riigikontroll

Kohalikud omavalitsused Meie 25.09.2018 nr 2-2.9/50094/4

Riigikontrolli ringkiri auditi „IT-turvameetmete rakendamine kohalikes omavalitsustes“ tulemuste kohta

Austatud kohaliku omavalitsuse juht

Riigi ja kohalike omavalitsuste asutustele kohustusliku infoturbe rakendamise juhendi ISKE[1] kohaselt on iga **asutuse juhtkonna** ülesanne **algatada** turvameetmete süsteemi rakendamise protsess **ning juhtida ja kontrollida** seda. Turvameetmete süsteemi rakendamine aitab kaasa ka mitme uue seaduse täitmisele, näiteks mais 2018 jõustunud otsekohalduv Euroopa Liidu isikuandmete kaitse üldmäärus 2016/679 ning värske küberturvalisuse seadus. Nii juba kehtiv kui ka peatselt kehtima hakkavad nõuded infoturbele eeldavad terviklikku teadmist (sh riskianalüüsi turvameetmete valiku alusena) asutuse andmetöötlusest.

Riigikontroll viis 2017. aastal 10 kohalikus omavalitsuses läbi auditi, mille eesmärk oli anda hinnang, kas omavalitsused on rakendanud nõuetele kohaselt infoturbemeetmeid. Testitud turbemeetmed valiti nendest ISKE tüüpmoodulitest, mille täitmisega on omavalitsustes ka varem probleeme olnud. Tähelepanekud ja ettepanekud, mida Riigikontroll pidas oluliseks, on koondatud 5. juunil 2018 koostatud Riigikontrolli kontrolliaruandesse nr 2-1.9/50094/2.

Tuginedes nii Riigikontrolli kui ka Riigi Infosüsteemi Ameti varasemate aastate kontrollkäikudel tuvastatud puudustele, on koostatud käesolev ringkiri. Kiri on saadetud kõikidele omavalitsustele eesmärgiga informeerida iga omavalitsuse juhtkonda nõuetest, millele peaks IT-turvalisuse tagamisel senisest enam tähelepanu pöörama. Riigikontroll loodab, et ringkirjas toodud tähelepanekud on omavalitsuse IT-spetsialistidele abiks omavalitsuse IT-turvalisuse probleemide selgitamisel ja nende lahendamisel.

[1] Infosüsteemide kolmeastmeline etalonturbe süsteem, mis on loodud eelkõige riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavatele infosüsteemidele ning nendega seotud infovaradele turvalisuse tagamiseks.

1 Töökohaarvutite kasutajatele tuleb anda piiratud õigusega kasutajakontod.[2]

Pääsuõigused (nt töökohaarvutile, serverile, andmekogudele) tohib väljastada töötajatele ainult sellises mahus, mis on hädavajalik nende tööülesannete täitmiseks, ja administreerimiseks mõeldud kontosid tohib kasutada vaid juhul, kui seda on ilmtingimata vaja. Kasutajatele kergekäeliselt administreerimisõiguste andmisega antakse ära kontroll asutuse arvutitesse installeeritava tarkvara üle. Kasutajad saavad sellisel juhul piiranguteta paigaldada töökohaarvutitesse endale meelepärast tarkvara, mis võib sisaldada pahavara, olla illegaalne, koormata võrgu ressursse jne. Pahavaraga nakatumise tagajärjed on leebemad, kui iga kasutaja (ja tema potentsiaalselt nakatunud arvuti) ei pääse ligi kõikidele võrguketastele ja sealsetele failidele. Eriti laialdased on kasutaja õigused, kui talle on antud administraatoriõigused domeenis.[3] Sellisel juhul võib kasutaja tegevus mõjutada ka teisi sisevõrgus asuvaid töökohaarvuteid ja seadmeid. Seetõttu on soovitatav eemaldada lokaalsed töökohaarvutite administreerimise õigused ja asendada need piiratud õigusega kasutajakontodega. Olukorras, kus kasutajad on administraatoriõigustega, sest IT-spetsialistil ei ole aega käia igas arvutis näiteks uuendusi paigaldamas, tasub kaaluda keskhalduse tarkvara kasutusele võtmist.

Halb praktika

- Asutuses antakse administraatori õigused kasutajale, et teha programmivärskendusi, sest keskhaldust ei ole sisse seatud.
- Kasutaja logib IT-spetsialisti teadmata arvutisse, kasutades lokaalset administraatori kontot, sest see ei olnud välja lülitatud.

