KINNITATUD
Eesti Advokatuuri juhatuse
18.04.2023. a otsusega

JUHEND ADVOKAADIBÜROO PIDAJALE INFOTURBEALASTE KAITSEMEETMETE RAKENDAMISEKS

Juhend on kehtestatud soovituslikuna advokatuuriseaduse § 12 p 18 alusel.

Sisukord

1. Juhendi eesmärk

Juhend infoturbealaste kaitsemeetmete rakendamiseks (edaspidi juhend) on koostatud eesmärgiga kirjeldada advokaadibüroo (edaspidi büroo) pidajale infoturbealaste parimate praktikate kohaseid kaitsemeetmeid (edaspidi meetmed), mille rakendamine annab eelduslikult minimaalse kaitse töödeldavatele andmetele ja nendega seotud varadele. Juhendi eesmärk ei ole reguleerida spetsiifiliselt isikuandmete töötlemise nõudeid büroos.

Juhend seab büroole soovituslikud miinimumnõuded seadusest ja kutse-eetikast tulenevale hoolsuskohustusele konfidentsiaalsuse ja büroo talitluspidevuse tagamisel.[1]

Juhendi koostamisel on lähtutud CIS (ingl *Center for Internet Security*) Top 20 kriitilistest küberturvalisuse kontrollide meetmetest ehk varasemalt tuntud kui SANS Top 20, mis on prioriseeritud küberturvalisuse parimate praktikate kogum takistamaks tänapäeval teadaolevate ohtude ja rünnakute realiseerimist.

CIS meetmed on mõeldud organisatsioonidele küberturvalisuse taseme parendamiseks. CIS meetmed muudavad küsimuse „Mida peaks tegema meie büroo?“ küsimuseks „Mida me kõik üheskoos peaksime tegema, et tõsta küberturvalisust kõige laiemas mõistes?“.[2] CIS meetmed on rahvusvaheliselt tunnustatud selle eest, et ekspertide poolt koostatud teave ohtude, äriinfotehnoloogia ja kaitsevalikute kohta on lihtsalt ja arusaadavalt kirja pandud andes büroole hea tööriista, kuidas efektiivselt hallata küberturvalisuse programmi. Sellest olenemata vajavad erineva suurusega ja keerukusega bürood veel rohkem abi ja juhendamist, et alustada kaitsemeetmete rakendamisega ning ressursside koondamisega. Seetõttu on arvestatud juhendi koostamisel büroode äri iseloomu ja kolme rakendusrühma metoodika asemel, nagu algupärases CIS20 meetmete kogumis, on meetmed grupeeritud kahte gruppi ning eemaldatud meetmed, mis ei kohaldu. Näiteks meetmed, mis on mõeldud tarkvara arendusega või tootmisega tegelevatele ettevõtetele.

Juhendis toodud meetmete rakendamiseks on arvestatud ka büroo andmete ja varade kaitse erinevat vajadust (kogus, tehnoloogia), töötajate arvuga ja kasutatavate teenuste (pilvteenused vms) iseloomuga.

- **Miinimummeetmed** – rakendatakse, kui büroos on 1-20 töötajat; spetsiaalset IT-töötajat ei ole. Miinimummeetmed on üldjuhul rakendatavad piiratud ekspertteadmistega ja nende eesmärk on takistada üldisi mittesihtotstarbelisi rünnakuid. Miinimummeetmed on rakendatavad väikese või kodukontori puhul saritoodete riist- ja tarkvara kasutamisel.
- **Täiendavad meetmed** – rakendatakse, kui büroos on rohkem kui 20 töötajat, sh töötaja(d), kes vastutab IT-infrastruktuuri haldamise ja kaitsmise eest. Täiendatavate meetmete eeldus on, et miinimummeetmed on rakendatud.

[1] Vt mh AdvS § 45, VÕS §-d 620 ja 625, EKTÄKS § 5 lg 2, EL isikuandmete kaitse üldmäärus, Eesti Advokatuuri eetikakoodeksi § 5, CCBE eetikakoodeksi p 2.3 jm.
[2] “CIS ControlsTM” (Versiooni 7.1) eestindus Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames.

Mõned meetmed sõltuvad büroos kasutatavast tehnoloogiast ja võivad vajada eriteadmisi, et teha õigeid installeerimisi ja konfigureerimisi. Meetmegruppide paremaks eristamiseks on miinimummeetmed juhendi allolevas tekstis tehtud roheliseks ja täiendavad meetmed lillaks. Enamik lillasse gruppi kuuluvaid CIS meetmeid eeldab IT baaspädevuse olemasolu või väljastpoolt bürood hankimist.

Juhend ei ole „üks-lahendus-sobib-kõigile“ mudel. Igal bürool on kohustus ise läbi viia eneseanalüüs ja hinnata, mis on kriitiline ja kohalduv konkreetsele ärile, andmetele, süsteemidele, võrkudele ja infrastruktuurile. Soovitatav on koostada meetmete juurutamise projekt, mille käigus koostatakse tegevuskava eesmärgi saavutamiseks. Eesmärgi püstitamisel tuleb arvesse võtta kõiki võimalusi, mis võivad mõjutada projekti edukust. Isegi väikest arvu meetmeid ei saa juurutada samaaegselt ilma, et oleks plaan olukorra hindamiseks, meetmete rakendamiseks ning kogu juurutusprotsessi juhtimiseks. Et oleks paremini mõistetav, mida meetme juures kirjeldatud tegevus aitab teha, siis on iga meetme juurde märgitud tema turvafunktsioon ning üldjuhul ka seotud vara liik.

Selleks, et bürool oleks võimalik läbi viia eneseanalüüs, on juhendi juurde loodud kasutamiseks nimekiri juhendis toodud infoturbekontrollidest nimega „Kontrollküsimustik“ (lisa nr 1). Büroo, kes soovib kaardistada lähtepunkti miinimummeetmete rakendamisest, peab „Kontrollküsimustiku“ tabelis esmalt valima veerus F „miinimummeetmed“, mille tulemusena filtreeritakse tabelist välja täiendavad meetmed märgistades vastuste veerus vastavad meetmed „ei kohaldu“ märgisega. Juhul, kui büroo soovib läbi viia eneseanalüüsi nii miinimum- kui ka täiendavate meetmete kohta, siis tuleb veerus F valida „täiendavad meetmed“. Sellisel juhul muutuvad kõik meetmed kohustuslikuks kuna täiendavate meetmete eelduseks on miinimummeetmete täielik rakendamine. Täiendavaid meetmeid ilma miinimummeetmeteta valida ei ole võimalik. Küsimustiku kõrvale on lisatud visuaalne kuvand, mis annab ülevaate jah ja ei vastustest ning aitab paremini visualiseerida kui kaugel ollakse eesmärgist soovitud meetmete rakendamisel.

2. Mõisted

AAA (ingl *authentication*, *authorization*, *accounting*) – võrkupääsu protokollide pere.

Auditlogi ehk revisjonlogi – seirevahend; revisjonkirjete kronoloogiline jada, igas kirjes on andmed konkreetse sündmuse kohta.

DNS server – server, millel hoitakse domeeninimeteenuse andmiseks vajalikke nime- ja aadressivastendusi.

Esemevõrk (ka asjade Internet; ingl *Internet of Things*) – Interneti pealisvõrk nutiseadmete ühendamiseks.

Halduskonto – tavakasutajast erinevate õigustega kasutaja (haldaja, hooldaja või seiraja) konto.

Hosti dünaamilise konfigureerimise protokoll (DHCP) – standardprotokoll, mis võimaldab arvutitel automaatselt saada IP-aadressi ja muid tööks TCP/IP-võrgus vajalikke parameetreid.

IP-aadress – alaline või ajutine tunnusnumber protokolli IP kasutavasse võrku kuuluva seadme identifitseerimiseks ja adresseerimiseks.

Jääkrisk – risk, mis jääb pärast riskikäsitlust, võib sisaldada tuvastamata riski.

Infoturbe kontrollid – kaitsemeetmed või vastumeetmed füüsilise vara, teabe arvutisüsteemide või muude varade turvariskide vältimiseks, tuvastamiseks, tõrjumiseks või minimeerimiseks.

Käsurida – tekstliides, milles käske sisestatakse klaviatuurilt.

Liivakast (ingl *sandbox*) – keskkond kahtlastest allikatest pärit koodi või programmi käituseks, tõkestab võimalikke ohtlikke toiminguid ja funktsioone.

