Mõningaid teabeturbe-alaseid soovitusi

Üldist

Milleks meile teabeturve[1]**?** Väga kokkuvõtlikult öelduna selleks, et meie valduses olevad andmed meiepoolse tahtluseta ei häviks, muutuks ega satuks võõrastesse kätesse ning et meie arvuteid ei kasutataks platvormina küberrünnakute tegemiseks.

Teabeturve ei piirdu üksnes infotehniliste turvameetmete rakendamisega, vaid kätkeb endas ka organisatsioonilisi ja füüsilisi julgeolekumeetmeid. **Ükski arvutisüsteem või tehnoloogia ei suuda tagada turvalisust, kui seda kasutavad inimesed ei käitu hoolikalt!**

Organisatsioonilised turvameetmed sisaldavad töökorralduse, turbesüsteemide kavandamise, halduse ja turvaintsidentide käsitlemisega seotud tegevusi. Teisisõnu seda, et kogudustes, kiriku allasutustes jne mõeldakse läbi, mil moel nende käsutuses olevaid andmeid hallatakse, millised on võimalikud ohud ja kuidas end nende vastu kaitstakse. Meetmete väljatöötamine on aga ainult pool võitu – neid tuleb ka järjepidevalt rakendada ja nende tõhusust hinnata. Pahalased teavad hästi, et inimest on palju kergem või ka odavam rünnata, kui keerulist infosüsteemi. Sellepärast peab ka meie teabeturbeline enesekaitse algama teadlikkusest ja tähelepanelikkusest. Vaja on läbi mõelda seegi, kuidas tagada koguduse/asutuse toimimine juhul, kui näiteks küberrünnaku tõttu[2] kaob internetiühendus või arvuti kasutamise võimalus.

Füüsilised turvameetmed hõlmavad endas kõikvõimalikke taristulisi ja mehaanilisi osiseid. Siia kuuluvad tundliku teabe säilikute hoidmiseks kasutatavad lukustatavad sahtlid/kapid/ruumid, aga seegi, et kõrvalisi isikuid ei jäeta omapäi ruumi, kus näiteks talitusteraamatud avariiulil või liikmeannetuste vastuvõtmise kviitungiraamatud lukustamata lauasahtlis asuvad.

Infotehnilised turvameetmed hõlmavad endas näiteks arvutite/nutiseadmete kaitsmist parooliga, salvestusseadmete sisu krüpteerimist jmt.

Järgnevalt mõned konkreetsemad soovitused igast valdkonnast.

Füüsilised turvameetmed

- **Ära jäta kõrvalist isikut üksi** või järelevalveta tööruumi või mujale hoonesse, kus tal võib tekkida ligipääs tundlikku teavet (sh delikaatsed isikuandmed koguduse liikmete, toimetatud talituste, laekunud annetuste vmt kohta) sisaldavatele andmekandjatele (nt USB mälupulkadele) või dokumentidele.

[1] Tuntud ka kui andmeturve või infoturve.
[2] Tutvu ka Riigi Infosüsteemi Ameti koostatud ohuhinnangute ning nendes antud soovitustega aadressil https://www.ria.ee/et/kuberturvalisus/ohuhinnangud.html

- Tea alati, kus asuvad olulist teavet sisaldavad mobiilsed andmekandjad (näiteks varukoopiate tegemiseks kasutatavad välised kõvakettad).
- Kanna hoolt selle eest, et külalised ja kliendid ei näeks arvuti ekraanil olevat tundlikku infot.
- Pikemaks ajaks töökohalt lahkudes lukusta tööruumi uks ja aknad. Kui ukse lukustamine ei ole võimalik, siis aseta dokumendid lukustatavasse sahtlisse või kappi.
- Tundlikku teavet sisaldavaid dokumente (sh paljundatud materjale, kviitunge, väljaprinte vmt) ei tohi niisama ära visata, vaid nende sisu tuleb muuta loetamatuks. Kõige lihtsam on seda teha küttekoldes (ahjus, kaminas), ent kasutada võib ka "paberihunti" vmt vahendeid.
- Jälgi, et hoone operatiivkaart ja riskianalüüs oleksid ajakohased.