2 Tarkvaratootjate avaldatud veaparandusi ja turvauuendusi tuleb regulaarselt paigaldada.[4]

Tarkvaralistes lahendustes avastatakse igapäevaselt nõrkusi, mida kasutades saab asutuse IT-süsteeme rünnata. Paikamata tarkvara tõttu kasvab arvutiviirustega nakatumise tõenäosus. Seetõttu tuleb kõikide IT-toodete kohta regulaarselt uurida, kas tootja on avaldanud uut infot võimalike turvalünkade ja nende kõrvaldamise kohta. Paljudel toodetel (nt operatsioonisüsteem, viirusetõrje) on automaatsed värskendusmehhanismid (nt *Windows Update*), mis teavitavad kasutajat saadaolevatest paikadest või värskendustest. Kuigi töökohaarvutite käsitsi uuendamise asemel on automaatse uuendamise lubamine kindlasti soovitatav, tuleb siiski ka kontrollida, et alla laetud (ingl *download*) uuendused oleks paigaldatud (ingl *install*). Näiteks kui kasutajatel ei ole kombeks oma arvutit sulgeda või uuendused tulevad peale ebasobival ajal, kus kasutaja ei nõustu taaskäivitust (ingl *restart*) tegema, siis ei saa alla laetud uuendused rakenduda. Seega tuleks tõsiselt mõelda, kas on põhjendatud jätta muudatuste paigaldamine kasutajate hooleks või paigaldada muudatused pärast allalaadimist automaatselt.

Hea praktika

Operatsioonisüsteemi vahetamisel on mõistlik võtta ühendust ka andmekogude pidamiseks kasutatavate tarkvaralahenduste pakkujatega, et selgitada välja, kas tarkvara töötab valitud operatsioonisüsteemiga või mitte.

Samuti ei tohi unustada, et ka automaatsete uuenduste mõju juba kasutatavatele IT-süsteemidele tuleks enne paigaldamist kontrollida ning testima peaks nõnda, et see ei mõjutaks teisi seadmeid.[5] Vastasel juhul võib näiteks pärast paigaldamist selguda, et uuenduse tõttu on häiritud muu tarkvara või riistvara (nt printerid) kasutatavus.

[2] ISKE meede M 2.8. IT-rakendustele ja andmetele pääsuõiguste andmine; M 2.220. Pääsu reguleerimise suunised.
[3] Võrgu domeen on loogiliselt ühte kuuluv grupp arvutiteid, mis jagavad keskset andmebaasi. Jagatav andmebaas sisaldab domeeni kuuluvate kasutajate kontosid (igal kasutajal on unikaalne konto koos selle kontoga seotud õigustega) ja turvainfot domeenis olevate ressursside kohta.
[4] M 4.324. Automaatsete uuendusmehhanismide konfiguratsioon turvapaikade ja muudatuste haldamisel; M 2.273. Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine.
[5] M 4.65. Uue riist- ja tarkvara testimine.

3 Kogu asutuse interneti andmeliiklus peab käima läbi korrektselt seadistatud tulemüüri.[6]

Turvalüüs (tulemüür) on riist- ja tarkvaratehnilistest komponentidest koosnev süsteem IP-võrkude omavaheliseks turvaliseks ühendamiseks. Tulemüür võib olla nii riistvaraline kui ka tarkvaraline. Töökohaarvutites saab tavaliselt seadistada tarkvaralise tulemüüri, mis on eriti oluline nt sülearvutites. Tulemüüri puudumisel ei ole asutuse IT-süsteem internetist tulevate ohtude (nt häkkerid, pahavara) eest kaitstud. Kui asutuse sisevõrk ei ole kaitstud, siis on võimalik välisvõrgust pärida mitmesuguseid andmeid, nt meiliaadresse, IP-numbreid, arvuti- ja kasutajanimesid.

Pelgalt tulemüüri olemasolust aga ei piisa – see tuleb ka korralikult seadistada, muudatused dokumenteerida ja selle operatsioonide logisid regulaarselt jälgida, et tuvastada võimalikke ründeid.[7] Tulemüüri seadistamisel tuleb silmas pidada, et tootja või levitaja poolsed algsätted ei pruugi olla piisavalt turvalised. Tulemüüride vaikimisi seadeid ei tasu seetõttu pimesi pidada optimaalseks ja kohe kasutamiseks võtta. Tulemüüri seadistuse põhimõtted peavad olema kirjas ning selle muudatusi tuleb alati põhjendada, et oleks selge, miks on konkreetset reeglit vaja, kes on selle reegli tellija ja mis ajavahemikul reegel kehtima peab.