Läbipaistev kast (ka valge kast; ingl *white box*) – süsteem või komponent, mille sisemus või teostus on teada.

Läbipaistmatu kast (ka must kast; ingl *black box*) – käsitlusobjekt, mille sisestruktuur pole teada ja mida uuritakse empiiriliste mudelitega.

Meiliklient (ingl *mail client*) – meiliprogramm või programmiroll, mis võimaldab ühe või mitme kasutaja kirju vastu võtta, talletada, koostada, saata, hallata.

Metaandmed (ingl *metadata*) – andmed andmete või andmeelementide kohta.

Multiautentimine (ingl *multifactor authenticator* ehk *MFA*) - autentimine mitme eri tüüpi identsustõendiga, näiteks kiipkaardi, parooli ja biomeetrikuga.

Paigahaldus (ingl *patch management*) – tegevus tarkvara ajakohasuse säilitamiseks ja riski vähendamiseks.

Pimeveeb (ingl *darkweb*) – Interneti üks pealisvõrke, ühendab veebisaite, mis on avalikult nähtavad, kuid varjavad neid majutatavate serverite IP-aadresse, seega ka majutajaid.

Saritoode ehk valmistoode (ingl *commercial off the shelf*) - valmiskomplektidena turustatav üldistatud litsentsilepingutega saritarkvara ja ärilise toega priivara, vastandina eritellimustootele.

SIEM (ingl *security information and event management*) ehk turvateabe ja -sündmuste haldus – tarkvara ja teenuste valdkond, mis integreerib turvateabe (turvalisust puudutava teabe tsentraliseeritud kogumine, esitus, arhiveerimine, seire ja analüüs) haldust ja turvasündmuste (turvalisust puudutav sündmus) haldust.

Vara omanik – isik, kes vastutab ühe või mitme infovara turbe eest: eraldab nende turvameetmeteks ressursid, kinnitab rakendatavad meetmed, volitab juurdepääsu, seirab meetmete toimivust.

Ühtne ressursilokaator (tuntud ka veebiaadressina; URL) – mehhanism ressursside identifitseerimiseks Internetist.

Võrguaadress – võrgustatud olemi aadress. Sõltuvalt kontekstist, kas IP-aadress, meiliaadress või veebiaadress.

3. Sissejuhatus infoturbesse

Infoturve on teabe konfidentsiaalsuse, tervikluse ja käideldavuse säilitamine, mis võib hõlmata ka muid omadusi, näiteks autentsust, jälitatavust, salgamise vääramist ja usaldatavust. Infoturbe rakendamine tagab, et büroos kaitstakse teavet volitamata kasutajate eest (konfidentsiaalsus), volitamata muutmise eest (terviklus) ning teabele on juurdepääs isikutel, kellel seda põhjendatult vaja on (käideldavus). Infoturvalisus saavutatakse lisaks tehnilistele vahenditele läbi struktureeritud riskijuhtimise, mille raames:

- tuvastatakse teave (sh andmed), seotud varad, volitamata juurdepääsust tingitud ohud, turvanõrkused ja mõju büroole;
- hinnatakse riskid;
- otsustatakse, kuidas riskid maandada või neid käsitleda (s.t riskide vältimine, maandamine, jagamine või aktsepteerimine);
- valitakse ja rakendatakse sobivad turvakontrollid;
- jälgitakse tegevusi ja tehakse vajadusel otsustes, kontrollides või hinnangutes kohendusi.

Ohud on potentsiaalsed turvakahjude algallikad, mis adekvaatsete kaitsemeetmete puudumisel võivad põhjustada turvarikkeid. Toime järgi võib ohud liigitada nelja põhitüüpi:

		Riistvara	**Tarkvara**	**Side**	**Andmed**
1.	Halvang	Teenuse tõkestus	Kustutus	Ummistus	Kaotsiminek
2.	Infopüük	Vargus	Kopeerimine	Pealtkuulamine	Kopeerimine
3.	Modifitseering	Konfiguratsiooni muutmine	Kahjurvara (loogikapomm)	Marsruudi muutmine	Järjestuse muutmine
4.	Võltsing	Kasutamise eitamine	Paroolipüüdeprogramm	Teesklus	Fiktiivsete andmete lisamine

Ohuallikate olemused jaotuvad stiihilisteks (keskkonnaohud, tehnilised rikked ja defektid, inimvead) ja rünnakuteks (lähtub inimesest ja valmis sihilikult kahju tekitama).

Selleks, et mõista kogu büroo riskiskaalat arvestades äri toimimist, eesmärke ja kõiki ressursse, peaks läbi viima tervikliku küberturbetaseme hindamise analüüsi koos infoturbealaste riskide hindamisega. Kasutades riskianalüüsi metoodikaid nagu näiteks CIS RAM, NIST Risk Management Framework või ISO27005 saavad bürood teha paremaid ja rohkem läbimõeldud otsuseid selle osas, kas oleks tarvis rakendada juhendis toodud miinimummeetmeid või täiendavaid meetmeid ning mil määral.

4. Meetmed

4.1. Andmete kaitse

Et teada, milliseid andmeid ja milliste turvameetmetega kaitsta, peab büroo andmed klassifitseerima. Andmete klassifitseerimine on üks peamisi viise, kuidas andmetele anda suhteline väärtus. Klassifitseerimise protsessi käigus liigitatakse andmed olulisuse ja äritegevuse mõju järgi, et teha kindlaks andmetega seotud riskid. Andmete liigitus on sisendiks teistele dokumendis toodud meetmete rakendamisele. Andmete kaitsemeetmete raames loodud protseduurid ja tehnilised kontrollid aitavad andmeid tuvastada, klassifitseerida, turvaliselt käidelda, säilitada ja kasutuselt kõrvaldada.

Tegevus	Turvafunktsioon
4.1.1. Miinimummeetmed:	
4.1.1.1. Looge andmehaldusprotseduur, kus on määratletud töödeldavate andmete liigid (nt isikuandmed, tehnilised andmed jne), andmete omanikud, käitlemine, säilitamisnõuded ja kõrvaldamisnõuded, mis tuginevad õigusaktidele või büroo sisemisele regulatsioonile. Protseduur tuleb üle vaadata ja ajakohastada vähemalt kord aastas või siis, kui toimuvad olulised muudatused, mis võivad protsessi mõjutada.	Tuvastamine (andmed)
4.1.1.2. Klassifitseerige andmed. Klassifitseerimiseks võib kasutada liike nagu näiteks „Avalik“, „Büroosisene“ või „Konfidentsiaalne“. Klassifikatsioon tuleb üle vaadata ja vajadusel ajakohastada vähemalt kord aastas või kui toimuvad olulised muudatused, mis võivad klassifitseerimist mõjutada.	Tuvastamine (andmed)
4.1.1.3. Kaardistage andmete liikumine (andmevood). Vaadake dokumentatsioon üle ja ajakohastage vajadusel või siis, kui toimuvad olulised muudatused, mis võivad dokumentatsiooni mõjutada.	Tuvastamine (andmed)
4.1.1.4. Krüpteerige eemaldatavatel andmekandjatel säilitatavad andmed vastavalt andmete klassifikatsioonile.	Kaitsmine (andmed)
4.1.1.5. Koostage andmetele juurdepääsu kontroll-loend andmebaaside, rakenduste ja infosüsteemide lõikes. Jälgige, et loendi andmed ja tegelikkus on vastavuses.	Kaitsmine (andmed)
4.1.1.6. Säilitage andmeid vastavalt andmehaldusprotseduurile.	Kaitsmine (andmed)
4.1.1.7. Hävitage/kustutage andmed, millel on kätte jõudnud säilitamise lõpp-kuupäev.	Kaitsmine (andmed)
4.1.1.8. Krüpteerige andmed büroo lõppkasutaja seadmetes, mis sisaldavad konfidentsiaalset infot. Näidisvahendid: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Kaitsmine (andmed)
4.1.1.9. Segmenteerige andmete töötlemine ja säilitamine vastavalt andmete liigile ja klassifikatsioonile.	Kaitsmine (võrk)
4.1.1.10. Krüpteerige emailiga, failivahetusrakendustega või muul viisil vahetatavad konfidentsiaalsed failid. Näiteks DigiDoc rakendus failide krüpteerimiseks.	Kaitsmine (võrk)
4.1.2. Täiendavad meetmed:	
4.1.2.1. Krüpteerige konfidentsiaalsed andmed edastamiseks. Näidisrakendused: transpordikihi turvalisus (ingl *transport layer security* ehk *TLS*), PKI (ingl *public key infrastructure*) emailide krüpteerimiseks.	Kaitsmine (andmed)

