele tuleb luua erinevad WiFi võrgud, mis hoiab ära olukorra, kus võõrad pääsevad võrgu kaudu ligi ettevõtte sisevõrgule.

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.

5 Kaitse oma töötajaid

Andmete ja kasutajate kaitsmiseks on tähtis, et igasugune süsteemidesse sisenemine 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.

5.1 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 kontorivõrk oleks turvaline, tuleb paika panna reeglid parooli keerukusele ja pikkusele. Parooli vahetus tuleb koheselt ette võtta, kui on kahtlus parooli lekkimisest või on toimunud mõni intsident. Kõikidel kontodel – töö- ja erakontodel ning ka erinevatel sotsiaalmeediakontodel – tuleks kasutada erinevaid paroole. Hea parool on tugev (vähemalt 15 tähemärki ja erisümbolitega) ning unikaalne. Tavaparooli asemel on soovitatav kasutada märgulauset. Märgulause koosneb neljast-viest 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 meelde jääv, kuid samas ei tohiks olla liiga lihtsasti ära arvatav.

Kui süsteemiseadistused võimaldavad, tuleks määrata sätteid, 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 ettevõtetes 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.

5.2 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 kommertsteenuse (Office 365, Gmail, Dropbox vms) võimaldab, siis tuleks sisse lülitada mitmikautentimine. See tähendab, et peale parooli nõutakse veel mingit autentimismeetodit, näiteks koodi sisestamist, telefonis kinnitamist, ID-kaarti kasutamist, krüptotokenit või mõne riistvaralise lahenduse nagu YubiKey kasutamist.

Kui mitmikautentimine on rakendatud, siis ei saa ründajad süsteemile ligi isegi parooli lekkimisel, sest neil puudub teine autentimiseks vajalik komponent.

5.3 Lihtsusta paroolide kasutamist

Kuna suurem osa süsteeme nõuab paroolide kasutamist, võib töötajal olla palju erinevaid kasutajanimed 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.

6 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.

6.1 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 -teenusepakkujad.

Kui mõni saadud e-kiri tundub kahtlane, siis tasub alati pöörduda oma IT-personali või -teenusepakkujate 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 aadressaadressil 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. 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).

6.2 Koolita töötajaid

Lisaks ettevõtte üldisele küberturbe taseme tõstmisele, tuleks korraldada töötajatele küberturvalisuse alase teadlikkuse suurendamise 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. Üks võimalus töötajate koolitamiseks on liituda RIA poolt pakutava Kübertestiga. Kübertest on e-õppe koolituskeskkond, mille eesmärgiks on tõsta ja hoida asutuse või ettevõtte töötajate küberturbeteadlikkust. Uuendame Kübertesti sisu igal aastal. Rohkem infot Kübertesti kohta leiad RIA [kodulehelt](#).²

6.3 Kontrolli regulaarselt töötajate teadmisi

Selleks et kontrollida, kas töötajate üldine juhendamine ja koolitamine on tulemust andnud, tuleb nende teadmisi regulaarselt kontrollida. See aitab õpitud 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 ettevõtte 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. Töötajate teadmisi on võimalik kontrollida ka punktis 6.2 „Koolita töötajaid“ välja toodud Kübertesti abil.

7 Valmistu intsidendiks ja 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, seadmete vargust või õnnetusi (tulekahju, üleujutus), mis hävitavad või rikuvad andmed. Seetõttu on oluline, et ettevõttel oleks paigas plaan, mida intsidendi korral teha ning kõik ettevõttele tähtsad andmed on varundatud ja varukoopiad talletatakse turvalises asukohas.

7.1 Tea, kuidas toimida intsidendi korral

Teavita küberintsidendi toimumisest RIA intsidentide käsitlemise osakonda CERT-EE (cert@cert.ee). Täiendavaks konsultatsiooniks ja intsidendi analüüsiks on vaja, et

² <https://www.ria.ee/kuberturvalisus/kuberruumi-analuu-ja-ennetus/kubertest>

organisatsioon on valmis intsidendi detaile jagama ning et organisatsioonil on kontaktisik, kes on volitatud CERT-EEga suhtlema.

Intsidendi korral alusta olukorra fikseerimisest:

1. talleta lokaalsed ja logiserveri logid;
2. säilita konfiguratsioon (nt tule müüri reeglid);
3. tee mõjutatud süsteemidest kettatõmmised;
4. talleta vähemalt viimane varukoopia enne intsidenti, võimalusel aga kõik selleks momendiks säilinud intsidendis osalenud süsteemide varukoopiad.

Kui olukord on kindlaks tehtud, tuleks määratleda intsidendi ulatus, muuhulgas kaardistada kõik mõjutatud süsteemid. Kompromiteeritud või kompromiteerimise kahtlusega süsteemid tuleb kiiremas korras isoleerida.

IT-teenuse töö taastamise käigus on oluline vältida asjakohaste tõendusmaterjalide (logide) hävimist süsteemi taastamise käigus. Intsidendi juurpõhjuste analüüsi tulemusena tuleks planeerida ka tegevused, et tulevikus sarnast olukorda vältida.