Hea praktika

Tulemüür tuleks seadistada põhimõttel, et ligipääs lubatakse ainult nendele teenustele, mis on hädavajalikud. S.t standardsättena lükatakse tagasi kõik ühenduspäringud väljast ja lubatakse neid, mille järele on kasutajatel vajadus oma tööülesannete täitmiseks.

4 Kasutajate pääsuõigused peavad olema ajakohased.[8]

Pääsuõigust IT-rakenduste ja andmete juurde võib anda ainult tööülesannete täitmiseks vajalikus ulatuses. KOVi ametnikud saavad ligi pereregistrisse, töötamise registrisse, haigekassasse, väärteomenetlejate portaali, sotsiaalteenuste ja -toetuste andmeregistrisse STAR, omavalitsuste teenuseportaali KOVTP, KOVi raamatupidamisprogrammi, Omniva e-arvekeskusesse jt. Välja jagatud pääsuõiguste dokumentatsioon peab olema ajakohane. Töösuhte lõppemise järel peab veenduma, et isik ei saa oma pääsuõigusi enam kasutada.

Töötaja vahetumisel tuleb uuele töötajale luua personaalne kasutajakonto. Seda ka juhul, kui võetakse tööle nt lapsehoolduspuhkusel oleva ametniku asendaja. Sama kasutajatunnuse kasutamine mitme töötaja poolt peaks olema keelatud, kuna probleemide korral kontrollitakse, kes ja mida arvutis või andmekogus tegi.[9] Vastasel juhul ei ole logidele toetudes probleemide põhjustajat võimalik selgelt kindlaks teha, sest süsteem näitab, et arvutiga või andmetega töötas ainult üks kasutaja. On ka võimalik, et ainus sisse loginud kasutaja peab tagajärgede eest vastutama ainuisikuliselt.

5 Andmete töötleja peab teadma, kuidas ja kus tema vastutuses olevaid andmeid ja nende varukoopiaid hoitakse.[10]

KOVide eripäraks andmete töötlemisel on standardlahenduste kasutamine. Sel juhul on andmed üldiselt majutatud ja varundatud tarkvaralahenduse pakkuja juures. Sellistel puhkudel peaks KOV veenduma, et nende andmete varukoopiate andmekandjatele on tagatud kiire juurdepääs ning seda ainult volitatud isikutel. Muu hulgas tuleb arvestada, et isikuandmete puhul on serveri asukohale seatud piirangud.[11] Näiteks on isikuandmeid lubatud töödelda väljaspool Eestit Euroopa Liidus asuvas ja Euroopa majanduspiirkonnas (EMP) või samaväärse andmekaitsetasemega riigis tegutsevas avalikus pilves kuni turvaklassini K2T1S1 (k.a). Piirangu on tinginud eelkõige vastutuse

[6] M 2.204. Ebaturvalise võrkupääsu tõkestamine; ISKE tüüpmoodulis B 3.301. Turvalüüs (tulemüür).
[7] M 2.299. Turvalüüsi (tulemüüri) turvapoliitika koostamine; M 4.47. Turvalüüsi operatsioonide logimine.
[8] M 2.8. IT-rakendustele ja andmetele pääsuõiguste andmine; M 3.6. Reguleeritud protseduur töösuhete lõpetamiseks.
[9] M 2.30. Kasutajate ja kasutajarühmade määramise protseduurid.
[10] M 6.20. Varukoopia andmekandjate õige ladustus.
[11] Isikuandmete kaitse seaduse § 18 lg 2.

jagunemine, turvameetmete rakendatuse kontrollimise keerukus ja läbipaistmatus, jurisdiktsioonilised erisused, serveriressursi jagamine teiste klientidega jm.[12] Varundamisel tuleks arvestada ka sellega, et õnnetusjuhtumite puhuks hoitakse andmete varukoopiad andmeid sisaldavast arvutist eraldi ruumis, võimaluse korral mõnes teises tuletõkketsoonis.