4.1.2.2. Serverites, rakendustes ja andmebaasides puhkeseisundis olevad andmed tuleb krüpteerida. Täiendavad krüpteerimismeetodid võivad hõlmata nt rakenduskihi krüpteerimist, kus juurdepääs andmesalvestusseadme(te)s olevatele andmetele ei võimalda juurdepääsu lihttekstis andmetele.	Kaitsmine (andmed)
4.1.2.3. Juurutage automatiseeritud tööriist [nt lekketõrje (ingl *data loss prevention* ehk *DLP*)], et tuvastada kõik varade kaudu salvestatud, töödeldud või edastatud büroo jaoks olulised või konfidentsiaalsed andmed, sh need, mis asuvad kohapeal või kaugteenuse pakkuja juures.	Kaitsmine (andmed)
4.1.2.4. Logige ligipääse konfidentsiaalsetele andmetele (alustades näiteks kasutajate ligipääsude logimisest ja tulevikus liikudes edasi logide keskhaldussüsteemi rakendamiseni), sh muutmist ja hävitamist.	Avastamine (andmed)

4.2. Varade haldamine

Vara saab kasutada digitaalteabe hankimiseks, töötluseks, talletamiseks, jaotamiseks ja sellel on büroo jaoks potentsiaalne või tegelik väärtus. Varade hulka kuuluvad: tarkvara, infokandjad (füüsilised ja digitaalsed), IT-seadmed (füüsilised ja virtuaalsed), litsentsid (ja litsentsitõendid), lepingud ja IT-varade halduse varad (süsteemid, vahendid, metaandmed). Varadeks võib lugeda ka teenused, mis on vajalikud varade halduse nõuete täitmiseks (nt tarkvara teenusena, riistvara hooldus, tarkvara tugi, koolitus). Varade haldamine on vajalik eelkõige seetõttu, et:

- Haldamata varad võivad muutuda turvanõrkusteks – omamata ülevaadet, millised riist- või tarkvarad on büroos kasutusel, võib tähendada seda, et võrgus võib olla nõrk koht, mida saab küberkurjategija ära kasutada.
- Aegunud vara võib negatiivselt mõjutada töövoogusid – teadmatus sellest, millised varad on töötajatele kättesaadavad, võib mõjuda nende tööle negatiivselt. Vananenud seadmed võrgus võivad näiteks põhjustada oluliste ärirakenduste töö aeglustumist.
- Andmete käideldavuse tagamiseks – võrgu infrastruktuuri kaart on oluline, et töötajad saaksid vajalikud ressursid siis kui neil on neid vaja.
- IT-varahaldus võib olla õigusnormidele vastavuse seisukohast ülioluline – nt EL isikuandmete kaitse üldmäärusest (lühendatult IKÜM või ingl *GDPR*) tuleneva andmesubjekti nõude „olla unustatud“ täitmine on võimatu, kui ei olda teadlik, kus ja milliseid andmeid hoitakse.
- Lisanduvaid varasid tuleb jälgida ja nendega arvestada võrgu struktuuris – kui seda ei tehta, siis võib see põhjustada võrguarhitektuuri ebatäpsusi, vajalike komponentide otsimise ajakulu suurenemist ja lünki küberturvalisuse tagamisel.
- Kasutusest väljaminevad varad vajavad nõuetekohast kõrvaldamist – tuleb luua reeglid, kuidas tagada, et andmed ei satuks kolmandate osapoolte kätte.

Riistvarade haldus aitab volitamata ja haldamata riistvarade tuvastamist. Tarkvara haldusandmete alusel saab tagada, et büroos installitakse ja saab käivitada ainult lubatud tarkvara ning et leitakse volitamata, litsentseerimata ja haldamata tarkvara, mille installimist ja kasutamist saab takistada. Riist- ja tarkvara turvaline konfiguratsioon on ülioluline küberturvalisuse, nõuetele vastavuse ja talitluspidevuse seisukohast, sest isegi ainult üks konfiguratsiooniviga võib põhjustada turvaintsidente ja teenushäireid.

Tegevus	Turvafunktsioon
4.2.1. Miinimummeetmed:	
4.2.1.1. Koostage ja hoidke ajakohasena ülevaadet (register) kõigist büroo varadest, millega töödeldakse (sh salvestatakse) teenuse osutamiseks andmeid, sh: lõppkasutaja seadmed (sh kaasaskantavad ja mobiilsed), võrguseadmed, mitteandmetöötlus-/esemevõrgu seadmed, pilveteenused ja serverid (sh virtuaalserverid). Registris peab olema: • seadme võrguaadress (kui see on staatiline ja tegemist ei ole avaliku pilveteenusega), • seadme tüüp, mark ja mudel, • vara omanik, • vara kasutav üksus (kui on), • märge, kas vara on võrguga ühenduse loomiseks heaks kiidetud. Mobiilsete seadmete puhul võivad MDM-tüüpi (ingl *mobile device management*) tööriistad seda protsessi vajaduse korral toetada. Vaadake üle ja värskendage registrit vähemalt kord aastas või sagedamini.	Tuvastamine (seadmed)
4.2.1.2. Tagage, et volitamata varade avastamiseks ja nendega tegelemiseks on olemas toimivad protseduurid. Büroo võib otsustada vara võrgust eemaldada, keelata vara kaugühenduse võrguga või panna vara karantiini.	Reageerimine (seadmed)
4.2.1.3. Koostage ja hoidke ajakohane register andmetega kõikidest lubatud tarkvaradest, mida mis tahes ärisüsteemide jaoks vaja on. Registris peab olema dokumenteeritud vähemalt: • tarkvara nimi, • kasutusel olev versioon, • väljaandja, • esmase installimise/kasutamise kuupäev ja • kasutuseesmärk. Võimalusel tuleb lisada rakenduse allalaadimise allikas – URL või rakenduse e-pood, publikatsiooni ja kasutuselt kõrvaldamise kuupäev. Ajakohastage registrit vähemalt kord aastas või sagedamini.	Tuvastamine (rakendused)
4.2.1.4. Veenduge, et lubatud tarkvara registrisse on kantud rakendused ja operatsioonisüsteemid, mis on tootja poolt toetatud ja saavad uuendusi. Toetamata tarkvara, mis on siiski vajalik büroo teenuse osutamiseks, tuleb dokumenteerida erandina, mille juures tuleb kirjeldada üksikasjalikult tarkvara kasutamisega kaasnevate riskide leevendavaid infoturbe kontrolle ja jääkriski aktsepteerimist. Vaadake register üle vähemalt kord kuus, kui juhtkonnas ei ole otsustatud teisiti, et tagada ajakohane info tarkvara toe olemasolu kohta.	Tuvastamine (rakendused)
4.2.1.5. Tagage, et volitamata tarkvara eemaldatakse kasutuselt või et on dokumenteeritud erand.	Reageerimine (rakendused)
4.2.1.6. Looge protseduur võrguseadmete, riist- ja tarkvara turvaliseks konfigureerimiseks. Vaadake dokumentatsioon üle ja ajakohastage seda igal aastal või siis, kui toimuvad olulised muudatused, mis võivad seda protseduuri mõjutada.	Kaitsmine (rakendused)
4.2.1.7. Võtke kasutusele automaatne ekraani lukustamine, s.t ekraan lukustub määratletud tegevusetuse perioodi ületamisel. Teenuse või serveri sessioon on	Kaitsmine (kasutajad)