Infotehnoloogilised turvameetmed

- **Hoia oma arvuti/nutiseadme tarkvara ajakohasena** (installeeri saadaolevad süsteemiuuendused).
- Töökohalt **lahkudes** (ka lühiajaliselt!) **lukusta arvuti** (MS Windowsiga arvutis vajuta klaviatuuril üheaegselt Ctrl+Alt+Del ja seejärel ekraanilt valik „Lock" või üheaegselt Windows logoga nuppu + tähte "L"; Mac OS arvutis vajuta üheaegselt "ctrl" + "cmd" + "Q"). Sama ka **nutiseadmega** – kui seda parasjagu ei kasuta, lukusta ekraan ja jälgi, et uuesti avamiseks oleks vajalik parooli või biomeetrilise tuvastuse (sõrmejälg, näotuvastus) kasutamine.
- **Varunda olulisi andmeid** regulaarselt (nt kord nädalas, vajadusel ka sagedamini) välisele kõvakettale, mis muul ajal (väljaspool otsest varundamist) ei ole füüsiliselt arvutiga ühendatud).
- Kui leiad **võõra mälupulga**, mälukaardi, MP3 mängija vmt, ära ühenda seda oma arvutiga – samamoodi nagu sa ju ka maast leitud süstalt oma käsivarde ei torka! Selline tundmatu mälupulk võib sisaldada pahavara ja selle ühendamisest arvutiga võib palju häda sündida.

Salasõna

- … peaks olema võimalikult pikk, aga samas hõlpsasti meeldejääv;
- peaks sisaldama suuri ja väikseid tähti ning numbreid ja/või erisümboleid;
- ei tohiks sisaldada kergesti äraarvatavaid kombinatsioone nagu nt inimese, kiriku/koguduse pühaku, koha- või lemmiklooma nime, autonumbrit, sünnikuupäeva vmt;
- peaks eri teenuste jaoks olema erinev (kasvõi nõnda, et parooli põhiosale lisatakse teenuse nimi veidi mugandatult: nt "M1nuF2cebookiP4rool!"; kindlasti ei tohi oma tööpostkasti salasõna kasutada internetifoorumitesse vmt sisse logimiseks);
- tuleks vahetada teatava regulaarsusega, ometi mitte nii sageli, et lõpuks enam ise ka ei mäleta, milline neist parasjagu kehtiv on;
- tuleb vahetada kindlasti kohe, kui kahtlustad selle teatavaks saamist kellelegi teisele;

- ei tohiks avaldada kellelegi teisele (eriti tööalaseid paroole!);
- … asemel võiks teenustesse sisenemisel eelistada ID-kaarti või Smart-ID teenust.

Tihtilugu määravad inimesed oma kasutajakonto salasõnaks enda, mõne oma pereliikme või lemmiklooma nime, sünnikuupäeva vmt. Seda tehes unustatakse, et suur hulk sellisest teabest on tänapäeval internetist avalikult leitav ning seda ka juhul, kui me ise me seda sinna riputanud pole.

Väga halvad paroolid on näiteks: Abc12345, Qwerty (järjestikused tähed klaviatuuril), 9876543 ja muud sarnased lihtsasti sisestatavad, aga ka sama lihtsasti ära arvatavad variandid. Samuti on üldlevinud salasõnad veel näiteks Test123, Par00l, Administraat0r, admin, salakala jne.

Et parooli oleks kerge meelde jätta, tasub panna see enda jaoks midagi tähendama, ometi nõnda, et salasõna sellest hoolimata kergesti ära arvatav poleks. Mida pikem parool, seda parem. Mõneski teenuses on võimalik paroolis kasutada ka tühikuid, nii et võime kasutada tervet lauset, näiteks “M3i3 r3liikvia on v2badus!”. Kui tühikud toetatud pole, võib nende asemel kasutada näiteks sidekriipsu.

Kontrollküsimused juhuks, kui parool on ununenud, käsitlevad tihti näiteks kodulooma nime või sünnikohta. Ka neid andmeid on pahalastel sageli võimalik internetist leida, mistap ei maksaks *recovery*-funktsiooni küsimustele liiga ausalt vastata.