6 Juurutada tuleb korrektne paroolihaldus, sh määrata parooli miinimumpikkus, aegumistähtaeg, ning lubada kasutajatel ise parool valida.[13]

IT-süsteemidesse sisenemiseks tuleb seada kasutajate tuvastus- ja autentimismehhanismid (s.o kasutajatunnus ja parool). Parooliks ei sobi nimi, auto numbrimärk, sünnikuupäev jms ning oma parooli peaks teadma vaid kasutaja. Ka uutele kasutajatele esmakordseks süsteemi sisenemiseks jagatud paroolid tuleb kohe pärast esimest kasutamist ära muuta. Liiga lühikeste ja triviaalsete kombinatsioonide (nt „BBBBBBBB“, „123456“) parooliks valimist tuleb takistada. Kui parooli keerukuse reegleid tehnilise vahenditega ei seata, siis võib kasutaja paroolivahetusel jätta parooli lahtri näiteks ka täiesti tühjaks ning edaspidi üldse mitte parooli sisestada.

Pärast parooli korduvat valesti sisestamist peaks autentimissüsteem juurdepääsu sulgema (teatud ajaks või püsivalt), et parooli ei saaks proovimise teel kõrvalised isikud mõistatada.

Isegi kui ollakse seisukohal, et parooli kohustusliku muutmise korral hakkaksid teenistujad paroole üles kirjutama, peaks süsteem kohustama kasutajat regulaarselt parooli muutma. Pärast parooli muutmist peaks IT-süsteem takistama vanade paroolide kasutamist (paroolide ajalugu). Vastasel juhul võib kasutaja jäädagi kasutama üht ja sama parooli ning nõutud paroolivahetus on ainult näiline.

Hea praktika

Triviaalsete paroolide kasutamine on tõkestatud tehniliste vahenditega. Poliitikasäte „paroolid peavad vastama keerukuse nõuetele“ on seatud. Parooli miinimumpikkus on 8 sümbolit. Süsteem salvestab nt 24 kasutatud parooli. Pärast 3-kordset parooli valesisestust kasutajakonto blokeeritakse.

Paroolipoliitika väljatöötamisel peaks läbi mõtlema ka kasutajatele õiguste andmise ning operatsioonisüsteemi võimalused. Näiteks kui kasutajatel on administraatoriõigused, siis saavad nad soovi korral muuta süsteemi seadistusi, sh paroolipoliitikat. Kui arvutites on kasutusel operatsioonisüsteem, mis on üldiselt kodukasutaja vajadustele arendatud, siis ei pruugi nendes üldse olla võimalusi paroolipoliitika seadistamiseks. Silmas tuleb pidada, et kodukasutajale mõeldud operatsioonisüsteemidega arvuteid ei ole võimalik liita ka domeeni (nt *Active Directory*). Kui paroolipoliitika on seadistatud domeenis olevatele arvutitele, siis nendele arvutitele, mida domeenis ei ole või kuhu domeeni kasutajana sisse ei logita, paroolipoliitika ei kehti.

Teadmiseks, et

Paljud süsteemid võimaldavad luua lahenduse *Single-Sign-On* (SSO), kus kasutajad ei pea ennast iga rakenduse juures uuesti sisse logima. Näiteks logitakse tavapäraselt sisse töökohaarvutisse ja saadakse kohe ligipääs ka tööjaama paigaldatud meilirakendusse, võrgukataloogidesse. Selliste süsteemide puhul tuleb paroolidega eriti hoolikas olla, sest kui volitamata isik saab parooli teada, on tal vaja ainult ühte kohta kasutaja autentimise andmed sisestada, et saada ligipääs suurele hulgale andmetele.

[12] Vt lisaks B 1.17. Pilvteenuse kasutamine.
[13] M 2.11. Paroolide kasutamise reeglid.

Üldiselt peaks süsteemi seadistama nii, et uus töötaja peab esmakordsel sisselogimisel oma parooli kohe ka ära vahetama. Kui kasutaja valib endale esmakordsel sisselogimisel ise parooli, siis ei ole kohene paroolivahetus oluline, kuid kui parooli on andnud IT-töötaja (sh kui parool ununeb), siis peab selle vahetama. Keegi teine peale kasutaja ei tohi teada tema töökohaarvutisse sisenemise parooli. S.t IT-töötaja jagatud ühekordsed paroolid tuleb vahetada, ja kui IT-spetsialist (sh majaväline) küsib kasutaja käest parooli, siis seda ei tohi mitte mingil ettekäändel anda.

Halb praktika

Parooli sisestamisel kuvatakse paroolivihje arvutiekraanil, kui on sisestatud vale parool. Lisaks selgub paroolivihjest, et kasutaja parool sisaldab perekonnanime ning tehniliselt ei peatata kasutajatunnust, kui on olnud mitmeid nurjunud sisselogimiskatseid.