soovitatav katkestada maksimaalselt 15 minuti pärast. Lõppkasutaja seadmete puhul on soovitatav mitte ületada 2 minutit.	
4.2.1.8. Rakendage ja hoidke ajakohasena tulemüür serverites, kus tulemüüri kasutamist toetatakse. Näidisrakendused: virtuaalne tulemüür, operatsioonisüsteemi tulemüür või kolmanda osapoole tulemüür.	Kaitsmine (seadmed)
4.2.1.9. Rakendage ja hoidke ajakohasena lõppkasutaja seadmetes hostipõhist tulemüüri või portide filtreerimise tööriista vaikimisi keelatud reegliga, mis katkestab kogu liikluse, välja arvatud need teenused ja pordid, mis on lubatud.	Kaitsmine (seadmed)
4.2.1.10. Hallake riist- ja tarkvara turvaliselt. Selleks võib kasutada rakendusi, mis võimaldavad näiteks konfiguratsiooni haldamist läbi versioneeritud infrastruktuuri halduse ja juurdepääsu haldusliidestele turvaliste võrguprotokollide kaudu, nagu Secure Shell (SSH) ja Hypertext Transfer Protocol Secure (HTTPS). Ärge kasutage ebaturvalisi haldusprotokolle, nagu Telnet (Teletype Network) ja HTTP, välja arvatud juhul, kui see on operatiivselt hädavajalik.	Kaitsmine (võrk)
4.2.1.11. Hallake riist- ja tarkvara vaikekontosid (nt juur-, administraatori- ja muud eelkonfigureeritud hankijakontod). Näidisrakendused võivad võimaldada vaikekontode keelamist või nende kasutuskõlbmatuks muutmist.	Kaitsmine (kasutajad)
4.2.2.Täiendavad meetmed:	
4.2.2.1. Kasutage büroo võrguga ühendatud riistvarade tuvastamiseks aktiivset kaardistustööriista. Konfigureerige tööriist nii, et seda saaks käivitada iga päev või sagedamini (näiteks võtta kasutusele CMDB server – ingl *configuration management database*).	Jälgimine (seadmed)
4.2.2.2. Kasutage hosti dünaamilise konfigureerimise protokolli (DHCP) logimist kõigis DHCP-serverites või IP-aadresside haldustööriistu, et uuendada riistvara registri andmeid.	Tuvastamine (seadmed)
4.2.2.3. Kasutage passiivset kaardistustööriista, et tuvastada büroo võrku ühendatud seadmeid ja automaatselt uuendada riistvararegistrit (nt IDS – *Intrusion Detection System*).	Tuvastamine (seadmed)
4.2.2.4. Kasutage võimaluse korral spetsiaalseid tööriistu tarkvara inventeerimiseks, et automatiseerida installitud tarkvara avastamist ja dokumenteerimist.	Tuvastamine (rakendused)
4.2.2.5. Kasutage tehnilisi kontrolle (nt lubatud rakenduste nimekiri), et tagada ainult volitatud tarkvara käivitumine. Vaadake kontrollid üle vähemalt kaks korda aastas.	Kaitsmine (rakendused)
4.2.2.6. Kasutage tehnilisi kontrolle tagamaks, et ainult volitatud tarkvara teegid (nt .dll, .ocx, .so jne) on lubatud laadida süsteemiprotsessi. Blokeerige volitamata teekide laadimine süsteemiprotsessi. Vaadake kontrollid üle vähemalt kaks korda aastas.	Kaitsmine (rakendused)
4.2.2.7. Kasutage tehnilisi kontrolle (nt digitaalallkirjad ja versioonikontroll), et tagada ainult lubatud skriptide (nt .ps1, .py jne) käivitus. Blokeerige volitamata skriptide käivitamine. Vaadake kontrollid üle vähemalt kaks korda aastas.	Kaitsmine (rakendused)
4.2.2.8. Desinstallige või keelake riist- ja tarkvaras mittevajalikud teenused (nt kasutamata failijagamisteenus, veebirakenduse moodul või teenusefunktsioon).	Kaitsmine (seadmed)
4.2.2.9. Konfigureerige ainult usaldusväärsed DNS-serverid. Näidisrakendused võimaldavad varasid konfigureerida nii, et nad kasutaks büroo kontrolli all olevaid DNS-servereid ja/või väliselt juurdepääsetavaid usaldusväärseid DNS-servereid.	Kaitsmine (seadmed)
4.2.2.10. Rakendage seadme automaatne lukustamine eelnevalt kindlaks määratud nurjunud autentimiskatsete arvu alusel lõppkasutaja seadmetes. Arvutite puhul ärge lubage rohkem kui 20 ebaõnnestunud autentimiskatset; tahvelarvutite ja	Reageerimine (seadmed)

nutitelefonide puhul mitte rohkem kui 10 ebaõnnestunud autentimiskatset. Näidisrakendused: Microsoft® InTune Device Lock ja Apple Configuration® Profile maxFailedAttempts.	
4.2.2.11. Rakendage büroo andmete põhjendatud (nt seade kadunud või varastatud) kaugkustutamist büroole kuuluvatest lõppkasutaja mobiilsetest seadmetest.	Kaitsmine (seadmed)
4.2.2.12. Veenduge, et lõppkasutaja mobiilsetes seadmetes, on töö- ja eraasjad eraldatud. Näidisrakendused: Apple'i® konfiguratsiooniprofiil või Androidi™ tööprofiil.	Kaitsmine (seadmed)

4.3. Juurdepääsude haldamine

Juurdepääsude haldus (sh kontohaldus) on protsess, mille käigus kontrollitakse ja jälgitakse, kellel on juurdepääs büroos olevale teabele ja ressurssidele. Juurdepääsude haldus on ülioluline turvainfrastruktuuri osa, sest aitab vältida volitamata juurdepääsu konfidentsiaalsetele või muudele vastavalt klassifitseeritud andmetele. Kasutajate mandaadid, kellel on juurdepääs süsteemile ja andmetele, on sageli andmepüügirünnakute sihtmärgid ning samuti võib büroos olla oma volitusi kurjasti ära kasutav töötaja. Identiteedi- ja juurdepääsuhalduse tööriistad aitavad kahtlasi tegevusi kiiresti tuvastada, olenemata sellest, kas need on toime pannud välised või sisemised kurjategijad.

Tegevus	Turvafunktsioon
4.3.1. Miinimummeetmed:	
4.3.1.1. Looge protseduur, eelistatavalt automatiseeritud, kuidas taotleda, anda ja muuta juurdepääsuõiguseid.	Kaitsmine (kasutajad)
4.3.1.2. Looge protseduur, eelistatavalt automatiseeritud, juurdepääsu tühistamiseks, lülitades välja kontode õigused lepingulise suhte lõppemisel, õiguste tühistamisel või kasutaja rolli muutumisel. Kontrolljälgede säilitamiseks ei tohiks kontosid koheselt kustutada.	Kaitsmine (kasutajad)
4.3.1.3. Koostööpartneritelt tuleb võimalusel nõuda MFA kasutamist. MFA jõustamine kataloogiteenuse või SSO pakkuja kaudu on selle kaitsemeetme rahuldav rakendamine.	Kaitsmine (kasutajad)
4.3.1.4. Nõudke MFA kasutamist kõigil juurdepääsudel kontodele või rakendustele ja kus võimalik kasutage SSO teenust.	Kaitsmine (kasutajad)
4.3.1.5. Kui võimalik, siis tuleb nõuda MFA kasutamist kõigi halduskontode puhul, olenemata sellest, kas neid hallatakse kohapeal või teenuseosutaja kaudu.	Kaitsmine (kasutajad)
4.3.1.6. Looge kõigi büroos hallatavate kontode (sh kasutajakontod, administraatorikontod, teeninduskontod) kohta register. Register peab sisaldama vähemalt isiku nime, kasutajanime, konto avamiskuupäeva, konto sulgemiskuupäeva ja üksust (kui on). Kontrollige, et kõik aktiivsed kontod on autoriseeritud, vähemalt kord kvartalis või sagedamini.	Tuvastamine (kasutajad)
4.3.1.7. Kasutage kõigi büroo varade jaoks kordumatuid paroole. Parimate tavade rakendamine hõlmab vähemalt 8-kohalist parooli kontodele, mis kasutavad MFA-d, ja 14-kohalist parooli kontodele, mis ei kasuta MFA-d.	Kaitsmine (kasutajad)
4.3.1.8. Kui võimalik, siis sulgege või keelake kõik passiivsed (latentsed) kontod pärast 45-päevast tegevusetuse perioodi.	Reageerimine (kasutajad)
4.3.1.9. Tagage, et kõik administraatoriõigustega kasutajad kasutavad kõrgendatud õigustega tegevusteks eraldi selleks otstarbeks loodud halduskontot. See konto peab	Kaitsmine (kasutajad)

olema ainult administratiivsete tegevuste jaoks ja seda ei tohi kasutada tavakasutaja tegevuste jaoks nagu nt internetis sirvimine või e-posti lugemine.	
4.3.1.10. Töötajad ei tohi kasutada büroo andmete töötlemiseks erameile. Kasutajatele peab looma büroo meilikonto. Kontohalduse tsentraliseerimiseks saab kasutada AD (Active Directory) või identiteeditеenust.	Kaitsmine (kasutajad)
4.3.2. Täiendavad meetmed:	
4.3.2.1. Looge autentimis- ja volitussüsteemide loend. Vaadake info üle ja vajadusel ajakohastage vähemalt kord aastas või sagedamini.	Tuvastamine (kasutajad)
4.3.2.2. Kui võimalik, siis tsentraliseerige juurdepääsukontroll.	Kaitsmine (kasutajad)
4.3.2.3. Rakendage rollipõhine juurdepääsukontroll, määrates ja dokumenteerides pääsuõigused, mis on vajalikud iga rolli jaoks büroos talle määratud ülesannete edukaks täitmiseks. Vaadake info üle, et kontrollida, kas kõik õigused on lubatud, vähemalt kord aastas või sagedamini.	Kaitsmine (kasutajad)
4.3.2.4. Nõudke MFA kasutamist võrgule kaugjuurdepääsuks.	Kaitsmine (kasutajad)