E-post ja sõnumirakendused

- **Ära ava tundmatutelt või kahtlasena tunduvatelt aadressidelt saadetud linke ega manuseid.** Pigem kahtle kui kahetse! Kahtluse korral võta saatjaga ühendust ja palu tal lingi või manuse sisu kirjeldada, kusjuures eriti hea on, kui saad seda teha mitte sama meiliaadressi, vaid mõne teise kanali (telefon, sõnumirakendus) vahendusel.
- **Ole ettevaatlik nn õngitsuskirjade suhtes**, milles palutakse sisestada kasutajatunnuseid ja paroole ehtsana näivatele teenustele.
- Kui pead interneti vahendusel edastama tundlikke andmeid, võiksid kaaluda **krüpteeritud siderakenduste**, näiteks Signali[3], kasutamist. Ka Apple-i rakendused iMessages ja FaceTime kasutavad krüpteeritud sidet. Tundlikku teavet sisaldavaid faile on üle interneti saatmiseks võimalik ka krüpteerida nõnda, et avada saavad üksnes krüpteerimisel määratud inimesed oma ID-kaardi abil. Selleks on vaja teada adressaadi isikukoodi.[4]

Elektronkiri on praegusajal kõiksugu petuskeemide, viiruste, lunavaraprogrammide jmt levitamise kõige levinumaid kanaleid, kuna elektronkirja saatmine ei maksa sama hästi kui midagi. Ka on kirja saatja raskesti tuvastatav: igaüks saab luua endale suvalise nimega tasuta e-posti aadressi, aga üsna hõlbus on võltsida ka päriselt olemasoleva e-postikonto aadressi. Sama käib ka sotsiaalmeedia kasutajakontode kohta.

---

[3] Vt https://www.signal.org
[4] Vt https://www.id.ee/rubriik/krupteerimine-id-abi/

Oma tööasju ei saa usaldada väliste e-posti serverite ega veebiportaalide hoolde (GMail.com, Facebook vmt). Selliste lehtede kasutustingimused ei pane neid vastutama millegi eest ega garanteeri andmete konfidentsiaalsust.

EELK.ee aadressidele saadetavad kirjad läbivad kõik rämpsposti filtri, kuid osa rämpspostist võib siiski filtrist läbi pääseda ja sinu postkasti jõuda. Niisugused kirjad tasub märgistada rämpspostiks (täpsemad võimalused sõltuvad kasutatavast e-posti haldamise programmist) ning kustutada avamata. Kui rämpspostile vastata või seal leiduvaid linke avada, teab selle saatja, et sinu e-posti aadress toimib ja jätkab rämpsposti saatmist, võib aga lisaks edastada sinu aadressi ka teistele rämpsposti saatjatele, nii et kirjade laviin suureneb veelgi.

Sotsiaalmeedia

- **Üheksa korda mõõda, üks kord postita!** Infot tohib internetis, olgu sotsiaalmeedias, enda veebilehel, e-postiloendites või mujal, avaldada alles pärast hoolikat kaalumist. Ka lühikest aega tähelepanu saav info, nt foorumipostitus, mis on suunatud vaid väikesele hulgale lugejatele, võib olenevalt olukorrast jääda väga kauaks internetis kättesaadavaks ja jõuda teinekord hoopis ootamatute inimesteni. Otsingutega, nt otsingumootorites või suhtlusvõrgustikes, saab koguda infot väga erinevatest valdkondadest. **Kõike, mida sa postitad, võidakse kasutada kõiksugu inimeste poolt igasugustel eesmärkidel!**
- Enne internetis info edastamist või avaldamist peab hoolikalt järele mõtlema, millise **mulje** võib see info jätta sinust ja kirikust, kus sa töötad, ning kas selle info edastamine on kindlasti vajalik. Lähtuda tuleb põhimõttest, et avaldada tohib ainult selliseid asju, mida kõlbaks avaldada ka oma nime all mõnes ajalehes või ise televisioonis kõnelda.
- Ära avalda ilma loata teiste inimeste **isikuandmeid**! Ära riku **autoriõigusi** (sh teiste tehtud fotode kasutamisel oma materjalides; kui kahtled, uuri järele, kas tohid seda või teist asja avaldada ja millistel tingimustel)!
- Andmed, millest ilmnevad usulised või filosoofilised veendumused (nt kogudusse kuulumine ja usulistest talitustest osa võtmine) on seaduse silmis **eriliiki** (varasemalt nimetatud kui delikaatsed) **isikuandmed** ja nende töötlemisele on seatud rida tingimusi.[5]
- Sotsiaalmeedias leviv info pärineb väga erineva usaldusväärsusega allikatest. Tuleb meeles pidada, et käimas on laialdane **infosõda** ja me kõik viibime tihtipeale selle lahinguväljadel. Kõik pole kuld, mis meile meeldivaid seisukohti toetab (või vastupidi).
- Kui paljud meist on valmis sõbrunema võhivõõra inimesega, kes tuleb tänaval ligi ja ennast sõbraks pakub? Ilmselt mitte väga paljud. Kübermaailmas ollakse **usaldavad** aga märksa varmamalt. Miljoneid eurosid kantakse igal aastal ootamatult hätta sattunud netisõpradele, kel tekkisid ootamatult rahalised raskused või kes vajavad