7 Alglaadimise seaded (BIOS) peavad olema kaitstud.[14]

BIOSi on vaja, et kasutaja saaks oma operatsioonisüsteemile ligi ja arvuti käivituks. Kui siseneda BIOSi seadetesse, siis seal saab muuta nt seadmeid, kust alglaadimist tehakse (nt kõvaketas, CD-ROM, DVD-ROM seade või USB draiv). Alglaadimine tehakse tavaliselt CD-lt, kui on vaja nt operatsioonisüsteem paigaldada. Hiljem tuleks aga BIOSi seadistus tagasi muuta kõvaketta pealt alglaadimisele. Laadimisjärjekorra muutmata jätmise korral on võimalik mööda pääseda turvamehhanismidest, nt autentimisest. Järjekorral ei ole aga tähtsust, kui BIOSi seadetesse pääseb sisse ilma paroolita. Kui parooli ei ole, saab ükskõik kes seadistada alglaadimise nt USB pealt ning sealtkaudu on juba võimalik arvutis olevad andmed kätte saada.

8 Asutusesiseseks kasutamiseks tunnistatud e-kirja manused ja sülearvutite kõvakettad on soovitatav krüpteerida.[15]

Konfidentsiaalsete (nii kasutamisel kui ka hilisemal hävitamisel) digidokumentide käitlemine on muutunud eriti aktuaalseks seoses maikuus jõustunud Euroopa Liidu uue andmekaitsemäärusega, mis nõuab paljude dokumentide (sh digitaalsete) konfidentsiaalsena hoidmist.

Et volitamata isikud ei pääseks ligi töökohaarvutis asuvatele konfidentsiaalsetele andmetele, tuleks arvuti kõvaketas võimaluse korral alati krüpteerida (nt *McAfee Endpoint Encryption, Sophos SafeGuard Enterprise, Windows BitLocker Drive Encryption*). Andmed peavad olema piisavalt kaitstud ka siis, kui arvuti on välja lülitatud, nt varguse korral. Kettasisu krüpteerimine on eriti oluline just sülearvutite puhul, kuna nende varguse oht on suurem ning ründajal on andmetele ligipääsemiseks väga palju aega. Samal ajal ei tohi unustada ka andmevahetust elektronposti teel. Et elektroonilist suhtlust ei saaks teel muuta ega pealt kuulata, on vaja tundlikku infot sisaldavate e-kirjade edastamisel krüpteerida asutusesiseseks kasutamiseks tunnistatud e-kirja manused (nt *DigiDoc3 Krüpto*).

[14] M 4.84. BIOSi turvamehhanismide kasutamine.
[15] M 4.337z. BitLockeri Drive Encryption'i kasutamine [z = soovituslik] (M4: Riistvara ja tarkvara); M 2.163. Krüptoprotseduure ja -tooteid mõjutavate tegurite määramine.

9 Töökohaarvutite tüüptarkvara kohta peab olema koostatud nimekiri, seda peab rakendama ning tagama, et kasutajad ei paigaldaks põhjendamatult nimekirja mittekuuluvat tarkvara.

Mittesoovitud riist- ja tarkvara (nt illegaalselt omandatud / litsentseerimata tarkvara, autorikaitse alla kuuluv tarkvara, kui selle vara kohta ei ole ostutõendit või muud legaalsust tõendavat dokumenti) paigaldamine ja kasutamine tuleb keelata ning tehniliste lahendustega takistada. Selgelt peab olema välja toodud, mis tarkvaratoode või mis nõuetele vastav tüüptarkvara üldse on aktsepteeritav.[16] Näiteks tuleks väga põhjalikult kaaluda, kas kommertspilve kasutamine suuremate failide edastamiseks on vastuvõetav ka sotsiaaltöö andmetega failide korral või tohib sellises pilves hoida ainult juurdepääsupiiranguta andmeid. Lisaks võib kaaluda, kas keelata erinevate seadmete (nt mälupulga) omavoliline ühendamine arvutivõrku või arvutiga. Tarkvaralitsentside puhul tuleb jälgida, kes litsentsi kasutada võib. Näiteks haridusasutustele on tihtipeale erinevad kontoritarkvara litsentsid tasuta, aga KOVidele see ei laiene.

Teadmiseks, et

operatsioonisüsteemi uuemale versioonile üleminekul on asutuse enda mure tõestada, et kunagi on ostetud tasuta üleminekuks (näiteks Windows 10 Pro-le) sobivad litsentsid. Vastasel juhul ei saa aktiveeritud operatsioonisüsteemi paigaldusi legaalseks pidada.