4.4. Logimine ja seire

Logimine on sündmuste andmete reaalajas logisse kandmine. Logi on kronoloogiliste sündmuste andmik, mis talletatakse andmefailide läbivaatuseks ja analüüsiks. Logisid genereerivad mitmed allikad, sh turvatarkvara (nt viirustõrjetarkvara, tulemüürid, sissetungide tuvastamise ja ennetamise süsteemid, serverite operatsioonisüsteemid, tööjaamad, võrguseadmed ja rakendused). Seire on protsesside, tegevuste ja meetmete oleku pidev kontroll, järelevalve ja kriitiline vaatlus oodatavatele tulemustele vastavuse otsusteks, otsustusaluste loomiseks ning andmete kogumiseks võrdluse eesmärgil.

Logihaldus (sh seire) on hädavajalik tagamaks, et turvaandmeid säilitatakse piisavalt üksikasjalikult ja vajaliku ajavahemiku jooksul. Rutiinne logianalüüs on kasulik turvaintsidentide, reeglite rikkumise, pettustegevuste ja seadmete tegevustõrgete tuvastamiseks. Logid on samuti vajalikud auditite ja krimianalüüsi tegemiseks, toetamaks büroosisest uurimist, aidates logikriteeriumite seadistamist, identifitseerides tegevustrende ja kindlaks määrata pikaajalisi probleeme.

Tegevus	Turvafunktsioon
4.4.1. Miinimummeetmed:	
4.4.1.1. Looge auditilogide haldusprotsess, mis kirjeldab logimisnõuded. Tuleb määratleda, milliseid logisid kogutakse, läbi vaadatakse ja säilitatakse. Protsess tuleb üle vaadata ja vajadusel ajakohastada igal aastal või siis, kui toimuvad olulised muudatused, mis võivad seda protsessi mõjutada.	Kaitsmine (võrk)
4.4.1.2. Koguge auditilogisid. Tagage, et logimine toimub vastavalt auditilogi haldusprotsessile.	Avastamine (võrk)
4.4.1.3. Veenduge, et kõigil logisid talletavatel süsteemidel on piisavalt salvestusruumi.	Kaitsmine (võrk)

4.4.2. Täiendavad meetmed:	
4.4.2.1. Standardiseerige aja sünkroonimine. Kus võimalik, siis konfigureerige vähemalt kaks sünkroonitud ajaallikat.	Kaitsmine (võrk)
4.4.2.2. Varades, kus töödeldakse eriliiglisi isikuandmeid või konfidentsiaalseid andmeid, peab olema logitud sündmuse allikas, kuupäev, kasutajanimi, ajatempel, lähteaadressid, sihtkoha aadressid ja muud andmed, mis võivad auditeerimisel abiks olla.	Avastamine (võrk)
4.4.2.3. Kui võimalik ja asjakohane, siis koguge DNS päringu auditilogisid.	Avastamine (võrk)
4.4.2.4. Kui võimalik ja asjakohane, siis koguge URL-i taotluse auditilogisid.	Avastamine (võrk)
4.4.2.5. Koguge käsurea auditilogisid. Näidisrakendused hõlmavad auditilogide kogumist PowerShellist®, BASH-ist™ ja kaughaldusterminalidest.	Avastamine (võrk)
4.4.2.6. Nii palju kui võimalik, tsentraliseerige auditilogide kogumine ja säilitamine.	Avastamine (võrk)
4.4.2.7. Säilitage auditilogisid vähemalt 90 päeva.	Kaitsmine (võrk)
4.4.2.8. Viige läbi auditilogide ülevaatus, et tuvastada kõrvalekaldeid või ebatavalisi sündmusi, mis võivad viidata võimalikule ohule. Tehke ülevaatusi iganädalaselt või sagedamini.	Avastamine (võrk)
4.4.2.9. Kui võimalik, siis koguge teenusepakkuja logisid. Näidisrakendused hõlmavad autentimis- ja volitustegevuste kogumist, andmete loomise ja kustutamise tegevusi ning kasutajahalduse tegevusi.	Avastamine (võrk)
4.4.2.10. Tsentraliseerige turbesündmuste hoiatus büroo varade vahel logi korrelatsiooni ja analüüsi jaoks. Parimate tavade rakendamine nõuab SIEM-i kasutamist, mis sisaldab määratletud sündmuste korrelatsioonihoiatusi. Sellele kaitsemeetmele vastab ka logianalüüsi platvorm, mis on konfigureeritud turvalisusega seotud korrelatsioonihoiatustega.	Avastamine (võrk)
4.4.2.11. Juurutage hostipõhine sissetungi tuvastuslahendus, kui see on asjakohane ja/või toetatud.	Avastamine (seadmed)
4.4.2.12. Juurutage vajaduse korral büroo varadele võrgu sissetungimise tuvastamise lahendus. Näidisrakendused hõlmavad võrgu sissetungimise tuvastamise süsteemi (IDS) või samaväärse pilveteenuse pakkuja (CSP) teenuse kasutamist.	Avastamine (võrk)
4.4.2.13. Vajaduse korral filtreerige liiklust võrgusegmentide vahel.	Kaitsmine (võrk)
4.4.2.14. Hallake büroo ressurssidega kaugühenduses olevate varade juurdepääsukontrolli. Büroo ressurssidele juurdepääsu summa kindlaksmääramine põhineb installitud ajakohasel kahjuritõrje tarkvaral, konfiguratsiooni vastavusel büroo turvalisele konfiguratsiooniprotsessile ning operatsioonisüsteemi ja rakenduste ajakohasuse tagamisel.	Kaitsmine (seadmed)
4.4.2.15. Koguge võrgu liiklusvoo logisid või võrguliikluse andmeid, et vaadata üle hoiatusi võrguseadmetest.	Avastamine (võrk)
4.4.2.16. Juurutage hostipõhine sissetungimise ennetamise lahendus varades, kui see on asjakohane ja/või toetatud. Näidisrakendused hõlmavad lõpp-punkti tuvastamise ja reageerimise (EDR) kliendi või hostipõhise IPS-agendi kasutamist.	Kaitsmine (seadmed)

4.4.2.17. Juurutage, kus võimalik, võrgu sissetungimise ennetamise lahendus. Näidisrakendused hõlmavad võrgu sissetungimise vältimise süsteemi (IPS) või samaväärse CSP-teenuse kasutamist.	Kaitsmine (võrk)
4.4.2.18. Juurutage porditasemel juurdepääsukontroll. Pordi tasemel juurdepääsukontroll kasutab 802.1x või sarnaseid võrgule juurdepääsu kontrollprotokolle, näiteks sertifikaate, ning võib sisaldada kasutaja ja/või seadme autentimist.	Kaitsmine (seadmed)
4.4.2.19. Tehke rakenduskihi filtreerimist. Näidisrakendused hõlmavad filtreerimispuhvrit, rakenduse kihi tulemüüri või lüüsi.	Kaitsmine (võrk)
4.4.2.20. Häälestage turbesündmuste hoiatuslävesid kord kuus või sagedamini.	Avastamine (võrk)

4.5. Turvanõrkuste haldus

Turvanõrkuste haldus on protsess süsteemi või IT nõrkuste ärakasutamise ennetavaks vältimiseks või nõrgendamiseks, mis tehakse koos riskihaldusega ja hõlmab nõrkuste tuvastamist, liigitamist, hindamist, kõrvaldamist ja leevendamist. Haldus annab büroole:

- Täiendava turvalisuse - rakenduste turvavead pakuvad küberkurjategijatele võimaluse siseneda arvutivõrku. Kogu vara ja äriandmete kaitsmiseks on ülioluline need nõrkused tuvastada. Turvanõrkused hinnatakse ja prioriseeritakse vastavalt raskusastmele. Hinnang aitab parandada IT-varade vigu ja kaitsta neid küberrünnakute eest.
- Kiire turvanõrkuste kõrvaldamise – rakenduste ja operatsioonisüsteemide õigeaegne turvapaikamine ning võrgu turvaseadete ümberkonfigureerimine.
- Tegevuste tõhususe – turvanõrkuste hindamise nimekiri aitab ekspertidel kõigepealt lahendada kõige kriitilisemad probleemid ja hiljem väiksemad.
- Nähtavuse ja aruandluse – selle tulemusena saab teha paremaid turvaotsuseid, tagamaks andmetele turvalisema keskkonna.