[5] Neist räägivad isikuandmete kaitse seadus ning Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679.

> raha Eestisse sõiduks pileti ostmiseks. Pole vist vaja täpsustada, et päriselus nendega kohtumiseni ei jõutagi.

Omaette teema, eriti praeguse infosõja tingimustes, on foorumites ja sotsiaalmeedias postitavad **trollid** ning nendega suhtlemine. On üsna ilmseid ja räigeid arvamusavaldusi, näiteks:

> *"Ega USA ja Nato ei pea plaani meid kaitsta, nad ikka peavad plaani Venemaad rünnata. Mis plaan saaks üldse olla Baltikumi kaitsimine? Väed tuuakse sisse ikka ründamiseks. Dessantväelased, lennukid. Need on ikka Venemaa ründamiseks mõeldud. Mis dessanti saa eestis teed? Ilmselt on neil plaanid olemas kuid Moskva ja suuremad sõjaväeosad kiiresti vallutada."* (LHV foorum 23.02.2022; *sic!*)

Üha sagedamini kohtab avaldusi, mis vähem ilmselt, kuid siiski Vene Föderatsiooni jutupunkte järgides püüavad tekitada usaldamatust Eesti Vabariigi institutsioonide ja riigikaitse vastu (stiilis "Vene väed on nagunii kahe päevaga Tallinnas ja ükski NATO meid ei aita."), jätta muljet, et "kõik valetavad ja seega ei olegi võimalik teada, kuidas asjad päriselt on" (näiteks stiilis "Aga äkki tõesti tapsid ukrainlased Donbassis lapsi – kust me teame!") jne.

Trollidega ei maksa vaidlusse laskuda. Miks? Ühelt poolt muidugi sellepärast, et see on asjatu aja raiskamine. Nagu vanarahvas ütleb: sotsiaalmeedias toimunud vaidlused pole eales kedagi pannud oma arvamust muutma. Oluline on aga seegi, et trollide postitustele reageerimisega aitame me tahtmatult kaasa nende levimisele. Seega: ära allu provokatsioonidele.

Facebookis selgelt vaenuõhutavaid (näiteks Eestis viibivate ukrainlaste vastu viha ärgitavat) postitusi tasub ka Facebookile raporteerida.[6]

Lisalugemist

Info küberturvalisuse valdkonna kohta on leitav Riigi Infosüsteemi Ameti kodulehelt (https://www.ria.ee/et/kuberturvalisus.html). Sealt leiab mh erinevat teavet olukorra kohta küberruumis, abistavat infot küberintsidentidest teavitamise kohta ning muid nõuandeid ja juhendeid. Samuti on soovitatav tutvuda ka veebilehel https://www.itvaatlik.ee olevate selgituste ja õpetustega.

Netitrollide tegevusest saab lisa kugeda Propastopi lehelt https://www.propastop.org ning muidugi "Infosõjas osalemise ABC":
https://www.targaltinternetis.ee/wp-content/uploads/2022/03/Infosojas_osalemise_ABC.pdf

[6] Vt https://www.propastop.org/2022/03/19/7809/