Tähelepanelik tasub olla ka tarkvara uuendusi tehes ja arvutite ostmisel. Mitmed tarkvarad, mida tööülesannete täitmiseks tegelikult vaja ei ole, tulevad kaasa uuendustega (nt MS *OneDrive*) või on arvuti müüja need eelnevalt paigaldanud.

Enamik operatsioonisüsteeme võimaldab mittesoovitud riist- ja tarkvara paigaldamist takistada kasutajakeskkonna (tavakasutaja, administraator) piiramisega. Piiramise eesmärk on hoida eemal ebasoovitavad programmid, mida pole tööülesannete täitmiseks vaja ja mis koormavad põhjendamatult IT-süsteemi.[17] Kui tehnilisi võimalusi tarkvara paigaldamise takistamiseks pole rakendatud, tuleb regulaarselt kontrollida, kas kasutajad peavad kinni mittesoovitud riist- ja tarkvara installeerimise ja kasutamise keelust. Aktsepteerimata tarkvara kasutamise tuvastamise muudab lihtsamaks ühetüüpsete tööjaamade rajamine, s.t ühtmoodi riist- ja tarkvara (sh versioonid) ning nende ühesugune konfiguratsioon. Lisaks lihtsustab see kasutajate nõustamist (hooldus, tugi ja korrashoid) ning muudatuste haldust. [18]

10 Tarkvara versioonid, millele tootja enam tuge ei paku, tuleb asendada uuema tarkvaraga.[19]

Igal tarkvaratootel on n-ö elutsükkel. Elutsükkel algab toote väljaandmisega ja lõpeb siis, kui seda enam ei toetata. Näiteks serveri operatsioonisüsteemi Windows 2000 ja 2003 tootja ei paku tarkvarale enam tuge, s.t tootja ei väljasta tarkvara turvauuendusi ega analüüsi tarkvara uusi avastatud nõrkusi. Samuti on lõppenud populaarse töökohaarvuti operatsioonisüsteemi Windows XP ja Windows Vista toetamine. Tuge ei pakuta enam ka kontoritarkvarale MS Office 2000, 2003 ja 2007. Töökohaarvutites ja serverites on soovitatav asendada tarkvara, millele enam tuge ei pakuta, võimaluse korral uuema tarkvaraga. Tooteid saab küll jätkuvalt kasutada pärast toe lõppemist, kuid see võib muuta arvuti haavatavaks turbeohtudest ja viirustest. Lisaks, kuna aina suurem osa tark- ja riistvaratootjaid optimeerib oma tooted uuemate tarkvaraversioonide jaoks, võib juhtuda, et mingi hetk kõik rakendused ja seadmed enam ei tööta. Näiteks ei levitata alates 2015. aastast enam ID-tarkvara ega pakuta kasutajatuge Windows XP operatsioonisüsteemi kasutajatele.

[16] M 2.88. Tüüptarkvara litsentsi- ja versioonihaldus.
[17] M 2.9. Aktsepteerimata riist- ja tarkvara kasutuse keeld.
[18] M 2.69. Tüüpsete tööjaamade rajamine.
[19] M 4.107. Tootja ressursside kasutamine.

11 Viirusetõrjetarkvara peab olema seadistatud nii, et oleks tagatud ajakohane regulaarne töökohaarvutite ja teisaldatavate seadmete skaneerimine. [20]

Saavutamaks efektiivset arvutiviirustevastast kaitset terve asutuse jaoks, tuleb tagada, et viiruste esinemine oleks takistatud või võimalikult kiiresti avastatav. Selleks tuleb töökohaarvuteid regulaarselt skaneerida viirustõrjeprogrammiga. Sobiva viirusetõrjeskanneri valimisel tasuks uurida, kuidas erinevad tooted on läbinud mõne sõltumatu teadusasutuse testid (nt *The Independent IT-Security Institute* (www.av-test.org)).[21]

Hea praktika

Viirusetõrjeprogramm on keskhaldusega, töökohaarvutites on kasutajatel tavaõigused ja nad ei saa teha muudatusi.

Viirusetõrjeprogrammi vaikeseadistused tuleks kindlasti üle kontrollida. Näiteks peaks veenduma, et viirusetõrje oleks püsivalt sisse lülitatud, skaneeriks ka teisaldatavaid seadmeid (nt mälupulk) ja oleks regulaarselt värskendatud, et see suudaks tuvastada ka uusi, aina juurde tekkivaid arvutiviirusi.[22] Lisaks peab veenduma, et kasutajad ei saa ise viirusetõrjeprogrammi välja lülitada või selle seadistust muuta.