Tegevus	Turvafunktsioon
4.5.1. Miinimummeetmed:	
4.5.1.1. Looge dokumenteeritud turvanõrkuste haldamise protsess. Vaadake dokumentatsioon üle ja ajakohastage seda igal aastal või siis, kui toimuvad olulised muudatused, mis võivad seda protsessi mõjutada.	Kaitsmine (rakendused)
4.5.1.2. Looge riskipõhine parandusprotsess, mis on dokumenteeritud igakuiste või sagedasemate kokkuvõtetega.	Reageerimine (rakendused)
4.5.1.3. Tehke rakenduste ja operatsioonisüsteemi värskendusi automaatse paigahalduse kaudu igakuiselt või sagedamini.	Kaitsmine (rakendused)
4.5.2. Täiendavad meetmed:	
4.5.2.1. Tehke automaatseid turvanõrkuste kontrolle büroo sisemistele teenustele kui ka büroovälised avatud varadele kord kvartalis või sagedamini. Viige läbi nii autenditud kui ka autentimata skaneerimine.	Avastamine (rakendused)
4.5.2.2. Parandage tarkvaras tuvastatud turvaauke igakuiselt või sagedamini, tuginedes parandusprotsessile.	Reageerimine (rakendused)

4.6. E-posti ja veebibrauseri turvalisus

E-postile ja veebile juurdepääs on kriitilise tähtsusega äritegevuse jaoks ja seetõttu peetakse seda üheks suurimaks ohupinnaks ning oluliseks rünnakute ja intsidentide allikaks. Meiliserverite, veebibrauserite või meiliklientide nõuetekohane kaitsmine võib drastiliselt vähendada turvaintsidente büroos ja parandab andmete turvalisust. E-posti ja veebibrauseriga seotud kaitsemeetmed aitavad vähendada rünnakukohti ja võimalusi, et ründajad ei saaks inimkäitumisega manipuleerida, kui kasutaja kasutab veebilehitsejat ja e-posti.

Tegevus	Turvafunktsioon
4.6.1. Miinimummeetmed:	
4.6.1.1. Tagage, et büroos on lubatud käivitada ainult tootjate toetatud veebilehitsejaid ja meilikliente, võimaluse korral kasutage ainult viimaseid tootjate pakutavaid versioone.	Kaitsmine (rakendused)
4.6.1.2. Kasutage domeeninimede süsteemi (DNS) filtreerimisteenuseid, et blokeerida ligipääs teadaolevalt pahatahtlikele domeenidele.	Kaitsmine (võrk)
4.6.2. Täiendavad meetmed:	
4.6.2.1. Rakendage võrgupõhised URL-i filtrid, mis ei luba külastada veebilehti, mida büroo pole heaks kiitnud. Näidisrakendused hõlmavad kategooriapõhist filtreerimist, mainepõhist filtreerimist või plokkloendite kasutamist. Filtreerimist tuleb rakendada büroo kõikides varades.	Kaitsmine (rakendused)
4.6.2.2. Desinstallige või keelake veebilehitsejas ja meilikliendis volitamata pistikprogrammid, laiendused ja lisarakendused.	Kaitsmine (rakendused)
4.6.2.3. Et vähendada võltsitud ja muudetud e-kirjade tõenäosust ehtsatelt domeenidelt, rakendage DMARC-i põhimõtted ja kontroll, alustades SPF- ja DKIM-standardite rakendamisest.	Kaitsmine (võrk)
4.6.2.4. Blokeerige kõik e-posti manused, kui failitüüp pole vajalik büroo äritegevuse jaoks.	Kaitsmine (võrk)
4.6.2.5. Juurutage ja hoidke ajakohasena meiliserveri pahavaravastaseid kaitseid (nt manuste skaneerimine ja/või liivakast).	Kaitsmine (võrk)

4.7. Kaitse pahavara eest

Pahavara on vahend (programm, koodilõik, skript, makro vms) infosüsteemi töö või kasutaja otseseks või kaudseks kahjustamiseks või häirimiseks, mis püüab koguda olulist teavet, saada lubamatut juurdepääsu või rünnata andmete konfidentsiaalsust, terviklust või käideldavust. Kaitsemeetmete rakendamine aitab takistada või kontrollida pahatahtliku rakenduse, koodi või skriptide paigaldamist, levimist ja käivitamist büroo varades.

Tegevus	Turvafunktsioon
4.7.1. Miinimummeetmed:	
4.7.1.1. Juurutage ja hoidke ajakohane pahavaravastane tarkvara kõigis büroo varades.	Kaitsmine (seadmed)
4.7.1.2. Konfigureerige pahavaravastaste signatuurfailide automaatsed värskendused kõigis büroo varades.	Kaitsmine (seadmed)

4.7.1.3. Keelake eemaldatavate andmekandjate automaatkäivitus.	Kaitsmine (seadmed)
4.7.1.4. Seadistage seadmed nii, et välise andmekandja sisestamisel või ühendamisel toimuks automaatselt pahavaratõrje skaneering.	Avastamine (seadmed)
4.7.1.5. Võimaluse korral lülitage sisse ründekoodi käivitamist takistavad funktsioonid, nagu Microsofti® andmekäitus tõrje (DEP), Windows® Defender Exploit Guard (WDEG) või Apple'i® süsteemi terviklikkuse kaitse (SIP) ja Gatekeeper™.	Kaitsmine (seadmed)
4.7.2. Täiendavad meetmed:	
4.7.2.1. Kasutage tsentraalselt hallatavat pahavaravastast tarkvara.	Kaitsmine (seadmed)
4.7.2.2. Kasutage käitumispõhist pahavaravastast tarkvara.	Avastamine (seadmed)

4.8. Talitluspidevus

Talitluspidevus on eelnev planeerimine ja ettevalmistus, tagamaks büroo võime jätkata äritegevust, tegevust, protsessi vms. Andmete taastamine aitab taastada büroo varad intsidendieelsesse ja usaldusväärsesse olekusse, milles süsteem, programm, andmebaas või muu süsteemiressurss saab täita nõutavaid ülesandeid. Arvutivõrgu infrastruktuuri haldus aitab luua parema stabiilsuse büroo tegevuses ja tehnoloogias, sh takistada ründajatel haavatavate võrguteenuste ja pääsupunktide ärakasutamist tegevuste halvamiseks. Turvatestimised aitavad kontrollida büroo varade tõhusust ja vastupidavust, tuvastades ja kasutades ära kontrollide (inimesed, protsessid ja tehnoloogia) nõrkusi ning simuleerides ründaja eesmärke ja tegevusi.