Küberintsidendi korral on oluline teavitada olukorrast oma kliente või koostööpartnereid, keda intsident mõjutab. Teatud juhtudel, näiteks isikuandmete lekke puhul, on ettevõtetel lausa kohustus teavitada Andmekaitse Inspeksiooni. Samuti tasuks juba intsidendi lahendamise käigus kaaluda, kas intsidendi kohta on vaja koostada raport ka politseile.

7.2 Loo taasteplaan

Ettevõtte toimepidevuse tagamiseks on oluline 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 konkreetsetes süsteemis kõige paremini orienteeruv spetsialist pole kättesaadav. Sel juhul on abiks taasteplaan, mis aitab kõige kriitilisemas olukorras kiiresti ja korrektselt süsteemi taastada.

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

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

Küberintsidendi korral ei pruugi serveris olevad dokumendid olla kättesaadavad, mistõttu on mõistlik hoida taasteplaani ka paberile prindituna varasemalt kokku lepitud kohas.

7.3 Oma ülevaadet sellest, mis süsteemides toimub

Lisaks IT-süsteemide kaitsmisele peab organisatsioonil olema ka hea ülevaade sellest, mis nende süsteemides toimub. See aitab võimalikke ründeid kiiremini märgata ja aru saada, kuidas ründaja sisse pääses.

Selleks tuleb seadistada logimine ja jälgida salvestatud logiandmeid. Oluline on, et logidesse jõuaks kogu vajalik info – näiteks võrguliikluse, turvaseadmete, domeenikontrollerite, serverite

(ka haldustegevuste), tööjaamade ja rakenduste logid. Logisid tuleks säilitada vähemalt 1 aasta, soovitatavalt kuni 3 aastat. See on vajalik selleks, et turvaintsidendi korral oleks võimalik kindlaks teha, millal kahtlane tegevus algas ja milliseid süsteeme see mõjutas – sest ründaja võib olla süsteemides pikalt enne, kui midagi juhtub.

Logid peaks asuma eraldi serveris ning olema varundatud, et need säiliks ka siis, kui süsteem rikutakse. Lisaks tasub paigaldada seirelahendus, mis jälgib süsteemide tööd ja turvaintsidente ning saadab vajadusel automaatseid teavitusi, et probleemidele kiiresti reageerida.

7.4 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. Muuhulgas tuleb varundada ka süsteemide taastamiseks vajalikud andmed, näiteks serverite või võrguseadmete seadistuste failid jm tehniline info.

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. Lisaks tasuks ühte varukoopiat hoida andmekandjal, mis on võrgust eraldatud. 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.

7.5 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 taasteplaani olemas ning kas proovitaastamised on tehtud. Kui vaja, tuleb luua taasteplaani ja korraldada proovitaastamine.

8 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.

8.1 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: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_et.

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. Samuti võivad kaitsmata domeenilt saadetud e-kirjad jääda kinni mõne meiliserveri rämpspostifiltrisse ja saajale mitte kohale jõuda. See võib tuua kaasa nii maine- kui ka rahakahju.

8.2 Kaitse end ohtude eest

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.

8.2.1 Vali tööriistad turvanõrkuste tuvastamiseks

Avalike teenuste rünnakuks kasutatakse tavaliselt ära teenuste (näiteks veebileht või e-posti server) tarkvaras olevaid turvaauke, nõrku turvasätteid, liiga lihtsaid või lekkinud paroole jne. Turvanõrkuste tuvastamiseks on olemas tööriistu, mis teevad seda automaatselt. Sellised tööriistad skaneerivad avalikke teenuseid ja loovad avastatud turvanõrkuste kohta ülevaatlikud aruanded. Peale nende avastamist tuleks IT-personalilt 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.

8.2.2 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 4.2 „Uuenda tarkvara regulaarselt“). Uuendama peab nii teenuse serveri kui ka teenuse enda tarkvara.

Domeeni kaitsmiseks kontrolli, et sinu domeeni halduskontaktide andmed domeeniregistris on korrektsed. CERT-EE seirab .ee domeeniruumi ja saadab kriitiliste turvanõrkustega või kompromiteeritud lehtede omanikele vastavad teavitused. Korrektsed andmed tagavad, et teavitused jõuavad õigeaegselt kohale.

Küsi IT-spetsialistilt

Kui server on teenusepakkuja juures majutuses ja tema hallata, siis tuleb teenusepakkujalt uurida, kas serveri tarkvara uuendatakse korrapäraselt ning millal viimati uuendused tehti.

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

1. Meiliserverite andmevahetuse kaitsmiseks tuleb lülitada sisse SMTP protokoll TLS-tugi, kasutada POP3s ja IMAPS protokolle ning serveri poolel ära keelata krüpteerimata POP3 ja IMAP protokollide tugi. Tähtis on kasutada e-posti serveri teenustel ainult usaldatud sertifikaate, mis on väljastatud õigele serveri täisnimele (FQDN – fully qualified domain name) ja sertifikaati on lubatud kasutada ka e-kirjade kaitsmiseks (Email protection);
2. 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. E-kirja mass-saatjate (näiteks Smaily, MailChimp jm) puhul ei tohiks neid lisada SPF-kirjesse, vaid kasutada hoopis DKIM-i. Vastasel juhul võib juhtuda, et kõik sama teenuse kasutajad saavad teise isiku nimel e-kirju saata;
3. 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.
4. 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 SPF-i ja DKIM-i, et oma poliitikale vastavust kontrollida. DMARC abil on võimalik saada raport selle kohta, kas keegi on üritanud saata kirju mujalt kui lubatud kohtadest.