12 Turvaintsidentidest tuleb teavitada CERT-EEd ja määrata nende käsitlemise eest vastutav isik.[23]

Turvaintsidentidest, mis viivad asutuse töö või elutähtsate teenuste katkestuste ohuni või mõjutavad teisi IT-süsteeme ja võrgupõhiseid lahendusi, tuleb teavitada Riigi Infosüsteemi Ameti infoturbe intsidentide käsitlemise osakonda CERT-EE. Intsidentidest saab CERT-EE teada kas riigivõrgu turvaseire[24] kaudu või annavad asutused ise teada, kui midagi kahtlast on nende IT-süsteemis juhtunud. Vastutus turvaintsidentide käsitlemise eest tuleb kirja panna nt vastutava isiku ametijuhendisse ja/või turvaintsidentide käsitlemise kontseptsiooni.

Intsidendi käsitlemisel ei piisa ainult kõvaketta puhtaks tegemisest ja andmete taastamisest. Turvaaukude kõrvaldamiseks tuleb intsidendist puudutatud IT-süsteemid võrgust eemaldada ja kõik failid (nt logifailid), mis võivad anda infot esinenud probleemide liigi ja põhjuse kohta, varundada. Kõikide turvaintsidendist puudutatud IT-süsteemide operatsioonisüsteemide ja rakenduste muutusi peab uurima, et veenduda, et süsteemi ei oleks manipuleeritud, ning ründejärgse taaskäivitamise järel tuleb muuta paroolid.

Näide

Pärast olulise turvaintsidendi avastamist võtab asutuse infoturbe eest vastutav isik ühendust CERT-EE-ga,

→ helistades numbril 663 0299;
→ kirjutades aadressil cert@cert.

Teavitamisel edastatakse turvaintsidendi kohta niipalju infot, kui võimalik.

13 Andmevarundus (mh arvutite ja serverite seadistused) peab olema tagatud ja kontrollitud.[25]

Andmevarunduskontseptsiooni[26] eesmärk on leida lahendus, kuidas arvestada piisavalt kõigi mõju-teguritega ja jääda samas majanduslikult talutavatesse kulupiiridesse. Vaid reeglipärane ja ulatuslik andmete varundamine suudab kindlalt tagada, et rikete, avariide, (tahtlike või tahtmatute)

[20] M 2.156. Sobiva viirusetõrjestrateegia valimine; M 4.3. Viirustõrjeprogrammi regulaarne kasutamine.
[21] M 2.157. Sobiva viirusetõrjeskanneri valimine.
[22] M 2.159. Viiruseskanneri värskendamine.
[23] M 6.65. Asjassepuutuvate isikute teavitamine turvaintsidentidest; M 6.59. Turvaintsidentide käsitlemise eest vastutavate isikute määramine.
[24] Välisvõrgu monitooringu ründetuvastuse seadmed (IDS) paigaldatakse vastavalt kokkuleppele asutusega ja selle kaudu edastatakse info tuvastatud ründekatsete kohta automaatselt CERTi.
[25] M 6.32. Regulaarne andmevarundus.
[26] M 6.33. Andmevarunduskontseptsiooni loomine.

kustutamiste korral on kõiki salvestatud andmeid võimalik teha uuesti kättesaadavaks. See on ühtlasi ka parim kaitse lunavararünde potentsiaalse kahju vastu.

Paljudes asutustes toimub andmevarundus selliselt, et töökohaarvuti kasutaja salvestab oma varundamisele kuuluvad andmed võrguserverisse või töökohaarvutis konkreetsesse kataloogi ning seejärel varundatakse (nt varundustarkvara abil[27]) vastavad andmed tsentraalselt. Selle protsessi puuduseks on tõsiasi, et andmevarunduse toimimine ja kvaliteet sõltub töötajate motivatsioonist ja distsiplineeritusest. Juhul kui kasutaja ei tee tööks olulistest andmetest regulaarselt varukoopiat, ei ole võimalik neid arvuti rikke korral enam taastada. Olukorras, kus ükskõik millised tööprotsesside toimimiseks olulised andmed on hävinud või neid on võltsitud, võib tööülesannete täitmine viibida või koguni seiskuda. Seetõttu on äärmiselt oluline, et andmevarunduse kohustuslike miinimumnõuete kohta oleks info edastatud kõikidele teenistujatele[28] ning kontrollitud, et varundamisele kuuluvad andmed salvestataks ka reaalselt vastavatesse serveritesse kas kasutajate endi poolt või automaatselt. Muidu võib näiteks sisevõrgust eemaldatud arvutite puhul jääda varundus tegemata. Funktsioneeriva andmevarundusprotsessi tagamiseks peab andmevarunduskontseptsioonis kehtestama ka nõude harjutada andmete taastamist praktikas.[29]