Tegevus	Turvafunktsioon
4.8.1. Miinimummeetmed:	
4.8.1.1. Looge andmete taastamisprotsess. Kirjeldage andmete taastamistegevuste skoop (ulatus), taastamise prioriteedid ja varundatud andmete turvalisusnõuded. Hoidke dokumentatsioon ajakohasena ja vaadake see üle vähemalt kord aastas või siis, kui toimuvad olulised muudatused, mis võivad protsessi mõjutada.	Taastamine (andmed)
4.8.1.2. Automatiseerige varukoopiate tegemine. Käivitage varukoopiaid kord nädalas või sagedamini, lähtudes andmete olulisusest või konfidentsiaalsusest.	Taastamine (andmed)
4.8.1.3. Kaitske taastatavaid andmeid samaväärselt algandmetega.	Kaitsmine (andmed)
4.8.1.4. Veenduge, et igal varukoopial on vähemalt üks varundussihtkoht võrguühenduseta (neile ei pääse võrguühenduse kaudu ligi). Näidisrakendused võivad sisaldada versiooni, mis juhib varundussihtkohti võrguühenduseta, pilve- või saidiväliste süsteemide või teenuste kaudu.	Taastamine (andmed)
4.8.1.5. Veenduge, et võrgu infrastruktuur oleks ajakohane. Näidisrakendused hõlmavad tarkvara kõige uuema stabiilse versiooni käitamist ja/või võrguteenusena (NaaS) kasutamist. Tarkvaratoe kontrollimiseks vaadake tarkvaraversioone üle kord kuus või sagedamini.	Kaitsmine (võrk)
4.8.2. Täiendavad meetmed:	
4.8.2.1. Testige varundust kord kvartalis või sagedamini.	Taastamine (andmed)

4.8.2.2. Looge turvaline võrguarhitektuur. Turvaline võrguarhitektuur peab käsitlema vähemalt segmenteerimist, minimaalselt privilegeeritud õigusi ja kättesaadavust.	Kaitsmine (võrk)
4.8.2.3. Halda võrgu infrastruktuuri turvaliselt. Näidisrakendused hõlmavad infrastruktuuri versioneeritud koodi kujul (*version-controlled-infrastructure-as-code*) ja turvaliste protokollide (nt SSH ja HTTPS) kasutamist.	Kaitsmine (võrk)
4.8.2.4. Koostage võrgu arhitektuuriskeemi(d) ja/või muu seonduv võrgusüsteemi dokumentatsioon. Vaadake dokumentatsioon üle ja värskendage seda igal aastal või siis, kui toimuvad olulised muudatused, mis võivad seda kaitsemeedet mõjutada.	Tuvastamine (võrk)
4.8.2.5. Tsentraliseerige AAA.	Kaitsmine (võrk)
4.8.2.6. Kasutage turvalisi võrguhaldus- ja sideprotokolle (nt 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise või uuem).	Kaitsmine (võrk)
4.8.2.7. Nõudke kasutajate autentimist büroo hallatavatele VPN- ja autentimisteenustele enne, kui nad pääsevad ligi büroo ressurssidele lõppkasutaja seadmetes.	Kaitsmine (võrk)
4.8.2.8. Kasutage võrgu administreerimiseks spetsiaalseid füüsiliselt või loogiliselt eraldatud tööjaamu kõigi haldusülesannete või haldusjuurdepääsu nõudvate ülesannete jaoks. Seadmed tuleb segmenteerida büroo primaarvõrgust ja neile ei tohiks lubada internetiühendust.	Kaitsmine (võrk)
4.8.2.9. Koostage testimisplaan, mis vastab büroo suurusele, keerukusele ja küpsusele. Plaanis tuleb märkida: testimise ulatus, nagu võrk, veebirakendus, rakenduse programmeerimisliides (API), hostitud teenused ja füüsiliste ruumide juhtelemendid; sagedus; piirangud, näiteks vastuvõetavad tunnid ja välistatud rünnakutüübid; kontaktpunkti andmed; heastamine, näiteks see, kuidas tulemused sisemiselt suunatakse; ja tagasiulatuvad nõuded.	Tuvastamine
4.8.2.10. Tehke perioodilisi väliseid läbistustestimisi mitte vähem kui kord aastas. Väline läbistustestimine peab hõlmama büroode ja keskkonnaalast luuret, et tuvastada kasutatavat teavet. Läbistustestimine nõuab spetsiaalseid oskusi ja kogemusi ning see tuleb läbi viia kvalifitseeritud osapoole kaudu. Katse võib olla läbipaistev kast (*white box*) või läbipaistmatu kast (*black box*).	Tuvastamine
4.8.2.11. Parandage turvameetmed pärast iga läbistustesti. Juhul, kui testimise käigus esineb leide või kui seda peetakse vajalikuks, muutke reegleid ja võimalusi, et tuvastada katsetamisel kasutatud tehnikaid.	Kaitsmine
4.8.2.12. Tehke perioodilisi sisemisi läbistustestimisi, mitte vähem kui kord aastas. Katse võib olla läbipaistev kast (*white box*) või läbipaistmatu kast (*black box*).	Tuvastamine

4.9. Intsidentide haldus

Intsidentide haldus on kahjuliku intsidendi tegeliku või võimaliku toimumisega seotud tegevuste haldus ja koordineerimine. Intsident on ootamatu sündmus, mis võib rikkuda äritegevusi või teabe turvalisust (nt teenuse, seadmete või vahendite kadu; süsteemi tõrge või ülekoormus; inimviga; lahknevus reeglitest või juhistest; füüsilise turvalisuse rike; süsteemi ohjamatu muutus; tarkvara või riistvara tõrge; pääsuõiguste rikkumine). Intsidentide haldamine aitab kiiresti avastada rünnakuid, tõhusalt ohjeldada võimalikku kahju, likvideerida ründaja kohalolekut ning taastada võrgu ja süsteemide terviklikkus ning samuti kaitsta büroo teavet ja mainet.

Tegevus	Turvafunktsioon
4.9.1. Miinimummeetmed:	
4.9.1.1. Määrake üks võtmeisik, kes juhib intsidentide käsitlemise protsessi. Juhtivtöötajad vastutavad intsidentidele reageerimise ja taastamise jõupingutuste koordineerimise ja dokumenteerimise eest ning võivad koosneda büroosisestest töötajatest ja kolmanda osapoole esindajast. Kui kasutate kolmandat osapoolt, tuleb määrata vähemalt üks büroosisene isik, kes teostab järelevalvet mistahes kolmanda osapoole töö üle. Vaadake protsess üle kord aastas või siis, kui toimuvad olulised muudatused, mis võivad seda protsessi mõjutada.	Reageerimine
4.9.1.2. Koostage nimekiri (sh kontaktandmed) osapooltest, keda tuleb turvaintsidentidest teavitada. Kontaktiks võivad olla büroo töötajaid, kolmanda osapoole esindaja, õiguskaitseasutus, kindlustuse pakkuja, asjaomased valitsusasutused, partnereid või muud sidusrühmad. Kontrollige kontakte igal aastal, et tagada teabe ajakohasus.	Reageerimine
4.9.1.3. Looge protsess, mille abil töötajad saavad intsidentidest teatada. Protsess peab kirjeldama aruandluse ajakava, töötajaid, kellele aru anda, aruandlusmehhanismi ja minimaalset esitatavat teavet. Veenduge, et protsess on kõikidele töötajatele kättesaadav. Vaadake üle kord aastas või siis, kui toimuvad olulised muudatused, mis võivad seda protsessi mõjutada.	Reageerimine
4.9.1.4. Looge intsidentidele reageerimise protsess, mis käsitleb rolle ja kohustusi, vastavusnõudeid ja suhtlusplaani. Vaadake üle kord aastas või siis, kui toimuvad olulised muudatused, mis võivad seda protsessi mõjutada.	Reageerimine
4.9.1.5. Määrake intsidentidele reageerimisel võtmerollid ja -kohustused. Vaadake üle kord aastas või siis, kui toimuvad olulised muudatused, mis võivad seda infot mõjutada.	Reageerimine
4.9.1.6. Määrake kindlaks, milliseid esmaseid ja teiseseid vahendeid kasutatakse intsidendi ajal suhtlemiseks ja sellest teatamiseks. Vahendid võivad olla telefonikõned või e-kirjad. Pidage meeles, et intsident võib vahendeid mõjutada. Vaadake üle kord aastas või siis, kui toimuvad olulised muudatused, mis võivad seda infot mõjutada.	Reageerimine
4.9.1.7. Viige läbi intsidentidele reageerimise õppusi ja stsenaariume intsidentidele reageerimise protsessi kaasatud võtmetöötajatele, et valmistuda reaalsetele intsidentidele reageerimiseks. Harjutused peavad testima suhtluskanaleid, otsuste tegemist ja töövooge. Tehke teste vähemalt igal aastal.	Taastamine
4.9.1.8. Tehke juhtumijärgseid ülevaateid. Intsidendijärgsed ülevaated aitavad vältida vahejuhtumi kordumist, tuvastades saadud õppetunnid ja võttes järelmeetmeid.	Taastamine
4.9.1.9. Kehtestage intsidendi kriteeriumid, sealhulgas tuleb vähemalt eristada intsidenti ja sündmust (nt ebanormaalne tegevus, turvanõrkus, andmete rikkumine, privaatsusintsident jne). Vaadake kriteeriumid üle kord aastas või siis, kui büroos toimuvad olulised muudatused, mis võivad seda kaitsemeedet mõjutada.	Taastamine

4.10. Turvateadlikkus ja koolitused

Turvateadlikkus on oluliste üldiste turvateemade teadmine, oskus säilitada enda käsutuses olevate varade turvalisust ning oskus õigesti käituda turvasündmuste ja -intsidentide puhul.