Häid nõuandeid ja soovitusi e-posti teenuse kaitsmiseks leiab ka RIA [blogist](#).³

8.2.3 Kaitse oma sotsiaalvõrgustiku kontosid

Tihti rünnatakse ettevõtete sotsiaalvõrgustiku kontosid, nagu X, LinkedIn, Facebook, Instagram jne. Ohus on ka ettevõtte juhtkonna ja võtmetöötajate kontod ning neid tuleb samamoodi kaitsta.

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

³ <https://www.ria.ee/blogi/taga-oma-organisatsiooni-e-kirjavahetuse-usaldusvaarsus-ja-turvalisus>

1. Loo ettevõtte sotsiaalmeedia kasutamise eeskiri. Reeglid peaksid muuhulgas sisaldama:
 - milliseid ja mis eesmärgiga sotsiaalmeedia kanaleid (platvormid, kontod ja lehed) organisatsioon kasutab;
 - mis töötaja mis kontole ligi pääseb ja mis õigustes kontosid hallata saab;
 - milline on varuligipääs kontole;
 - kuidas toimub ligipääsude üleandmine tööülesannete muutumise või töötaja lahkumisel;
 - kuidas töötaja sotsiaalvõrgustikes käitub.
2. Kasuta tugevaid parooli ja vaheta salasõnad, kui ettevõttest lahkub töötaja, kes pääseb ettevõtte kontodele ligi.
3. Lülita sisse mitmeastmeline autentimine.
4. Kontrolli regulaarselt olemasolevad sotsiaalmeedia kontosid. Eemalda alati ligipääsud töötajatelt, kes neid ei vaja.
5. Kontrolli üle kontode sätted. Aeg-ajalt võivad platvormid privaatsussätteid uuendada või võib olemasolev seadistus muutuda.
6. Kui kontod ei ole aktiivselt kasutuses, tuleks neid kaitsta ja jälgida sarnaselt aktiivses kasutuses olevate kontodega, et tuvastada võimalik ülevõtmine.
7. Kasutades platvormide haldamiseks mõnda välist teenusepakkujat, tuleb leppida kokku, et konto ja sisu omandiõigus on siiski ettevõttel.

Küsi IT-spetsialistilt

Kui ettevõtte 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.

9 Pööra tähelepanu tarneahelale

Kujutame ette, et sama IT-teenuse tarkvara kasutavad korraga advokaadibüroo, poekett ja ehitusfirma. Selle asemel, et neid eraldi rünnata, võib ründajal olla lihtsam murda sisse tarkvarasse, mida nad kõik kasutavad – ja sealtkaudu saada ligipääs kõigi nende süsteemidele. Seda nimetatakse tarneahelaründeks.

Sellised ründed võivad halvata süsteemide töö, rikkuda andmeid ja lekkida tundlikku infot. Sageli toovad need kaasa nii rahalist kahju kui ka maine kahjustamist.

Kui kasutad mõne teise ettevõtte (ehk kolmanda osapoole) tark- või riistvara, tuleb arvestada, et sellega kaasnevad ka tarneahela turvariskid.

Et riske vähendada, tasub:

1. kontrollida, kas teenusepakkujal on tehtud turvaauditid ja kas need katavad ka sinu ettevõtte jaoks olulised teemad;
2. sõlmida leping, kus on kirjas näiteks logide haldus, võrkude järelevalve, ligipääsuõiguste jagamine ning võrkude eraldamine (segmenteerimine);
3. määrata teenustele ja toodetele konkreetset turvanõudeid ja lisada need lepingusse;

4. leppida kokku, kes on kontaktisikud ja kuidas toimib suhtlus probleemide korral;
5. kokku leppida, mida tehakse teenusekatkestuse või muu turvajuhtumi puhul;
6. küsida regulaarselt teenusepakkuvalt ülevaateid süsteemide seire kohta.

Pea meeles!

Kontrolli, kas lepingus sätestatud küberturbenõuetest peetakse kinni ja tee kindlaks, kuidas teenusepakkuja intsidente, haavatavusi, turvapaikasid ja turvanõudeid käsitleb.

Eraldi tähelepanu tasub pöörata tarneahela turvalisusega seotud riskihaldusele. Näiteks tuleb dokumenteerida teenusepakkujad ja määratleda, millised riskid võivad kaasneda kolmanda osapoole tarkvara või riistvara kasutamisega. Riskide vähendamiseks tasub tutvuda Eesti infoturbestandardi (E-ITS) riskihaldusjuhendiga, aga ka standardi rakendamisega laiemalt.⁴

⁴ <https://eits.ria.ee/>