Hea praktika

Kaugtööl olles sünkroonitakse automaatselt tööjaama andmed serverisse siis, kui sülearvuti ühendatakse asutuse sisevõrku.

14 IT-spetsialisti tööülesannete ülevõtmine puhkuse vm eriolukorra ajal peab olema korraldatud.

Hea praktika

- ✓ On kokkulepe kohaliku arvutifirmaga, kes on nõus tulema nt riistvara ära vahetama.
- ✓ On asutud teenuseid välja viima enda majast, et sõltuvus IT-töötajast väheneks.

Süsteemi sujuva töö tagamiseks peab administraatoril olema sellest ülevaade.[30] Süsteemi ülevaade on ka süsteemi kontrollivõimaluse eelduseks (nt probleemsete seadistuste kontrollimine, muudatuste sisu kontrollimine). Kui administraator peaks ootamatult oma tööst kõrvale jääma, peaks ka tema asendajal olema võimalik süsteemist ülevaade saada. Näiteks kui valdavalt on kogu teadmine süsteemi seadistustest ja muudatustest kohaliku IT-spetsialisti peas, siis võib uuel inimesel tekkida raskusi IT-süsteemi administreerimise jätkamisega. Seetõttu peaksid administraatorite tehtud süsteemimuudatused olema dokumenteeritud, võimaluse korral peaks see toimuma automaatselt.

IT-spetsialisti asendamine peab olema reguleeritud[31] ning asendajal peab olema piisav väljaõpe, et süsteemiadministraatori tööülesandeid täita. Kui oma töötajate seast sobilikku isikut ei leita, tuleks kaaluda majaväliste jõudude kaasamist (nt sõlmitud kokkulepe kohaliku IT-ettevõttega).

15 Serveriruumis või selle vahetus läheduses peab olema gaasikustuti.[32]

Pulberkustuteid, mis vastavad tuleklassidele A (tahked ained), B (põlevad vedelikud) ja C (gaasid), ei tohiks kasutada elektriliste ja elektrooniliste seadmete kustutamiseks, kuna kustutuse tagajärjel tekkinud kahju on enamasti ülemäära suur. Seetõttu ei ole soovitatav serveriruumide vahetusse lähedusse paigutada pulberkustuteid, vaid tarvitada eranditult selleks sobivaid gaasikustuteid.

[27] Näiteks Synology Data Replicator, GFI Backup, Cobian Backup, Veeam Backup Agent, Backup PC, Veritas.
[28] M 6.36. Minimaalse andmevarunduse kontseptsiooni määratlemine.
[29] M 6.41. Andmete taastamise harjutamine.
[30] M 2.34. IT-süsteemi muutuste dokumenteerimine.
[31] M 3.3. Asendamise korraldamine.
[32] M 1.7. Tulekustutid.

Ainult nii on võimalik vältida seda, et põlengu tõttu tekkinud ärevushoos ei kasutataks ekslikult pulberkustutit.

16 IT-rakenduste ebapädevast kasutamisest tingitud kahjud on välditavad.[33]

On ülimalt oluline, et kasutajad läbiksid enne IT-kasutusel põhinevate tööülesannete ülevõtmist ka piisava koolituse. See puudutab nii standardsete programmipakettide kui ka spetsiaalselt arendatud tarkvara kasutama õppimist. Lisaks on tarvis koolitusi korraldada ka siis, kui IT-rakenduses on toimunud suured muudatused. Juhul kui vastava IT-rakenduse kohta on olemas kergesti mõistetavad käsiraamatud, võib koolituse asemel kehtestada ka nõude, et töötajatel tuleb end uue materjaliga iseseisvalt kurssi viia.

Lugupidamisega

/allkirjastatud digitaalselt/

Ines Metsalu-Nurminen
peakontrolör

Meeli Saksing
Meeli.Saksing@riigikontroll.ee

[33] M 3.4. Väljaõpe enne programmi tegelikku kasutamist.