Turvateadlikkuse tõstmine aitab mõjutada töötajate käitumist, et vähendada büroo infoturbe riske. Küberkurjategijad on edukalt ära kasutanud üksikisikute käitumist (sh teadlikkust), et rikkuda ettevõtete võrke ja olulisi infrastruktuure. Sihtmärgiks võetud isikud, kes ei ole teadlikud ohtudest, võivad tahtmatult eirata turvakontrolle ja –protsesse ning võimaldada sellega nt andmelekke.

Tegevus	Turvafunktsioon
4.10.1. Miinimummeetmed:	
4.10.1.1. Looge töötajatele turvateadlikkuse programm. Programmi eesmärk on harida büroo töötajaid kuidas büroo varasid ja andmeid turvaliselt käsitleda. Viige koolitus läbi vähemalt kord aastas. Vaadake koolituse sisu üle ja ajakohastage seda igal aastal või siis, kui toimuvad olulised muudatused, mis võivad kaitsemeedet mõjutada.	Kaitsmine
4.10.1.2. Koolitage töötajaid, et nad tunneksid ära suhtlusrünnakud (ingl *social engineering*), andmepüügi (ingl *phishing*), eelsõnumite saatmise (ingl *pre-texting*) ja kannul sisenemise (ingl *tailgating*).	Kaitsmine
4.10.1.3. Koolitage töötajaid autentimise parimate tavade osas. Näidisteemad hõlmavad MFA-d, paroolide koostamist ja identimisteabe haldamist.	Kaitsmine
4.10.1.4. Koolitage töötajaid, et nad teaksid kuidas konfidentsiaalseid ja büroo jaoks olulisi andmeid tuvastada ja õigesti säilitada, edastada, arhiveerida ja hävitada. See hõlmab ka töötajate koolitamist puhta ekraani ja laua poliitika osas (nt ekraani lukustamine, kui nad büroo varast eemale astuvad, füüsiliste ja virtuaalsete tahvlite kustutamine andmetest koosolekute lõpus ning andmete ja varade turvaline salvestamine).	Kaitsmine
4.10.1.5. Koolitage töötajaid, et nad oleksid teadlikud tahtmatu andmelekke põhjustamisest. Näidisteemad hõlmavad tähtsate andmete valesti edastamist, kaasaskantava lõppkasutaja seadme kaotsiminekut või andmete avaldamist soovimatutele vaatajaskondadele.	Kaitsmine
4.10.1.6. Koolitage töötajaid, et nad suudaksid ära tunda võimaliku intsidendi ja oleksid võimelised sellest teatama.	Kaitsmine
4.10.1.7. Koolitage töötajaid, et nad oskaksid kontrollida tarkvaraparanduste aegumisi või automatiseeritud protsesside ja tööriistade tõrkeid ning neist vastavalt teatada. Osa sellest koolitusest peaks hõlmama IT-töötajate teavitamist mistahes riketest automatiseeritud protsessides ja vahendites.	Kaitsmine
4.10.1.8. Koolitage töötajaid ohtudest, mis kaasnevad ettevõtetele ebaturvaliste võrkudega ühenduse loomisega ja nende kaudu andmete edastamisega. Kui bürool on kodukontoris töötavaid töötajaid, peab koolitus sisaldama juhiseid tagamaks, et kõik kasutajad konfigureerivad turvaliselt oma koduvõrgu infrastruktuuri.	Kaitsmine
4.10.1.9. Viige läbi rollispetsiifiline turvateadlikkuse ja -oskuste koolitus. Näiteks turvalise süsteemihalduse kursused IT-spetsialistidele, OWASP® Top 10 turvanõrkuste teadlikkuse ja ennetamise koolitus veebirakenduste arendajatele ning suhtlusrünnakute teadlikkuse koolitus kõrgetasemeliste rollide jaoks.	Kaitsmine

4.11. Väliste teenuseosutajate haldus

Tagamaks teenuste osutamine ja talitluspidevus on väga oluline väliselt teenuseosutajalt teenuse saamise kiirus, kvaliteetsus, turvalisus ja õigeaegsus. Turvalisusnõude tagamiseks tuleb kontrollida, et teenuseosutajad tagavad neile usaldatud teenuse osutamiseks vajalike andmete või

süsteemide turvalise käsitluse, sõlmida vastavasisulised lepingud ning vajadusel nõuda tõendeid turvalisuse tõendamiseks. Teenuseosutajaks võib olla partnerettevõte, kes pakub teenust füüsiliselt või siis digitaalne teenusepakkuja nagu Microsoft Sharepoint või Teams.

Tegevus	Turvafunktsioon
4.11.1. Miinimummeetmed:	
4.11.1.1. Koostage füüsiliste teenuseosutajate nimekiri koos kontaktandmetega. Vaadake nimekiri üle ja ajakohastage kord aastas või siis, kui toimuvad olulised muudatused, mis võivad seda infot mõjutada.	Tuvastamine
4.11.1.2. Klassifitseerige nii füüsiliste kui ka digitaalsete teenuste pakkujad. Klassifitseerimise kaalumine võib hõlmata ühte või mitut omadust, nagu teenuse osutamiseks kasutatavate andmete olulisus, andmemaht, kättesaadavuse nõuded, kohaldatavad eeskirjad, olemuslik risk ja maandatud risk. Ajakohastage ja vaadake klassifikaatorid üle kord aastas või siis, kui toimuvad olulised muudatused, mis võivad klassifikatsiooni mõjutada.	Tuvastamine
4.11.1.3. Veenduge, et lepingud või teenuse osutamise tingimused teenuseosutajatega sisaldaksid turvanõudeid (nt minimaalsed infoturbe nõuded, turvaintsidentidest ja/või andmetega seotud rikkumisest teavitamine ja neile reageerimine, andmete krüpteerimise nõuded ja andmete hävitamise kohustus). Turvanõuded peavad olema kooskõlas büroo teenuseosutaja halduspoliitikaga. Vaadake lepingud ja teenuse osutamise tingimused igal aastal üle, et tagada, et lepingutes ei puuduks asja- ja ajakohased turvanõuded.	Kaitsmine
4.11.1.4. Teenuseosutaja tegevuse lõpetamine turvaliselt (nt kasutaja- ja teenusekonto deaktiveerimine, andmevoogude lõpetamine ja büroo andmete turvaline kõrvaldamine teenuseosutaja süsteemidest).	Kaitsmine (andmed)
4.11.2. Täiendavad meetmed:	
4.11.2.1. Looge teenuseosutajate haldusprotsess. Protsess peab käsitlema teenuseosutajate klassifikatsiooni, inventarinimestikku, hindamist, seiret ja tegevuse lõpetamist. Vaadake protsess üle ja ajakohastage seda kord aastas või kui büroos toimuvad olulised muudatused, mis võivad seda protsessi mõjutada.	Tuvastamine
4.11.2.2. Hinnake teenuseosutajaid vastavalt haldusprotsessile. Hindamise ulatus võib varieeruda sõltuvalt klassifikatsioonist (klassifikatsioonidest) ja võib hõlmata sertifikaatide kontrolli (nt ISO, SOC 2, PCI vastavustunnistus AoC jms), kohandatud küsimustikud või muud asjakohased protsessid. Hinnake teenuseosutajaid uuesti igal aastal või uue või uuendatud lepingute puhul.	Tuvastamine
4.11.2.3. Jälgige teenuseosutajaid vastavalt eelnevalt kokkulepitud ja juurutatud haldusprotsessile. Jälgimine võib hõlmata teenuseosutaja nõuetele vastavuse perioodilist ümberhindamist, teenuseosutaja pressiteadete jälgimist ja pimeveebi jälgimist.	Avastamine (andmed)